Inhaltsübersicht

		Seite
Vorwort		V
Bearbeiterverzeichnis		XLV
Abkürzungsverzeichnis		XLIX

Teil I. Allgemeine datenschutzrechtliche Grundlagen und Strukturen

Kapitel 1.	Vom Volkszählungsurteil zur Datenschutz-Grundverordnung	1
Kapitel 2.	Die Europäische Dimension des Datenschutzes	48
Kapitel 3.	Anwendbares Datenschutzrecht und Zuständigkeit der Aufsichtsbehörden	69
Kapitel 4.	Internationaler Datenschutz	140
Kapitel 5.	Bestimmung des anwendbaren Rechts	156

Teil II. Datenschutzorganisation

Kapitel 1.	Datenschutzmanagement und Datenschutzprozesse	167
Kapitel 2.	Betrieblicher Datenschutzbeauftragter	180
Kapitel 3.	Selbstkontrolle und Datenschutzaufsicht	205
Kapitel 4.	Compliance und Datenschutz	218
Kapitel 5.	Datenschutz und Zertifizierung	236

Teil III. Archivierung und Entsorgung

Kapitel 1.	Datenschutzkonzepte	257
Kapitel 2.	Technische und organisatorische Maßnahmen	303
Kapitel 3.	Archivierung und Protokollierung als Problem des betrieblichen Datenschutzes	320

Teil IV. Datenschutz und Personal

Kapitel 1.	Beschäftigtendatenschutz	331
Kapitel 2.	„Bring Your Own Device“ und Datenschutz	370
Kapitel 3.	Datenschutz und Mitbestimmung	385
Kapitel 4.	Sozialdatenschutz	398

Teil V. Datenschutz in Betrieb, Unternehmen und Konzern

Kapitel 1.	Konzerndatenschutz	453
Kapitel 2.	Internationaler Datenverkehr	475

Kapitel 3. Präventive Compliance und Whistleblowing im Konzern 492
Kapitel 4. Datenschutz in der Unternehmenstransaktion 524

Teil VI. Outsourcing und neue Technologien als Herausforderung für den Datenschutz

Kapitel 1. Outsourcing 547
Kapitel 2. Auftragsdatenverarbeitung 564
Kapitel 3. Customer Relationship Management und Datenschutz 601
Kapitel 4. Nachweispflicht für die Datenherkunft 619
Kapitel 5. Cloud Computing 627
Kapitel 6. Cyberwar und Datenschutz 679
Kapitel 7. Smart Metering und E-Mobility 703

Teil VII. Datenschutz in verschiedenen Kommunikationsformen

Kapitel 1. Datenschutz im Internet 731
Kapitel 2. Web 2.0, Mobile Apps und die datenschutzrechtlichen Anforderungen 747
Kapitel 3. Social Communities und deren datenschutzrechtliche Auswirkungen auf die Unternehmenspraxis 797
Kapitel 4. Datenschutz in der Telekommunikation 811
Kapitel 5. Pflichten zur Herausgabe von und zur Auskunftserteilung über Daten 847

Teil VIII. E-Commerce

Kapitel 1. Kundendatenschutz 869
Kapitel 2. Bonitätsbewertung 881
Kapitel 3. Opt-in/Opt-out 903
Kapitel 4. Datenweitergabe an Handelspartner und Offenlegungspflichten; Shophosting 926
Kapitel 5. Online-Zahlungsverkehr 967

Teil IX. Datenschutz im Gesundheitssektor

Kapitel 1. Umgang mit Patientendaten 991
Kapitel 2. Elektronische Patientenakte 1028
Kapitel 3. Telemonitoring 1042

Teil X. Information als Wirtschaftsgut

Kapitel 1. Adresshandel 1061
Kapitel 2. RFID, Smartcards und Cookies 1079
Kapitel 3. Werbung im Internet 1104
Kapitel 4. Bewertungsportale 1129
Kapitel 5. Datenschutzkonformer Einsatz von Suchmaschinen im Unternehmen 1137

Teil XI. Datensicherheit

Kapitel 1. Technische und organisatorische Maßnahmen 1155
Kapitel 2. Schutz von Betriebs- und Geschäftsgeheimnissen 1178

Teil XII. Konfliktmanagement im Datenschutz

Kapitel 1. Strategie und Taktik im Umgang mit Datenschutzverletzungen 1189
Kapitel 2. E-Discovery 1198
Kapitel 3. Haftungsrisiken und deren Versicherung 1224

Teil XIII. Straf- und Ordnungswidrigkeitenvorschriften im Bereich des betrieblichen Datenschutzes 1261

Sachverzeichnis 1297

Inhaltsverzeichnis

Seite

Vorwort ... V
Bearbeiterverzeichnis ... XLV
Abkürzungsverzeichnis ... XLIX

Teil I. Allgemeine datenschutzrechtliche Grundlagen und Strukturen

Kapitel 1. Vom Volkszählungsurteil zur Datenschutz-Grundverordnung

A. Entwicklung des Datenschutzes ... 4
I. BDSG ... 4
II. Weitere Kodifikationen und europäische Regelungen ... 6
1. Kompetenz ... 9
2. Errungenschaften ... 9
III. Recht auf informationelle Selbstbestimmung und dessen Weiterentwicklung ... 10

B. Zum Stand des Datenschutzrechts ... 13
I. Allgemeines ... 13
II. BDSG ... 13
1. Anwendung ... 13
2. Adressat ... 14
3. Begriffe, Definitionen ... 14
4. Verbotsprinzip ... 15
5. Aufgabe und Zweck des BDSG ... 15
III. DS-GVO ... 16

C. Modernisierungsbedarf ... 20
I. Modernisierungsbedarf aufgrund der Rechtsprechung ... 20
1. Innerer Bereich der Zurückgezogenheit ... 20
2. Zweckbindung ... 21
3. Recht auf informationelle Selbstbestimmung ... 21
II. Modernisierungsbedarf aufgrund der sonstigen Entwicklung ... 27
1. Ansätze, Materialien ... 27
2. EU: Digitale Agenda ... 28
3. USA-Impulse ... 28
4. Europarat ... 29
III. Unvollständiger Ansatz zum Beschäftigtendatenschutz (2009) ... 30
IV. Datenschutz-Grundverordnung ... 31
1. Grundbausteine ... 32
2. Neue Instrumente ... 32

