

# Inhaltsverzeichnis

	Seite
Vorwort .....	V
Abkürzungsverzeichnis .....	XXIII
Literaturverzeichnis .....	XXXI

§ 1. Einführung ( <i>Rüpke</i> ) .....	1
A. Kommunikationstechnische Entwicklungsstufen .....	1
B. Das hergebrachte/fortwirkende deutsche Konzept .....	1
C. Europäische Rechtsentwicklung .....	3
D. Zur Gesamtdarstellung .....	4

## 1. Teil. Grundlagen des Datenschutzes

### 1. Abschnitt. Historisch-gesellschaftliche und sozialwissenschaftliche Orientierung

§ 2. Geschichte des Datenschutzrechts im 20. Jahrhundert ( <i>v. Lewinski</i> ) .....	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. Berufsrechtliche 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. Datenschutzgesetze und Volkszählungsurteil .....	18
I. Vorfeld .....	18
1. Staat als „Großer Bruder“ .....	19
2. Nicht-öffentlicher Bereich .....	19

	Seite
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 .....	24
I. Telekommunikationsdatenschutz .....	24
II. Internet .....	25
H. Europäisierung des Datenschutzrechts .....	25
I. Europarechtliche Regelungen .....	26
II. Europäische Rechtsprechung .....	27
III. Weiterentwicklung des europäischen Rechtsrahmens für den Datenschutz .....	27
IV. Das BDSG 2018 .....	28
§ 3. Leitlinien für den Datenschutz auf informations- und kommunikationstheoretischer Grundlage ( <i>Rüpkke</i> ) .....	29
A. Ausgangslage .....	29
I. Neue Anforderungen .....	29
II. Informationelle Selbstbestimmung im deutschen Recht .....	30
III. Personenbezug und Gesellschaft .....	32
IV. Informationeller „Start“ für das BDSG .....	32
B. Das Konzept Information .....	33
I. Entwicklung in neuer Zeit (20. Jhdt.) .....	33
II. Information und Kommunikation bei Luhmann .....	35
III. Information in Sozial- und Rechtswissenschaft .....	37
1. Kritischer Ansatz bei Albers .....	37
2. Information im Verwaltungsverfahren und nach IFG .....	39
3. Folgerung .....	39
C. Perspektiven .....	40
<b>2. Abschnitt. Verfassungsrechtliche Basis in der Bundesrepublik</b>	
§ 4. Grundrechtliche Gewährleistung des Datenschutzes – Probleme, Lösungsansätze, Alternativen ( <i>Rüpkke</i> ) .....	42
A. Ausgangslage .....	42
B. Generalisierender Schutz personenbezogener Informationen .....	43
C. Sozialcharakter der – personenbezogenen – Information .....	45
I. Zur Rechtsprechung des BVerfG .....	45
II. Eingrenzung informationellen Persönlichkeitsschutzes .....	46
1. Geheimnisse .....	46
2. Probleme informationeller Zuordnung .....	47
3. Folgerung .....	47
D. Privatheit (nebst Intimität) insbesondere .....	48
E. Grundrechtliche Bedeutung des Persönlichkeitsschutzes und des Rechts auf informationelle Selbstbestimmung im nicht-öffentlichen Bereich (Drittwirkung) .....	49
I. Persönlichkeitsrecht .....	49



II. Das Recht auf informationelle Selbstbestimmung insbesondere	51
III. Systematische Folgerungen .....	53
IV. Weiterreichende verfassungsrechtliche Fragen .....	54
§ 5. Ausgewählte Probleme des Datenschutzes gemäß Rechtsprechung des BVerfG ( <i>Rüppe</i> ) .....	55
A. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme .....	56
I. Schutzbereich .....	56
II. Eingriffe/Schranken .....	57
III. Parallelen zu anderen Gewährleistungen des Persönlichkeitsbereichs .....	58
IV. Erweiterte Bedeutung der G-VliS .....	59
V. Abgrenzung zum Recht auf informationelle Selbstbestimmung	59
1. Begründung des BVerfG und Kritik .....	59
2. Wesentliche Unterscheidung .....	59
3. Perspektivenwechsel .....	60
B. Schutz des (unantastbaren) Kernbereichs privater Lebensgestaltung .....	62
I. Entwicklung .....	62
II. Neu ausgeprägter Kernbereich .....	63
III. „Unantastbarkeit“ .....	65
1. Problemstellung .....	65
2. Herkömmliche Regeln .....	65
3. Unantastbarkeit im Grundgesetz .....	66
a) Grundlagen .....	66
b) Leitlinien in der Rechtsprechung des BVerfG zu Art. 1 Abs. 1 GG .....	67
c) Einschränkungen der Menschenwürde systematisch betrachtet .....	68
4. Praktische Ergebnisse für den Kernbereich privater Lebensgestaltung .....	69
IV. Zweistufiges Kontrollverfahren insbesondere .....	70
1. Erste Stufe: Abgrenzung im Echtzeit-(Live)Verfahren .....	70
2. Zweite Stufe: Einschaltung eines Unabhängigen .....	71
C. Automatisierter Datenabgleich, auch „Rasterfahndung“ .....	73
I. Bedeutung für die Praxis und für das grundrechtliche Verständnis .....	73
II. Kein Grundrechtseingriff bei Nichttreffern gemäß jüngerer Rechtsprechung des BVerfG .....	74
III. Kritische Prüfung der (Nicht-)Eingriffsthese .....	75
1. Breit angelegte Überwachung? .....	75
2. Involvierte Daten und/oder personenbezogene Informationen? .....	76
3. Eingeschlossene Übermittlungsvorgänge .....	77
4. Hohe Einschreitschwelle? .....	78
IV. Ausblick .....	78
D. „Vorratsdatenspeicherung“ .....	80
I. Entwicklung bis hin zu einer Entscheidung des BVerfG .....	80