Seite

3. Nicht eingelöste Vorgaben vom 4.11.2010 33
4. Kritik 34
V. Einzelne Aspekte der Defizite geltenden Rechts 35
1. Intransparenz 35
2. Technisch veraltet 35
3. Keine Berücksichtigung der Rechtsprechung(sentwicklung) 36
4. Zahnloses Gesetz, schwache Sanktion 37
5. BDSG keine Marktverhaltensregelung? 37
6. Nebeneinander der diversen Rechtsinstitute 38

D. Grundrecht auf Netzzugang 39

E. Informationsethik und Datenschutz 42

Kapitel 2. Die Europäische Dimension des Datenschutzes

A. Europarechtlicher Rahmen 50
I. Motivation 50
II. Gegenwärtiger Rechtszustand 51
1. Richtlinien 51
2. Sonstiges Sekundärrecht 51
3. Primärrecht 52
4. Weitere Normen und „Softlaw" 56
III. Sekundärrechtlich determinierte europäische datenschutzrechtliche Grundsätze 57
1. Anwendbarkeit nur bei Personenbezug und nur bei natürlichen Personen 57
2. Verarbeitung nach Treu und Glauben (Art. 6 Abs. 1a DSRL) 57
3. Zweckbindungsgrundsatz (Art. 6 Abs. 1a und 1b DSRL) 57
4. Richtigkeit (Art. 6 Abs. 1d DSRL) 58
5. Datenvermeidung und Datensparsamkeit (Art. 6 Abs. 1c und 1e DSRL) 58
6. Unterscheidung sensible/nicht sensible Daten (Art. 7 und 8 DSRL) 58
7. Verbot mit Erlaubnisvorbehalt 58
8. Betroffenenrechte 59
9. Unabhängige Vorabkontrolle 59
IV. Aktuelle Entwicklungen de lege ferenda – Datenschutz-Grundverordnung (DS-GVO) 59
1. Genese 59
2. Ziele 60

B. Judikatur 62
I. Lindqvist (C-101/01) 62
II. Österreichischer Rundfunk (C-465/00, C-138/01, C-139/01) 63
III. Vorratsdatenspeicherung (C-201/06) 63
IV. Markkinapörssi (C-73/07) 63

Seite

V. Datenschutzbeauftragter I (C-518/07) ... 63
VI. Rijkeboer (C-553/07) ... 63
VII. Datenschutzbeauftragter II (C-614/10) ... 64
VIII. Bavarian Lager (C-28/08 P) ... 64
IX. Agrarbeihilfen (C-92/09, 93/09) ... 64
X. ASNEF (C-468/10, C-469/10) ... 64
XI. Promusicae (C-275/06) ... 64
XII. Scarlet (C-70/10) ... 64
XIII. Vorratsdatenspeicherung II (C-293/12, C-594/12, C-46/13) ... 64
XIV. Google Spain (C-131/12) ... 65
XV. Ungarische Datenschutzbehörde – Jóri (C-288/12) ... 65
XVI. Safe Harbor (C-362/14) ... 65
XVII. Dynamische Internetadressen (C-582/14) ... 65

C. Internationale Vorgaben ... 66

D. Internationaler Datentransfer ... 67
I. Rechtslage nach DSRL ... 67
1. Datenverarbeitung durch eine inländische verantwortliche Stelle ... 67
2. Datenverarbeitung durch eine ausländische Stelle mit Sitz im EU-Ausland ... 67
3. Datenverarbeitung durch eine ausländische Stelle mit Sitz in einem Drittstaat ... 67
4. Übermittlung in einen Drittstaat ... 67
II. Rechtslage nach der DS-GVO ... 68

Kapitel 3. Anwendbares Datenschutzrecht und Zuständigkeit der Aufsichtsbehörden

A. Einführung ... 74
I. Die Struktur der kollisionsrechtlichen Prüfung ... 74
II. Rechtsgrundlagen ... 75
III. Gang der Darstellung ... 76

B. Das anwendbare Datenschutzrecht nach dem BDSG ... 76
I. Die maßgebliche Kollisionsnorm ... 76
1. Die gesetzliche Regelung des anwendbaren Datenschutzrechts ... 76
2. Die aktuelle EuGH-Rechtsprechung zum Datenschutzkollisionsrecht ... 78
II. Die Anknüpfung an Sitz und Niederlassung der verantwortlichen Stelle 84
1. Begriff und Belegenheit der verantwortlichen Stelle ... 84
2. Kollisionsrechtliche Gleichstellung von Tochtergesellschaft und Zweigniederlassung ... 86
3. Niederlassungen als verantwortliche Stelle ... 86
4. Begriff und Belegenheit der Niederlassung ... 87

Seite

5. Die Zuordnung der Datenverarbeitung zu einer Niederlassung 91
6. Ergebnis: Der datenschutzrechtliche Niederlassungsbegriff 97
7. Anwendbares Datenschutzrecht in der internationalen Unternehmensgruppe 98
8. Kollisionsrechtliche Abspaltung der Anforderungen an die technische Sicherheit 101
9. Einzelfälle zur Niederlassung 102
10. Niederlassungen in Drittstaaten 104

III. Die Anknüpfung an den Ort der Datenverarbeitung 106
1. Ort der Datenverarbeitung und anwendbares Datenschutzrecht 106
2. Belegenheit von Rechnern im Inland 107
3. Datenverarbeitung über Websites 108
4. Ferngesteuerte Datenverarbeitung auf dem Rechner des Internetnutzers 109
5. Erhebung von Daten im Inland bei grenzüberschreitender Kommunikation 111
6. Nichtanwendung des BDSG auf Datentransit 111

IV. Das anwendbare Datenschutzrecht bei der Auftragsdatenverarbeitung ... 112
1. Die akzessorische Anknüpfung der Auftragsdatenverarbeitung 112
2. Das für die technischen und organisatorischen Maßnahmen maßgebliche Recht 113

V. Umfang des Datenschutzstatuts und Statutenwechsel 114

C. Räumlicher Anwendungsbereich der Datenschutz-Grundverordnung 115

I. Die Kollisionsnormen der Datenschutz-Grundverordnung 115

II. Die Anknüpfung an die Niederlassung (Art. 3 Abs. 1 DS-GVO) 116
1. Der Begriff der Niederlassung 116
2. Die Zuordnung der Datenverarbeitung zur Niederlassung 117

III. Die Anknüpfung an die Verarbeitung von Daten Betroffener in der Union (Art. 3 Abs. 2 DS-GVO) 117
1. Das Marktortprinzip 117
2. Daten Betroffener in der Union 118
3. Anbieten von Waren oder Dienstleistungen 118
4. Datenverarbeitung zum Zweck der Beobachtung 121

D. Die internationale Zuständigkeit der Aufsichtsbehörden 123

I. Einführung 123

II. Die Zuständigkeitsregelung des Art. 55 DS-GVO 124
1. Die Grundlagen der Zuständigkeit 124
2. Die Anknüpfung an die Niederlassung 125
3. Auswirkungen auf Betroffene und weitere Zuständigkeitsgründe ... 125
4. Internationale Zuständigkeit aufgrund mitgliedstaatlichen Rechts .. 126

III. Zuständigkeit bei grenzüberschreitender Datenverarbeitung 126
1. Das Konzept der federführenden Zuständigkeit 126
2. Der Anwendungsbereich der Regeln zur federführenden Aufsichtsbehörde 128

Seite

IV. Die Kooperation der Aufsichtsbehörden ... 131
1. Der Begriff der Hauptniederlassung ... 131
2. Die Modifikation der Zuständigkeit (Art. 56 Abs. 2–5 DS-GVO) ... 134
3. Die Zusammenarbeit der Aufsichtsbehörden ... 136
V. Zuständigkeit der Aufsichtsbehörden in Fallgruppen ... 137
1. Unternehmen mit (Haupt-)Niederlassung in Deutschland ... 137
2. Unternehmen mit (Haupt-)Niederlassung in anderen EU-Staaten ... 138
3. Unternehmen mit (Haupt-)Niederlassung im Drittstaat ... 139

Kapitel 4. Internationaler Datenschutz

A. Einführung ... 141

B. Nordamerika ... 142
I. USA ... 142
II. Einige Konsequenzen ... 146
III. Kanada ... 147

C. Asien ... 148
I. Indien ... 149
II. Volksrepublik China/Hongkong ... 150
III. Japan/Südkorea ... 151

D. Südamerika ... 152

E. Australien/Neuseeland ... 153

Kapitel 5. Bestimmung des anwendbaren Rechts

A. Datenschutzrechtlicher Regelungszweck und Normadressaten ... 156
I. Verfassungsrechtliches Differenzierungsgebot ... 158
1. Grundrechtliche Konkordanz ... 158
2. Normadressaten ... 159
II. Sachzusammenhang und Regelungskompetenz ... 160
1. Sachzusammenhang ... 160
2. Regelungskompetenz ... 160

B. Öffentliche und nicht öffentliche Stellen als Normadressaten ... 161
I. Begriff der öffentlichen und nicht öffentlichen Stelle ... 161
1. Abgrenzungsfragen ... 161
2. Öffentliche Unternehmen ... 162
3. Religionsgemeinschaften ... 163
4. Nicht öffentliche Stellen ... 163
II. Auswirkungen auf die datenschutzrechtliche Regelungssystematik ... 164

C. Subsidiaritätsprinzip im Datenschutz ... 164
I. BDSG als Auffangregelung ... 164

Seite

II. Bereichsspezifische Vorschriften ... 165
1. Öffentlicher Bereich ... 165
2. Nicht öffentlicher Bereich ... 165

Teil II. Datenschutzorganisation

Kapitel 1. Datenschutzmanagement und Datenschutzprozesse

A. Allgemeines ... 167

B. Die Rechenschaftspflicht in der DS-GVO ... 168

C. Auswahl des Datenschutzbeauftragten: intern oder extern? ... 168

D. Datenschutzaudit und Bewertung des Datenschutzrisikos ... 170
I. Erfassung aller datenschutzrelevanten Prozesse ... 171
II. Rechtliche Bewertung und Risikoanalyse ... 172
III. Datenschutz-Folgenabschätzung in der DS-GVO ... 172

E. Verfahrensverzeichnisse ... 173
I. Öffentliches Verfahrensverzeichnis ... 173
II. Interne Verfahrensübersichten ... 174

F. Implementierung von Datenschutzprozessen ... 176
I. Prozess: Einbindung des Datenschutzbeauftragten bei neuen Verfahren 177
II. Prozess: Datenschutzrechtliche Prüfung ... 178
III. Prozess: Schulungen und Verpflichtung auf das Datengeheimnis ... 178
IV. Weitere Prozesse ... 179

Kapitel 2. Betrieblicher Datenschutzbeauftragter

A. Bestellung des betrieblichen Datenschutzbeauftragten ... 181
I. Bestellungspflicht ... 181
1. Allgemeines ... 181
2. Voraussetzungen ... 182
3. Bestellungspflicht in der DS-GVO ... 183
II. Ordnungsgemäße Bestellung durch Bestellungsurkunde ... 184
1. Schriftlicher Vertrag ... 184
2. Zeitpunkt der Bestellung ... 184
3. Inhaltliche Gestaltung ... 185
4. Anzeigepflicht in der DS-GVO ... 185
5. Bestellung eines externen Datenschutzbeauftragten ... 185
6. Bestellung zum Konzerndatenschutzbeauftragten ... 186
7. Befristung der Bestellung ... 186
8. Mitbestimmung des Betriebsrats ... 187
III. Abberufung eines Datenschutzbeauftragten ... 187
1. Wichtiger Grund für die Abberufung ... 188
2. Arbeitsrechtliche Anforderungen an die Abberufung ... 188

Seite

3. Sonderfall: Fusionen und Übernahmen (M&A) ... 189
4. Abberufung eines externen Datenschutzbeauftragten ... 190
5. Abberufung auf Verlangen der Aufsichtsbehörde ... 190

IV. Sanktionen ... 190

B. Anforderungen an den betrieblichen Datenschutzbeauftragten ... 191

I. Erforderliche Fachkunde ... 191
1. Allgemeines ... 191
2. Juristische Kenntnisse ... 192
3. IT-Kenntnisse ... 194
4. Sonstige Fähigkeiten ... 194

II. Erforderliche Zuverlässigkeit ... 194
1. Allgemeines ... 194
2. Subjektive Kriterien ... 195
3. Objektive Kriterien/Interessenkollisionen ... 195