	Seite
II. Die weitere Entwicklung – geprägt durch Urteile des EuGH ....	81
III. Anzuwendender Grundrechtsschutz .....	83
IV. Bisherige staatlich verordnete anlasslose Speicherungen .....	84
V. Das Metadaten-Register: Speicherung/Nutzung, Datensicherung .....	85
VI. Neue gesetzliche Regelung / verbleibende Bedenken .....	87
 <b>3. Abschnitt. Europarechtliche (primärrechtliche) Basis</b> 	
§ 6. Art. 8 EMRK in Anwendung auf personenbezogene Informationen durch den EGMR ( <i>Rüppe</i> ) .....	90
A. Ausgangspunkt: Privatleben im weiteren Sinne .....	90
B. Beruf, Wirtschaft .....	91
C. Besondere Arten personenbezogener Informationen .....	92
D. Öffentlichkeit .....	93
E. Persönlichkeitsschutz .....	95
§ 7. Grundrechtliche Gewährleistungen in der EU ( <i>Rüppe</i> ) .....	97
A. Rechtlicher Rahmen .....	97
I. Rechtsetzungskompetenz der EU .....	97
II. Grundrechtlicher Gewährleistungsbereich in der EU .....	98
B. Der vor Inkrafttreten der Grundrechte-Charta (bis zum 1.12.2009) gewährleistete Schutz .....	99
I. Persönlichkeitsschutz und Transparenz bei der öffentlichen Hand .....	99
1. Namen(sliste) von Lobbyisten .....	99
2. Parlamentarische Aktivitäten .....	101
II. Persönlichkeitsschutz und Transparenz individueller wirtschaftlicher Verhältnisse .....	101
1. Überblick zu Einkünften (Deutschland, Österreich) .....	101
2. Steuergeheimnis in Deutschland .....	102
3. Einkünfte, Vermögen, Steuern: Transparenz in Europa .....	103
C. Der von der Charta der Grundrechte der EU gewährleistete Schutz .....	106
I. Systematik .....	106
II. Rechtsprechung des EuGH .....	107
III. Zur weiteren Interpretation des Art. 8 GRCh .....	109
1. Entstehung der Charta-Bestimmung .....	109
2. Verfassungen – Überlieferungen – der Mitgliedstaaten .....	109
IV. Folgerungen .....	110
 <b>2. Teil. Datenschutzrecht in neuer Gestalt:</b> <b>Die Datenschutzgrundverordnung 2016/679 vom 27.4.2016 insbesondere</b> 	
<b>1. Abschnitt. Geltungsbereich der DS-GVO</b>	
§ 8. Sachlicher Geltungsbereich (Art. 2 DS-GVO) ( <i>Rüppe</i> ) .....	115
A. Rechtssystematische Eingrenzungen .....	115
I. Grundregeln .....	115
II. Abgrenzung zum Geltungsbereich der neuen Richtlinie 2016/680 und deren Umsetzung im BDSG 2018 .....	116