C. Die rechtliche Stellung des Datenschutzbeauftragten im Unternehmen ... 198

I. Weisungsfreiheit ... 198
II. Anbindung an die Unternehmensleitung ... 199
III. Benachteiligungsverbot ... 200
IV. Unterstützungspflicht ... 200
V. Besonderer Kündigungsschutz ... 200

D. Aufgaben und Pflichten des betrieblichen Datenschutzbeauftragten ... 201

I. Hinwirken ... 201
II. Unterstützung durch die Aufsichtsbehörde ... 201
III. Einzelne Aufgaben ... 202
IV. Verschwiegenheitspflicht ... 203

E. Haftung des betrieblichen Datenschutzbeauftragten ... 203

Kapitel 3. Selbstkontrolle und Datenschutzaufsicht

A. Allgemeines, Aufgaben ... 205

B. Verhältnis der beiden Einrichtungen zueinander ... 208

I. Unterstützung des Beauftragten ... 208
II. Befugnis der Aufsichtsbehörde zu Anordnungen ... 209
III. Abberufung ... 210
IV. Betretungsrechte ... 210

C. Weitere Formen der Selbstkontrolle und der Fremdkontrolle ... 211

I Audit ... 211
II. DS-GVO ... 212

D. Grundsätze, Instrumente ... 213

E. Der Betriebsrat als datenschutzrechtliche „Kontrollinstanz“ ... 216

Seite

Kapitel 4. Compliance und Datenschutz

A. Einführung 219

B. Der Begriff Compliance 221
I. Verwendung in Normen 221
II. Definition Compliance und Abgrenzung zu Governance 223

C. Compliance und Datenschutz 224
I. Rechtsgrundlagen 226
II. Verantwortlichkeit 228
1. Meldung – Verfahrensverzeichnis 229
2. Vorabkontrolle 230
3. Betrieblicher Datenschutzbeauftragter 230
4. Auftragsdatenverarbeitung 231

D. Datenschutz bei Governance 233

E. Folgen fehlender Beachtung datenschutzrechtlicher Regelungen 233

Kapitel 5. Datenschutz und Zertifizierung

A. Einführung 237

B. Selbstregulierung 239

C. Datenschutzaudit im BDSG 241

D. Besonderheiten bei Cloud Computing 244

E. Verhaltensregeln, Branchenregeln 245

F. Safe Harbor – eine Art Test, Privacy Shield 248

G. Zertifizierung und Verhaltensregeln gemäß DS-GVO 251
I. Zertifizierung 251
II. Verhaltensregeln 254

Teil III. Archivierung und Entsorgung

Kapitel 1. Datenschutzkonzepte

A. Speicherpraxis zwischen Aufbewahrungs- und Löschpflicht 261
I. Fortschreitende Digitalisierung, billiger Speicherplatz und Auslagerung als Herausforderungen an die betriebliche Gedächtnisorganisation 261
II. Begriffe: Aufbewahrung, Archivierung, Speicherung, Ablage, Löschung, Vernichtung, Entsorgung 262
III. Schwierigkeiten der Phasenabgrenzung 266
IV. Praxis der Datenschutzbehörden 267
V. Rechtsprechungspraxis 277

Seite

B. Archivierung ... 279
I. Bedeutung: Revisions- und IT-Sicherheit, IT-Compliance, E-Discovery, Beweisqualität von E-Mails ... 279
II. Rechtsgrundlagen ... 280
1. Datenschutzrechtliche Speicherbefugnis ... 280
2. Handels- und steuerrechtliche Anforderungen, GoB, GOBD ... 283
3. Papierloses Büro, ersetzendes Scannen ... 290
4. Betriebliche Mitbestimmung ... 293

C. Entsorgung ... 294
I. Bedeutung ... 294
II. Gesetzliche Anforderungen an Löschung und Entsorgung von personenbezogenen Daten ... 295
1. Begriff des Löschens ... 295
2. Differenzierung nach Art des Datenträgers ... 296
3. Datenschutzrechtlicher Löschanspruch ... 297

Kapitel 2. Technische und organisatorische Maßnahmen

A. Archivierung ... 303
I. Zentrale/dezentrale Archivierung ... 303
II. Langzeitarchivierung ... 305
1. Archivierung von Arbeitsprozessdaten ... 305
2. Archivierung digitaler Signaturen ... 306
III. Dokumentenmanagementsysteme ... 307
IV. Externe Archivierung ... 308

B. Entsorgung ... 309
I. Technische Löschverfahren ... 309
1. Löschen durch Überschreiben ... 309
2. Magnetische Durchflutung und thermische Zerstörung ... 310
3. Mechanische Zerstörung ... 311
4. Unterstützung durch DIN 66399 ... 313
II. Datenschutzgerechte Entsorgungskonzepte ... 313
1. Technische und organisatorische Maßnahmen nach BDSG ... 313
2. Datenschutzkonformes Löschkonzept nach DIN 66398:2016-05 ... 314
III. Entsorgung durch Dienstleister ... 318

Kapitel 3. Archivierung und Protokollierung als Problem des betrieblichen Datenschutzes

A. Konflikt zwischen IT-Sicherheit/Revisionssicherheit und Datenschutz ... 320
I. Erlaubte Privatnutzung ... 321
II. Rückgabe von Firmengeräten/Ausscheidensregelung ... 323

B. Urheberrechtliche Zulässigkeit der Archivierung ... 324

Seite

C. Umgang mit Datenbeständen, insbesondere mit Altbeständen 325
I. Cloud-Storage und Dokumentenmanagementsysteme in der Cloud 325
II. Big Data – Datenbanken, Datenportabilität und Doublettenvermeidung 328

Teil IV. Datenschutz und Personal

Kapitel 1. Beschäftigtendatenschutz

A. Einleitung 333

B. Beschäftigtendatenschutz unter der DS-GVO 334
I. Regelungsspielraum nach Art. 88 Abs. 1 337
1. Bestimmung des mitgliedstaatlichen Regelungsspielraums 337
2. Abgrenzung der Spezifizierung zur Auslegung und zu Beschränkungen, Abweichungen und Ausnahmen 341
II. Regelungsspielräume nach Art. 6 Abs. 2 und Abs. 3 DS-GVO 342
1. Datenverarbeitung zur Erfüllung einer gesetzlichen Verpflichtung .. 343
2. Bestimmung des mitgliedstaatlichen Regelungsspielraums nach Art. 6 Abs. 2 DS-GVO 345
3. Bestimmung des mitgliedstaatlichen Regelungsspielraums nach Art. 6 Abs. 3 UAbs. 2 DS-GVO 348
III. Konkurrenzen 349

C. Kodifikation des Beschäftigtendatenschutzes 350

D. Datenschutzbezogene Betriebsvereinbarungen 354
I. Datenschutzbezogene Betriebsvereinbarungen de lege lata 354
II. Datenschutzbezogene Betriebsvereinbarungen de lege ferenda 356

E. Fragerecht des Arbeitgebers 357
I. Fragerecht des Arbeitgebers de lege lata 357
1. Arbeitsrecht 358
2. Datenschutzrecht 358
II. Fragerecht des Arbeitgebers de lege ferenda 362

F. Datenabgleich zu Compliance-Zwecken 363
I. Datenabgleich de lege lata 365
1. Präventive Kontrollen; Verhinderung statt Aufdeckung 366
2. Aufdeckung von Ordnungswidrigkeiten und Vertragsverletzungen ... 367
II. Datenabgleich de lege ferenda 367

G. Videoüberwachung am Arbeitsplatz 367
I. Videoüberwachung de lege lata 367
1. Videoüberwachung von Arbeitsplätzen in öffentlich zugänglichen Bereichen 367

Seite

2. Videoüberwachung von Arbeitsplätzen in öffentlich nicht zugänglichen Betriebsbereichen ... 368
3. Videoüberwachung im öffentlichen Raum außerhalb des Arbeitsplatzes ... 369

II. Videoüberwachung de lege ferenda ... 369

Kapitel 2. „Bring Your Own Device" und Datenschutz

A. Einleitung ... 371

B. BYOD und die rechtlichen Implikationen ... 372

I. Erscheinungsformen des BYOD ... 372
1. Nutzung privater IT zu dienstlichen Zwecken ... 372
2. Unechtes BYOD ... 373

II. BYOD im rechtlichen Kontext ... 374
1. Gewerbliche Schutzrechte ... 374
2. Arbeitsrecht ... 374
3. Handels- und steuerrechtliche Dokumentations- und Aufbewahrungspflichten ... 375
4. Datenschutz ... 375

III. BYOD und Datenschutz ... 376
1. Anwendbarkeit datenschutzrechtlicher Vorschriften ... 376
2. Kontrollrechte und -pflichten ... 378
3. Einführung des BYOD im Unternehmen ... 382
4. Skandalisierungspflicht ... 383

C. Zusammenfassung ... 384

Kapitel 3. Datenschutz und Mitbestimmung

A. Einleitung ... 387

B. Datenschutz und Mitbestimmung ... 388

I. Der Schutz des allgemeinen Persönlichkeitsrechts als mitbestimmungsrechtliche Aufgabe ... 388
1. Datenschutzrechtliche Anknüpfungspunkte ... 388
2. Mitbestimmungsrechtliche Tatbestände ... 389

II. § 87 Abs. 1 Nr. 6 BetrVG als tatbestandliche Grundlage für die mitbestimmungsrechtliche Verankerung des Datenschutzes ... 392

III. Datenschutz innerhalb der Arbeitnehmervertretung ... 393

IV. Verhältnis des Arbeitnehmerdatenschutzes nach dem BetrVG zum BDSG ... 395
1. Anwendbarkeit des BDSG – Subsidiaritätsgrundsatz ... 395
2. Möglichkeit der Verschlechterung ... 395

V. Betrieblicher Datenschutzbeauftragter und das Verhältnis zur Mitbestimmung ... 396

VI. Typische Regelungsmaterien für datenschutzrechtliche Betriebsvereinbarungen ... 397

Seite

Kapitel 4. Sozialdatenschutz

A. Bedeutung des Sozialdatenschutzes für Arbeitnehmer 401

B. Das System des Sozialdatenschutzes 401
I. Rechtsgrundlagen 401
1. Nationales Verfassungsrecht 401
2. EU-Rechtsrahmen 403
3. Einfachgesetzliche Grundlagen 405
II. Sozialgeheimnis 406
III. Begriff der Sozialdaten 406
1. Allgemeines 406
2. In § 35 SGB I genannte Stellen 406
3. Zweckbindung 407
4. Betriebs- und Geschäftsgeheimnisse 408
5. Anonymisierte und pseudonymisierte Daten 408
6. Gutachten als Sozialdaten 410
IV. Verlängerter Sozialdatenschutz 410
V. Technische Vorkehrungen 411

C. Erheben von Daten 413
I. Begriff des Erhebens 413
II. Erhebung auf Grundlage einer Einwilligung 414
III. Erforderlichkeit der Erhebung 417
1. Allgemeines 417
2. Gebot der Transparenz und der Direkterhebung 417
3. Erhebung auf Vorrat 422
4. Die Erhebung spezifischer Daten 423
5. Unzulässige Erhebungsmethoden 425

D. Auswirkungen auf Mitwirkungspflichten 426

E. Die Nutzung und Verarbeitung von Daten 427
I. Speichern, Verändern, Nutzen von Daten 427
II. Übermitteln von Daten 428
1. Abgrenzung Übermittlung/Nutzung 428
2. Voraussetzungen einer Übermittlungsbefugnis 428
3. Verhältnismäßigkeit der Übermittlung 431
4. Aktenübersendung an Sozialgerichte 432
5. Übermittlungsbefugnis durch Einwilligung? 432
6. Übermittlung ohne Einwilligung oder normative Befugnis 433
7. Verantwortung für die Übermittlung 434
8. Übermittlungen ohne Ersuchen 434

F. Erhebung, Verarbeitung und Nutzung von Sozialdaten im Auftrag 436

G. Der Anspruch auf Berichtigung, Löschung und Sperrung gemäß § 84 SGB X 439

Seite

H. Auskunftsanspruch ... 441

I. Der Datenschutzbeauftragte ... 443

J. Sanktionsnormen ... 444

K. Schadensersatz ... 445
I. Allgemeines ... 445
II. Haftung nach § 82 S. 1 SGB X ... 446
III. Haftung nach § 82 S. 2 SGB X ... 446