	Seite
III. „Öffentlicher Bereich“ .....	117
1. Unterscheidung zwischen öffentlichem und nicht-öffentlichem Bereich .....	117
2. Deutsche Ausgestaltung im öffentlichen Bereich .....	118
3. Innerstaatliche Gesetzgebungskompetenzen .....	119
a) Öffentlicher Bereich .....	119
b) Nicht-öffentlicher Bereich .....	120
B. Eingrenzungen von der Sache her .....	120
I. Technik der Informationsverarbeitung .....	121
1. Automatisierte Verarbeitung .....	121
2. Nichtautomatisierte Verarbeitung im „Dateisystem“ .....	121
a) Begriffliches .....	121
b) Zielsetzung .....	122
c) Akten insbesondere .....	123
II. Persönliche und familiäre Tätigkeiten .....	124
C. Besonders geregelte Bereiche .....	126
I. Unionsrecht .....	126
II. Mitgliedstaatliches Recht .....	126
1. Nicht-öffentlicher Bereich .....	126
2. Öffentlicher Bereich .....	128
a) Bereichsspezifisches Recht und Subsidiarität des allgemeinen Datenschutzrechts .....	128
b) „Deckungsgleichheit“ .....	129
§ 9. Räumlicher Geltungsbereich ( <i>Rüppe</i> ) .....	130
A. Problemstellung .....	130
B. Lösungswege .....	130
 <b>2. Abschnitt. Rechtlich vorgegebene Grundstruktur für die Verarbeitung personenbezogener Informationen</b> 	
§ 10. Betroffene. Personenbezogene Informationen ( <i>Rüppe</i> ) .....	132
A. Einführung .....	132
B. Personenbezogene Informationen (Merkmale) .....	133
C. Mehrfacher bzw. eingeschränkter Personenbezug .....	135
I. Grundmodell .....	135
II. Gesteuerter Personenbezug .....	136
III. Sachdaten. Geodaten .....	138
D. Identifizierte oder identifizierbare Betroffene .....	140
I. Die Einzelnen im Fokus .....	140
II. Die Bedeutung des informationellen Umfelds .....	140
III. Zusatzwissen im rechtlichen Rahmen .....	142
IV. Zusatzwissen Dritter .....	142
1. Relativer/absoluter Personenbezug .....	142
2. Dynamische IP-Adresse als personenbezogenes Datum? .....	143
V. Abstufung zwischen identifizierten und identifizierbaren Betroffenen .....	145
1. Pseudonymität .....	145
2. Eingeschränkte Anwendung datenschutzrechtlicher Bestimmungen gemäß Art. 11 DS-GVO .....	146

	Seite
E. Zusammenfassung. Ausblick .....	147
§ 11. Verantwortliche und andere im Rahmen der Verarbeitung mitwirkende Stellen ( <i>Rüppe</i> ) .....	149
A. „Verantwortlicher“ .....	149
B. Beschäftigte .....	150
C. „Auftragsverarbeiter“ .....	151
I. Rechtliche Grundlagen .....	151
II. Anwendungen .....	152
D. „Gemeinsam Verantwortliche“ (Art. 26 DS-GVO) .....	153
I. Vorangegangene Regelungen gemeinsamer Verantwortlichkeit .	153
II. Inhalt und Ausprägungen gemeinsamer Verantwortlichkeit .....	155
III. Besondere Verarbeitungskonstellationen im Internet .....	156
IV. Telemediendienste (Hostprovider/Portale), Nutzer und Betroffene .....	157
V. Résumé .....	159
1. Öffnung zu neuem Lösungsweg .....	159
2. Hemmnisse? .....	160
E. Dritte und Empfänger .....	161
§ 12. Rechtsgrundlagen der Verarbeitung ( <i>Rüppe</i> ) .....	162
A. Datenschutzrechtlicher Regelungsansatz in der DS-GVO .....	162
B. Informationsverarbeitung auf gesetzlicher Grundlage (Art. 6 Abs. 1 lit. b-f) .....	163
I. Vertragsrechtliche Beziehungen .....	163
II. Erfüllung von Rechtspflichten .....	164
III. Wahrnehmung öffentlicher Aufgaben .....	165
IV. Wahrung berechtigter Interessen Privater .....	166
V. Schutz lebenswichtiger Interessen .....	168
C. Erforderlichkeit/Verhältnismäßigkeit .....	168
I. Kausalzusammenhang? .....	168
II. Diskrepanzen der Interpretation .....	169
III. Erforderlichkeit/Verhältnismäßigkeit im (alten) Polizeirecht ....	171
IV. Rechtsprechungspraxis .....	173
V. Ausgewählte Folgerungen .....	175
1. Vertragsverhältnis .....	175
2. Verbundene Unternehmen .....	176
3. Öffentliche Verwaltung .....	177
D. Zweckbindung .....	177
§ 13. Einwilligung und andere Willensäußerungen ( <i>v. Lewinski</i> ) .....	180
A. Willensäußerungen im Datenschutzrecht .....	180
I. Rechtsnatur .....	181
1. Datenschutzrechtliche Einordnung .....	181
2. Zivilrechtliche Einordnung .....	181
a) Mitgliedstaatliche oder europäische Rechtsgeschäftslehre? .....	181
b) Willenserklärung oder Realakt? .....	182
3. Kein Grundrechtsverzicht .....	182