L. Datenschutz im sozialgerichtlichen Verfahren ... 448
I. Geltung des Datenschutzes auch im Gerichtsverfahren ... 448
II. Die in Betracht kommenden Datenschutznormen ... 449
III. Datenschutz innerhalb desselben Gerichts ... 449
IV. Übermittlung von Daten außerhalb des Sozialgerichtsprozesses ... 450
V. Konsequenzen von Verstößen gegen das Recht auf informationelle Selbstbestimmung ... 451

Teil V. Datenschutz in Betrieb, Unternehmen und Konzern

Kapitel 1. Konzerndatenschutz

A. Einleitung ... 455

B. Grundlagen des Konzerndatenschutzes ... 455
I. Fehlendes Konzernprivileg ... 455
II. Datenübermittlungsverbot mit Erlaubnisvorbehalt ... 458
III. Der Konzern als Subjekt der Datenschutzaufsicht ... 458

C. Datenschutzkonforme Ausgestaltung von Datenweitergaben im Konzern ... 459
I. Auftragsdatenverarbeitung ... 459
II. Datenübermittlungen im Rahmen von Funktionsübertragungen ... 460
1. Übermittlung von Beschäftigtendaten im „konzerndimensionalen Arbeitsverhältnis“ ... 461
2. Übermittlung von Beschäftigtendaten im Rahmen von Funktionsübertragungen ... 463
3. Übermittlung besonderer Arten personenbezogener Daten ... 464
III. Datenübermittlungen auf Basis von Betriebsvereinbarungen ... 465
IV. Datenübermittlungen auf Basis von Einwilligungen ... 465

D. Datenweitergaben bei Umstrukturierungen und Umwandlungen ... 466
I. Betriebsübergang ... 466
II. Due Diligence-Prüfungen ... 467
III. Umwandlungen (Verschmelzung, Abspaltung etc.) ... 467

Seite

E. Fallgruppen praxisrelevanter Datenübermittlungen und -verarbeitungen im Konzern ... 467
I. Organisationsbezogene Datenübermittlungen ... 468
1. Konzernweites Kommunikationsverzeichnis ... 468
2. Matrix-Strukturen ... 468
3. Aufteilung von Produktions- und Arbeitsprozessen ... 469
4. Zentralisierung von Compliance-Funktionen ... 469
II. Zentralisierung von Human Resources-Aufgaben ... 470
1. Lohn- und Gehaltsabrechnung ... 470
2. Zentrale Personalverwaltung ... 470
3. Konzernübergreifende Skill-Datenbanken ... 472
III. Sonstige Shared Services ... 472
1. IT-Leistungen ... 472
2. Werbe- und Marketingleistungen ... 473
3. Übermittlung von Kundendaten ... 473

F. Internationale Datentransfers ... 474

Kapitel 2. Internationaler Datenverkehr

A. EU-Datenschutz für den Datentransfer ins Ausland ... 476

B. Datenschutz im Geschäftsverkehr mit den Vereinigten Staaten/außerhalb der EU ... 478
I. EU-US Privacy Shield ... 479
II. Standardvertragsklauseln ... 483
III. Binding Corporate Rules (BCR) ... 485

C. Outsourcing ... 486

D. Vertragsgestaltung im internationalen Datenverkehr ... 488

Kapitel 3. Präventive Compliance und Whistleblowing im Konzern

A. Einleitung ... 494

B. Allgemeine Vorgaben für eine Compliance-Organisation ... 495

C. Elektronische Systeme zur präventiven Compliance ... 496
I. Verpflichtung zur Vorhaltung von Systemen und Daten? ... 497
1. Allgemeine Compliance-Vorgaben ... 497
2. Vorgaben für Banken, Versicherungen und Wertpapierdienstleistungsunternehmen ... 497
II. Allgemeine Vorgaben zum Zugriff auf Daten bei Datenabgleichen ... 498
1. Vorgaben des BDSG zur präventiven Compliance ... 499
2. Datenabgleiche beschränkende Sondernormen ... 501
3. Mitbestimmungsrecht des Betriebsrats ... 503

Seite

4. Pflicht zur Information des betrieblichen Datenschutzbeauftragten 503
5. Pflicht zur Information des/der betroffenen Arbeitnehmer(s) 504
6. Sanktionen bei Verletzung des Datenschutzrechts 504

III. Empfehlungen für die Praxis 505
1. Begrenzungen des automatisierten Datenabgleichs 505
2. Trennung von dienstlichen und privaten E-Mails 506
3. Abschluss von Betriebsvereinbarungen 508

D. Whistleblowing-Systeme 509
I. Einleitung 509
II. Aufbau eines Whistleblowing-Systems 509
III. Inhaltlicher Anwendungsbereich 510
IV. Datenschutzrechtliche Vorgaben 511
1. Einwilligung 511
2. Grundsätzliche Anforderungen an Aufnahme und Verarbeitung von Hinweisen 512
3. Anonymität des Hinweisgebers 513
4. Einbindung eines externen Ombudsmanns 514
5. Übermittlung an andere Konzerngesellschaften 515
6. Sonstige datenschutzrechtliche Anforderungen 515
7. Einbindung des Datenschutzbeauftragten 516
8. Einbindung des Betriebsrats und Betriebsvereinbarung 516
V. Empfehlungen für die Praxis 517

E. System zur Security Breach Notification nach § 42a BDSG 517

F. Stellung des Datenschutzbeauftragten im Verhältnis zum Compliance-Beauftragten 518
I. Einleitung 518
II. Rechtliche Anforderungen an Aufgabe und Stellung des Datenschutzbeauftragten 519
III. Rechtliche Anforderungen an Aufgabe und Stellung des Compliance-Beauftragten 520
IV. Bewertung 522

Kapitel 4. Datenschutz in der Unternehmenstransaktion

A. Einleitung 525

B. Datenschutzrechtlicher Rahmen für die Übermittlung von personenbezogenen Daten an Interessenten und deren Berater 527
I. Beschäftigtendaten 527
1. Einwilligung 527
2. Betriebsvereinbarungen 529
3. Zulässigkeit nach §§ 28, 32 BDSG 530
II. Kunden- und Lieferantendaten 531

Seite

III. Besondere personenbezogene Daten ... 532
IV. Durch Sondernormen geschützte Daten ... 533
V. Sanktionen bei Verletzung des Datenschutzrechts ... 533