	Seite
II. Begrifflichkeit .....	183
1. Legaldefinition, Gesetzesbegriffe und Lücken .....	184
2. Umfassende Nomenklatur .....	184
III. (Kommendes) Datenrecht .....	185
B. Allgemeine Anforderungen an Willensäußerungen .....	186
I. Modi der Willensäußerung .....	186
II. Freiwilligkeit .....	187
1. Grenzen des willensäußerungsbasierten Konzepts .....	188
a) Macht- und Wissensasymmetrien .....	188
b) Rationale Apathie .....	189
c) Individualität der Willensäußerung und soziale Aspekte von Datenverarbeitung .....	190
2. Asymmetrien und Abhängigkeitsverhältnisse .....	190
3. Koppelungsverbote .....	191
4. Einwilligungsverbot und Unbeachtlichkeit der Willens- äußerung .....	191
III. Willensäußerungen von Minderjährigen und beschränkt Geschäftsfähigen .....	192
1. Allgemeine Einsichtsfähigkeit und typische Altersgrenzen ...	192
2. Datenschutzrechtliche Rechtsgeschäftsfähigkeit .....	194
IV. Spezialgesetzliche Regelungen und mitgliedstaatliche Abweichungsmöglichkeiten .....	195
C. Datenschutzrechtliche Willenserklärungen .....	196
I. Einwilligung .....	196
1. Informiertheit und Transparenz .....	196
a) Vorangehende Unterrichtung .....	196
b) Vorangehende Belehrung .....	197
c) Verständlichkeit .....	197
2. Bestimmtheit .....	197
3. Form .....	198
a) Grundsatz der Formfreiheit .....	198
b) Formvorgaben .....	198
aa) AGB .....	198
bb) Ausdrücklichkeit bei sensiblen Gesundheitsdaten ...	199
cc) Ausdrücklichkeit bei automatisierten Einzelent- scheidungen .....	200
dd) Schriftform bei Einwilligungen im Beschäftigungs- verhältnis .....	200
c) Nachweisbarkeit .....	200
4. Rechtswirkungen .....	200
a) Konstitutiver Erlaubnistatbestand .....	200
b) Zeitpunkt und Wirksamkeitsdauer .....	200
c) Folgen ungenügender Einwilligung .....	201
II. Widerspruch .....	201
1. Transparenz als Voraussetzung .....	202
2. Bestimmtheit .....	202
3. Formfreiheit .....	202
4. Rechtswirkungen .....	203

	Seite
III. Widerruf von Einwilligung und Widerspruch .....	204
1. Beschränkungen und Bedingungen .....	204
2. Informiertheit .....	205
3. Bestimmtheit .....	205
4. Formfreiheit .....	205
5. Rechtswirkungen .....	205
a) Rückgriff auf gesetzliche Erlaubnisnormen .....	205
b) Rückwirkung auf Vertragsverhältnisse .....	205
6. Verhältnis zur Anfechtung .....	206
IV. Stellvertretung .....	206
1. Gewillkürte Vertretung .....	206
2. Gesetzliche Vertretung. Minderjährige .....	207
V. Genehmigung .....	208
VI. Verzicht auf Betroffenenrechte .....	208
VII. Verhältnis datenschutzrechtlicher Ansprüche zur Unwirk- samkeit des Rechtsgeschäfts .....	208
D. Bloße Willensäußerungen .....	209
I. Formfreiheit von Einverständnis und Einwand .....	209
II. Kenntnis des Verantwortlichen .....	210
III. Wegfall des Einverständnisses und des Einwands .....	210
IV. „Vertretung“ und „Genehmigung“ bei Einverständnis und Einwand .....	210
§ 14. Datenklassen ( <i>Rüppe</i> ) .....	211
A. Allgemein zugängliche Quellen .....	211
B. Äußerer Umgang/Kontakt einerseits und Inhalte andererseits .....	212
C. Wirtschafts- und Finanzinformationen .....	213
D. Verarbeitung „besonderer Kategorien personenbezogener Daten“ (sensitive Information) .....	214
I. Normative Grundlagen .....	214
II. Ein vormaliges interpretatorisches Missverständnis .....	214
§ 15. Rechte der betroffenen Person ( <i>Rüppe</i> ) .....	217
A. Informationsfluss vom Verantwortlichen zum Betroffenen .....	217
I. Regelmäßige Informationspflichten des Verantwortlichen .....	217
1. Die Pflichten im einzelnen .....	217
2. Einschränkungen der Informationspflicht .....	219
a) Fälle nachträglicher Zweckänderung .....	219
b) Fälle der Erhebung-nicht-beim-Betroffenen .....	219
aa) DS-GVO .....	219
bb) BDSG 2018 .....	220
c) Übersicht .....	221
3. Wertung .....	222
II. Auskunftsrecht des Betroffenen .....	222
1. Grundlagen .....	222
2. Charakteristika der Auskunftspflicht .....	223
3. Einschränkungen des Rechts auf Auskunftserteilung .....	224
a) DS-GVO .....	224