C. Übermittlung von personenbezogenen Daten im Rahmen der Due Diligence und Verhandlungen ... 533
I. Grundsätze der Zulässigkeitsprüfung ... 534
II. Daten der Vorstände bzw. Geschäftsführer ... 535
III. Beschäftigtendaten ... 535
IV. Kunden- und Lieferantendaten ... 536

D. Übermittlung von personenbezogenen Daten in der Phase zwischen Signing und Closing ... 537

E. Übermittlungen von personenbezogenen Daten nach dem Closing ... 538
I. Share Deal ... 538
II. Asset Deal ... 538
III. Unternehmenserwerb durch Verschmelzung oder Abspaltung ... 541

F. Vorbereitung der Unternehmenstransaktion ... 542
I. Vorbereitung von Listen ... 542
II. Abschluss von Vertraulichkeitsvereinbarungen ... 543
1. Allgemeines ... 543
2. Drittlandtransfer ... 543
III. Abschluss eines Auftragsdatenverarbeitungsvertrags mit Datenraumanbietern ... 544
IV. Einbindung des betrieblichen Datenschutzbeauftragten ... 544
V. Einbindung des Betriebsrats ... 545
VI. Benachrichtigung der Betroffenen ... 546

Teil VI. Outsourcing und neue Technologien als Herausforderung für den Datenschutz

Kapitel 1. Outsourcing

A. Ausschreibung und Vergabe von Aufträgen ... 548
I. Begriff ... 548
II. Formen ... 549
III. Verhandlung, Auftragserteilung, Vergabe ... 551
IV. Cloud-Besonderheiten ... 552
V. Big Data ... 555

B. SLA-Gestaltung im Hinblick auf den Datenschutz ... 557

C. Transition und Betriebsübergang, Retransition ... 561

Seite

Kapitel 2. Auftragsdatenverarbeitung

A. Auftragsdatenverarbeitung in der EU gemäß BDSG und EG-DSRL 566
I. Privilegierung nach § 11 i. V. m. § 3 Abs. 8 BDSG 566
II. „Funktionsübertragung" 569
III. Voraussetzungen, Maßgaben, Durchführung 570
1. Vertragsvorgaben BDSG 2009 570
2. Maßgaben 571
3. Vertrag 571
4. Zehn Punkte 572
5. Vertragsformulierung 572
6. Aufgaben und Formen 573
IV. Ausführungen zu den zehn Vertragspunkten im Einzelnen 576
1. Gegenstand und Dauer 576
2. Umfang, Art und Zweck 577
3. Technische und organisatorische Maßnahmen 578
4. Berichtigung, Löschung und Sperrung 578
5. Nach Abs. 4 bestehende Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen 578
6. Berechtigung zur Begründung von Unterauftragsverhältnissen 579
7. Kontrollrechte des Auftraggebers 579
8. Mitzuteilende Verstöße 579
9. Umfang der Weisungsbefugnisse 580
10. Rückgabe überlassener Datenträger 580
V. Auswahl, Kontrolle 581
VI. Entsprechende Geltung von § 11 Abs. 1–4 BDSG 583
VII. Beauftragter für den Datenschutz 586

B. Auftragsverarbeitung gemäß DS-GVO 587
I. Definition, Auswahl 587
II. Maßgaben, Pflichten bei Auftragsverarbeitung 587
III. Vertrag, Vertragsgestaltung, Subunternehmer 588
IV. Datenschutzbeauftragter, Aufsicht 590
V. Datenschutz-Folgenabschätzung 591
VI. Haftung, Bußgeld, Entlastung 591
VII. Abgrenzung zu Joint Controllership 592

C. Internationale Auftragsdatenverarbeitung 592
I. EU-Standardvertragsklauseln 593
II. BCR 594
III. Safe Harbor, Privacy Shield (Adäquanz-Entscheidung) 596

D. Spezialprobleme bei Cloud Computing 597

Seite

Kapitel 3. Customer Relationship Management und Datenschutz

A. Customer Relationship Management – Pflege und Profilbildung als betriebswirtschaftliches Instrument ... 602

B. CRM und Datenschutz ... 603
I. Grundsatz ... 603
II. Gegenstand des CRM – personenbezogene Daten ... 604
III. Erfordernis der Einwilligung ... 605
IV. Hinweispflicht ... 608
V. Gesetzlicher Erlaubnistatbestand ... 608
1. Eigene geschäftliche Zwecke ... 609
2. Wahrung berechtigter Interessen der verantwortlichen Stelle ... 610
3. Allgemein zugängliche Daten ... 612
VI. Verarbeitung oder Nutzung zu Werbezwecken ... 613
1. CRM als Kundenbindungs- und Akquisemittel ... 613
2. Listenprivileg ... 613
3. Besondere Zweckbindung ... 614
VII. Datenpflege und -veredelung ... 614
1. Hinzuspeichern ... 614
2. Besondere Anforderungen an den Datenbestand infolge erweiterter Auskunftspflichten ... 615

C. CRM im Konzern ... 616
I. Konzernbegriff und fehlendes Konzernprivileg ... 616
II. Datenarten und Datenherkunft bei Übermittlungen im Konzern ... 617
III. Zusammenfassung ... 618

Kapitel 4. Nachweispflicht für die Datenherkunft

A. Herkunftsnachweis im Zusammenhang mit Auskunftsansprüchen ... 619
I. Sinn und Zweck der Regelung ... 620
1. Herkunft der personenbezogenen Daten ... 620
2. Speicherverpflichtung aus § 34 Abs. 1 BDSG ... 620
II. Sonderregelung bei geschäftsmäßiger Übermittlung (§ 34 Abs. 1 S. 3, 4 BDSG) ... 621
1. Auskunfts- und Speicherpflicht ... 621
2. Sonderregelung (§ 34 Abs. 1 S. 4 BDSG) ... 621

B. Herkunftsnachweis nach § 34 Abs. 1 lit. a BDSG ... 622
I. Inhalt der Regelung ... 622
II. Problematik der Regelung – die Rijkeboer-Entscheidung des EuGH ... 623

C. Herkunftsnachweis gemäß § 9 BDSG ... 624

D. Änderungen durch die DS-GVO ... 625
I. Allgemeines ... 625

Seite

II. Herkunftsnachweise nach Art. 14 Abs. 2 lit. f DS-GVO 625
III. Herkunftsnachweis im Zusammenhang mit Auskunftsverlangen 625
IV. Organisationskontrolle 625