	Seite
b) BDSG 2018 .....	224
III. Datenportabilität .....	225
B. Interventionsrechte des Betroffenen .....	227
I. Berichtigung .....	227
II. Löschung .....	227
1. Systematik .....	227
2. Information an Dritte .....	228
III. Einschränkung der Verarbeitung (Sperrung) .....	229
 <b>3. Abschnitt. Steuerung riskanter Verfahren</b>	
§ 16. Automatisierte Einzelentscheidung einschließlich Profiling ( <i>Eckhardt</i> ) .....	231
A. Verbot der automatisierten Entscheidung im Einzelfall .....	232
I. Automatisierte Entscheidung im Einzelfall .....	232
1. Automatisierte Verarbeitung .....	233
2. Profiling .....	233
II. Verbot der automatisierten Entscheidung im Einzelfall .....	234
1. Ausschließlichkeit der automatisierten Verarbeitung .....	234
2. Rechtliche Wirkung und erhebliche Beeinträchtigung .....	235
B. Ausnahmen vom Verbot der automatisierten Einzelentscheidung ...	236
I. Ausnahmen vom Verbot der automatisierten Einzelentscheidung (Abs. 2) .....	236
II. Schutz der Rechte der betroffenen Personen (Abs. 3) .....	237
III. Ausschluss besonderer Kategorien personenbezogener Daten (Abs. 4) .....	237
IV. Einschränkung nach Art. 23 DS-GVO .....	238
C. Zulässigkeit der automatisierten Einzelentscheidung und Transparenz .....	238
I. Zulässigkeit einer automatisierten Einzelentscheidung .....	238
II. Informationspflichten in Bezug auf die automatisierte Einzelentscheidung .....	239
D. Regelung des Profiling in der DS-GVO .....	240
I. Zulässigkeit des Profiling .....	240
II. Transparenz in Bezug auf das Profiling .....	241
III. Profiling zur Direktwerbung .....	241
IV. Scoring nach dem BDSG 2018 .....	242
§ 17. Verzeichnis von Verarbeitungstätigkeiten, Datenschutz-Folgenabschätzung, Vorherige Konsultation ( <i>Eckhardt</i> ) .....	244
A. Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DS-GVO) .....	245
I. Überblick .....	246
II. Regelung in der DS-GVO .....	246
1. Verpflichtung zum Führen eines Verzeichnisses von Verarbeitungstätigkeiten .....	246
2. Gegenstand und Inhalt des Verzeichnisses .....	247
a) Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen .....	247
b) Verzeichnis von Verarbeitungstätigkeiten des Auftragsverarbeiters .....	248

	Seite
3. Form und Bereitstellung des Verzeichnisses .....	249
4. Befreiung vom Führen des Verzeichnisses .....	249
5. Sanktionierung eines Verstoßes .....	251
B. Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) .....	251
I. Überblick .....	252
II. Regelung in der DS-GVO .....	253
1. Verpflichtung zur Datenschutz-Folgenabschätzung .....	253
2. Pflicht zur Durchführung einer Datenschutz-Folgenab-	
schätzung .....	254
a) Zweistufigkeit der Regelung in Art. 35 DS-GVO .....	254
b) Gegenstand der Datenschutz-Folgenabschätzung .....	254
c) Pflicht zur Durchführung einer Datenschutz-Folgenab-	
schätzung .....	255
3. Durchführung einer Datenschutz-Folgenabschätzung .....	256
4. Datenschutz-Folgenabschätzung im Rahmen des Gesetz-	
gebungsverfahrens .....	258
5. Verhaltensregelungen und Zertifizierungen .....	259
6. Übergangsregelung für die Datenschutz-Folgenabschätzung .....	259
7. Sanktionierung eines Verstoßes .....	259
C. Vorherige Konsultation (Art. 36 DS-GVO) .....	260
I. Überblick .....	260
II. Regelung in der DS-GVO .....	260
1. Verpflichtung zur Vorherige Konsultation .....	260
2. Voraussetzungen und Inhalt einer Vorherige Konsultation ...	260
a) Aufgabe des Verantwortlichen .....	262
b) Aufgabe der Aufsichtsbehörde .....	262
3. Übergangsregelung für die Vorherige Konsultation .....	263
4. Sanktionierung eines Verstoßes .....	263
§ 18. Übermittlung personenbezogener Daten in die USA ( <i>Eckhardt</i> ).....	264
A. Einführung .....	264
B. Übermittlung personenbezogener Daten in Drittländer .....	265
I. Überblick und Systematik .....	265
II. Zweistufigkeit der Zulässigkeitsprüfung .....	265
III. Allgemeine Grundsätze der Datenübermittlung .....	266
IV. EuGH zur Übermittlung personenbezogener Daten in Dritt-	
staaten .....	267
V. EU-US Privacy Shield .....	269

#### 4. Abschnitt. Datensicherheit. Technischer/organisatorischer Datenschutz

§ 19. Sicherheit der Verarbeitung ( <i>Eckhardt</i> ) .....	271
A. Überblick .....	272
B. Verpflichteter und Inhalt der Verpflichtung .....	273
I. Verpflichteter .....	273
II. Inhalt der Verpflichtung .....	274
1. Gegenstand der Bewertung .....	274



2. Pflicht zu technischen und organisatorischen Maßnahmen (Abs. 1) .....	275
3. Kriterien zur Beurteilung der Angemessenheit des Schutzniveaus (Abs. 2) .....	277
4. Verhaltensregeln und Zertifizierungen (Abs. 3) .....	278
5. Verpflichtung der Personen mit Zugang zu personenbezogenen Daten .....	278
6. Sicherheit der Verarbeitung nach DS-GVO und IT-Sicherheit .....	279
III. Datenschutz als Grenze der Sicherheit der Verarbeitung .....	280
IV. Relevanz im Rahmen der Festsetzung einer Sanktion .....	281
V. Bußgeldsanktion .....	281
C. Regelungen in Deutschland .....	281
D. NIS-Richtlinie .....	282
§ 20. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellung ( <i>Eckhardt</i> ) .....	284
A. Überblick über die historische Entwicklung .....	284
B. Überblick und Ziel .....	285
C. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellung .....	286
I. Regelungsadressat des Art. 25 DS-GVO .....	286
II. Datenschutz durch Technikgestaltung (Data Protection by Design) .....	287
III. Datenschutzfreundliche Voreinstellung (Data Protection by Default) .....	288
IV. Genehmigte Zertifizierungsverfahren .....	289
V. Technisch-organisatorische Maßnahmen .....	289
VI. Relevanz im Rahmen der Festsetzung einer Sanktion .....	289
VII. Sanktionierung eines Verstoßes .....	290
D. Bewertung des Ansatzes .....	290

### 5. Abschnitt. Datenschutzkontrolle

§ 21. Interne (Selbst-)Kontrolle: Datenschutzbeauftragter ( <i>Eckhardt</i> ) .....	291
A. Benennung eines Datenschutzbeauftragten .....	293
I. Unionsweite Benennung eines Datenschutzbeauftragten .....	294
1. Behörden und öffentliche Stellen .....	294
2. Benennungspflicht aufgrund der Kerntätigkeit .....	296
II. Pflicht zur Benennung eines Datenschutzbeauftragten nach nationalem Recht .....	297
III. Freiwillige Benennung eines Datenschutzbeauftragten .....	300
IV. Qualifikation des Datenschutzbeauftragten .....	301
V. Modalitäten der Benennung eines Datenschutzbeauftragten .....	303
VI. Sanktion der Nichtbenennung .....	304
B. Stellung des Datenschutzbeauftragten .....	305
I. Einbeziehung des Datenschutzbeauftragten .....	305
II. Pflicht zur Unterstützung des Datenschutzbeauftragten .....	306
III. Weisungsfreiheit .....	307

	Seite
IV. Benachteiligungs- und Abberufungsverbot .....	308
V. Direkte Berichtslinie .....	308
VI. Anrufungsrecht der betroffenen Person .....	308
VII. Pflicht zur Geheimhaltung und Vertraulichkeit .....	309
VIII. Weitere Aufgaben des Datenschutzbeauftragten .....	310
IX. Verbot der Interessenkollision .....	310
C. Aufgaben des Datenschutzbeauftragten .....	311
I. Unterrichtung und Beratung .....	312
II. Überwachung der Einhaltung des Datenschutzrechts .....	312
1. Überwachungs- und Handlungssystem der Verantwortlichen.....	313
2. Pflicht des Datenschutzbeauftragten .....	313
III. Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung .....	314
IV. Zusammenarbeit mit und Ansprechpartner der Aufsichtsbehörde .....	314
V. Risikobasierter Ansatz .....	315
§ 22. Datenschutzaufsichtsbehörden ( <i>v. Lewinski</i> ) .....	316
A. Allgemeines .....	316
B. System der Datenschutzaufsicht .....	317
I. Allgemeine Datenschutzbehörden .....	317
1. Europäischer Datenschutzbeauftragter .....	317
2. Mitgliedstaatliche Datenschutzaufsichtsbehörden .....	318
a) Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI) .....	318
b) Landesdatenschutzbeauftragte .....	318
II. Koordinierungsgremien und Netzwerke .....	319
1. Europäischer Datenschutzausschuss .....	319
2. Koordinierungsgremien bundesstaatlicher Datenschutzaufsicht .....	319
a) Konferenz der Datenschutzbeauftragten .....	319
b) Düsseldorfer Kreis .....	320
c) Vertretung im Europäischen Datenschutzausschuss .....	320
III. Sektorielle Aufsicht .....	321
1. Medien .....	321
2. Kirchen und Religionsgemeinschaften .....	321
3. Berufsgeheimnissen unterliegende Bereiche .....	322
4. Gerichte .....	323
IV. Europäische Kommission .....	323
V. „Konkurrierende“ Aufsichtsbehörden .....	324
VI. Stiftung Datenschutz .....	324
C. Zuständigkeit der Aufsichtsbehörden .....	325
I. Europarechtliches Territorialitätsprinzip .....	325
II. Innerstaatliche Zuständigkeitsabgrenzung von BfDI und Landesdatenschutzbehörden .....	325
D. Stellung der Aufsichtsbehörden .....	326
I. „Völlige Unabhängigkeit“ der Aufsichtsbehörden .....	326



	Seite
II. Ausstattung der Aufsichtsbehörde .....	327
1. Personelle Ausstattung .....	327
2. Sachliche Ausstattung .....	328
3. Finanzielle Ausstattung .....	328
III. Leitung der Aufsichtsbehörde .....	328
1. Persönliche und fachliche Anforderungen .....	328
2. Wahl und Ernennungsverfahren .....	329
3. Amtszeit .....	329
4. Verschwiegenheitspflicht .....	329
5. Aussageverweigerungsrecht .....	329
E. Handeln der Aufsichtsbehörde .....	330
I. Aufgaben der Aufsichtsbehörde .....	330
1. Klassische Aufsichtstätigkeit .....	330
2. Informationelle Aufgaben .....	330
a) Hinweispflicht an Betroffene, Verantwortliche und die Öffentlichkeit .....	330
b) Tätigkeitsbericht .....	331
3. Beratende Aufgaben .....	331
4. Untersuchungen .....	331
5. Beobachtende Aufgabe .....	331
6. Beschwerdestelle .....	332
7. Datenschutzzertifizierung .....	332
8. Genehmigungen .....	332
9. Sonstige Aufgaben .....	332
10. Aufgaben der JI-RL .....	332
II. Befugnisse der Aufsichtsbehörde .....	333
1. Untersuchungsbefugnisse .....	333
2. Abhilfebefugnisse .....	334
3. Genehmigungsbefugnisse .....	334
4. Beratende Befugnisse .....	334
5. Weitere Befugnisse .....	335
6. Befugnisse nach der JI-RL .....	335
7. Umsetzung in mitgliedstaatliches Recht .....	335
8. Ausübung der Befugnisse.....	336
F. Zusammenarbeit der Aufsichtsbehörden .....	336
I. Formen der Zusammenarbeit .....	336
1. Kooperationsangebote und Amtshilfe .....	336
2. Kohärenzverfahren .....	337
3. Dringlichkeitsverfahren .....	338
II. Zusammenarbeit und Unabhängigkeit .....	338
III. Netzwerk und Legitimation .....	339
G. Rechtsschutz gegen Aufsichtsbehörden .....	339
I. Vorgaben der DS-GVO und verwaltungsgerichtlicher Rechts- schutz .....	339
II. Staatshaftung .....	340
III. Entscheidungen des Europäischen Datenschutzausschusses .....	341

6. Abschnitt. Haftung, Sanktionen	Seite
§ 23. Haftung ( <i>v. Lewinski</i> )	342
A. Schadenersatzrecht	342
I. Anwendbare Normen	343
1. Datenschutzrecht	343
2. Zivilrechtliche Haftung	343
a) Vertragliche und vorvertragliche Ansprüche	344
b) Deliktische Ansprüche	344
3. Öffentlich-rechtliche Haftungsansprüche	344
II. Anspruchsberechtigter	345
III. Anspruchsverpflichtete	345
IV. Anspruchsvoraussetzungen	346
1. Schaden	346
2. Rechtswidriges Handeln (Datenschutzverstoß)	347
3. Kausalität	347
4. Verschulden	347
V. Modifikationen des Anspruchs	348
VI. Schadenersatzhöhe	348
VII. Beweislast	349
VIII. Keine Versicherungspflicht	350
IX. Rechtsweg, Geltendmachung	350
X. Übertragbarkeit, Vererblichkeit	350
Exkurs: Bereicherungsausgleich	351
B. Verbandsklage	352
C. Wettbewerbliche Haftung	352
I. Lauterkeitsrecht	352
1. Anwendungsbereich des Wettbewerbsrechts	353
2. Datenschutzverstoß als Wettbewerbsverstoß	353
a) Wettbewerbsbezug des Datenschutzrechts	353
b) Wettbewerbsrechtliche Unlauterkeit	355
3. Geltendmachung/Rechtsfolgen	355
II. Datenschutzverstöße im Kartellrecht	355
§ 24. Straf- und Bußgeldtatbestände ( <i>v. Lewinski</i> )	357
A. Rechtstaatliche Grenzen des Datenschutzsanktionsrecht	358
I. Verweisungstechnik	358
II. Unverständlichkeit	359
III. Fehlende Bestimmtheit	359
IV. Folgen einer Unionsrechtswidrigkeit oder Verfassungswidrigkeit	360
B. Datenschutzordnungswidrigkeiten	361
I. Bußgeldtatbestände	361
1. Verstöße gegen Pflichten der Verantwortlichen bzw. der Auftragsverarbeiter	361
2. Verstöße gegen Pflichten der Zertifizierungs- und Überwachungsstellen	362
3. Verstöße im Rahmen der konkreten Verarbeitung	362
4. Weitere Bußgeldtatbestände nach dem BDSG	363
5. Weitere Bußgeldtatbestände nach dem BDSG	363



	Seite
II. Täter .....	363
III. Tatbegehungsformen .....	364
IV. Bußgeldverfahren .....	365
V. Sanktionen .....	365
1. Verwarnung .....	365
2. Bußgeld .....	366
a) Höhe des Bußgelds .....	366
b) Maßstäbe der Bußgeldbemessung .....	367
C. Datenschutzstraftaten .....	368
I. Strafnormen des allgemeinen Datenschutzrechts .....	368
II. Strafnormen im bereichsspezifischen Datenschutzrecht .....	369
III. Allgemeines Strafrecht .....	370

### 3. Teil. Ausgewählte, von der DS-GVO nicht umfasste Bereiche

§ 25. Gerichtsbarkeit ( <i>Rüpke</i> ) .....	371
A. Zur Anwendbarkeit des Datenschutzrechts .....	371
I. Überblick .....	371
II. Veränderter Grundansatz .....	372
III. Verfassungsrechtliche Anbindung .....	373
IV. Datenschutzrechtliche Leitprinzipien im Gerichtsverfahren ....	373
B. Beteiligte. Öffentlichkeit .....	375
I. Parteiöffentlichkeit .....	375
II. Parteivortrag .....	375
III. Verwendung der Information jenseits des Gerichtsverfahrens...	376
IV. Saalöffentlichkeit .....	377
1. Inhalt und Umfang .....	377
2. Bewertung .....	378
V. Veröffentlichung gerichtlicher Entscheidungen .....	379
1. Publikationsgebot .....	379
2. Pseudonymisierung .....	380
3. Rechtliche Folgerung .....	380
§ 26. Datenschutz im Bereich Telekommunikation ( <i>Eckhardt</i> ) .....	383
A. e-Privacy Richtlinie .....	384
B. Verhältnis der DS-GVO zur e-Privacy-Richtlinie und den nationalen Regelungen .....	385
I. Verhältnis der DS-GVO zur e-Privacy-Richtlinie .....	385
II. Verhältnis der DS-GVO zu den Datenschutzbestimmungen des TKG und des TMG .....	386
1. Datenschutzbestimmungen des TKG .....	386
2. Datenschutzbestimmungen des TMG .....	388
3. E-Commerce-Richtlinie .....	389
III. Zusammenfassung .....	390
C. Datenschutz in der Telekommunikation .....	390
I. Datenschutz im Telekommunikationsgesetz .....	390
1. Schutzbereich .....	390
a) Schutzgegenstand .....	390
b) Persönlicher Schutzbereich .....	391

	Seite
2. Dienstespezifischer Anwendungsbereich .....	392
3. Verpflichteter Personenkreis – Datenschutz .....	393
a) Diensteanbieter und geschäftsmäßiges Erbringen von Telekommunikationsdiensten .....	393
b) Abgrenzung zum Erbringen von Telekommunikations- diensten .....	393
4. Inhalt der Verpflichtung und Rechtmäßigkeitstatbestände ....	395
a) Informationspflichten (§ 93 TKG) .....	395
b) Einwilligung (§ 94 TKG) .....	396
c) Gesetzliche Rechtmäßigkeitstatbestände des TKG .....	397
aa) Bestandsdaten (§ 95 TKG) .....	397
bb) Verkehrsdaten (§§ 96, 97 TKG) .....	398
cc) Dienst mit Zusatznutzern und Standortdaten (§ 98 TKG) .....	400
dd) Einzelverbindungs nachweis (§ 99 TKG) .....	401
ee) Weitere telekommunikationsspezifische Regelungen (§§ 100–107 TKG) .....	401
ff) Technische Schutzmaßnahmen und Daten- und Informationssicherheit (§§ 109, 109a TKG) .....	403
II. Schutz des Fernmeldegeheimnisses (§§ 88–90 TKG) .....	404
D. Datenschutz in den Telemedien .....	405
Sachverzeichnis .....	407