E. Fazit 626

Kapitel 5. Cloud Computing

A. Cloud Computing und Datenschutz 630
I. Einführung, Definition, technische Hintergründe 630
1. Definition und Abgrenzung 630
2. Basis des Cloud Computing: Virtualisierung 631
3. Cloud-Modelle 632
4. Cloud Service-Typen 633
5. Aspekte der Datensicherheit 634
II. Cloud Computing und Datenschutz 636
1. Anwendbares Datenschutzrecht 636
2. Verlagerung von personenbezogenen Daten in die Cloud 637
3. Übermittlung der Daten ins Ausland 639
4. Auswirkungen der DS-GVO auf das Cloud Computing 639
III. Lösungsansätze 640
1. Verschlüsselung von personenbezogenen Daten in der Cloud 640
2. Nutzung von Trusted Computing-Technologien 642
3. Nutzung von Private Clouds 643
IV. Fazit 643

B. Transnationale Clouds 644
I. Die transnationale Dimension des Cloud Computing 646
II. Anwendbares Datenschutzrecht bei transnationalen Clouds 647
1. Anwendbarkeit des BDSG auf Cloud Provider mit Niederlassung im Inland 649
2. In einem anderen EU-Mitgliedstaat belegener Cloud Provider 650
3. In einem Drittland belegener Cloud Provider 651
III. Auftragsdatenverarbeitung unter Beteiligung von Cloud Providern in Drittländern 653
1. Cloud Provider als Auftragnehmer in einem Drittland 653
2. Cloud Provider als Auftraggeber in einem Drittland 654
IV. Weitergabe personenbezogener Daten an Cloud Provider im Ausland .. 654
1. Voraussetzungen 654
2. Angemessenes Datenschutzniveau im Empfängerland 654
3. Kein angemessenes Datenschutzniveau im Empfängerland 655
4. Zulässigkeit der Übermittlung 662

C. Entnetzung 663
I. Grundsätzliche Erwägungen 663
1. Zunehmendes Bedrohungspotenzial durch die zunehmende Vernetzung 663

Seite

2. Abschottung und Entnetzung als technisch-organisatorische Gegenstrategie ... 664
II. Abschottung und Entnetzung von Systemen als datenschutzrechtlich gebotene Maßnahme ... 666
1. Gesetzliche Bestimmungen zur IT-Sicherheit ... 666
2. Schutz und Entnetzung unternehmensinterner Systeme ... 670
3. Vernetzung mit externen Systemen, Outsourcing, Cloud Computing ... 677

Kapitel 6. Cyberwar und Datenschutz

A. Vernetzung ... 681
I. Einführung ... 681
II. Gesetzliche Grundlagen ... 682
III. Code is Law ... 683
IV. Cyber-Terrorismus ... 683

B. Der Datenschutzbezug, vor allem über Sicherheit und Prävention ... 684
I. Informationssicherheit ... 684
II. Datenbevorratung ... 686
III. Cyberwar- und Spionageabwehr ... 687
IV. Aufgabenstellung ... 688
V. Sensible Schwachstellen ... 688
VI. Mitarbeiter ... 689
VII. Whistleblowing ... 691
VIII. Funktionsübertragung ... 692
IX. Sicherheitsüberprüfungen ... 692
X. Datenschutz-Folgenabschätzung (DS-GVO) ... 695

C. Haftung, Sicherheitsrechtlicher Rahmen ... 698

Kapitel 7. Smart Metering und E-Mobility

A. Einleitung ... 705

B. Grundlagen des Smart Metering und der E-Mobility ... 705
I. Technische Grundlagen und Begriffsbestimmungen des Smart Metering und der E-Mobility ... 705
II. Wesentliche Anwendungsgebiete des Smart Metering und der E-Mobility ... 707
III. Sektorspezifische rechtliche Grundlagen des Smart Metering und der E-Mobility ... 708

C. Datenschutz beim Smart Metering und der E-Mobility ... 709
I. Art und Umfang der betroffenen personenbezogenen Daten ... 709
1. Art der betroffenen personenbezogenen Daten ... 709
2. Umfang der betroffenen personenbezogenen Daten ... 710

Seite

II. Berechtigte Stellen ... 711
III. Anwendbare allgemeine datenschutzrechtliche Grundsätze, insbesondere Datenvermeidung und -sparsamkeit ... 712
IV. Sektorspezifische datenschutzrechtliche Regelungen im Bereich des Smart Metering ... 713
1. Erhebung, Verarbeitung und Nutzung personenbezogener Daten ... 714
2. Auskunfts-, Einsichts- und Informationspflichten ... 719
3. Löschungspflichten und weitere Betroffenenrechte ... 721
4. Datenschutz-Folgenabschätzung ... 722
5. Sanktionen ... 722
V. Besondere datenschutzrechtliche Probleme der E-Mobility ... 722
1. Bewegungsprofile ... 723
2. Authentifizierung und Datenübermittlung ... 723

D. Datensicherheit beim Smart Metering und der E-Mobility ... 724
I. Allgemein zu berücksichtigende Grundsätze der Datensicherheit ... 726
II. Zertifizierungspflichten ... 727
1. Zertifizierungspflicht des Smart-Meter-Gateways ... 727
2. Zertifizierungspflicht des Smart-Meter-Gateway-Administrators ... 728
III. Spezielle Anforderungen an das Smart-Meter-Gateway ... 729
IV. Spezielle Anforderungen an das Sicherheitsmodul ... 730

Teil VII. Datenschutz in verschiedenen Kommunikationsformen

Kapitel 1. Datenschutz im Internet

A. Internetregulierung in Deutschland ... 732
I. Vom IuKDG und zum TMG ... 733
II. Personenbezug von IP-Adressen ... 734
1. Objektiver Personenbezug ... 735
2. Relativität des Personenbezugs ... 736
3. Infektionstheorie ... 737
4. Bewertung durch den EuGH ... 738
5. IP-Adressen von internen Rechnern ... 738
6. Bewertung von IPv6 ... 739
7. Personenbezug von IP-Adressen in der DS-GVO ... 739

B. Das Telemediengesetz ... 740
I. Überblick ... 740
II. Anwendungsbereich ... 740
1. Begriff der Telemedien ... 740
2. Ausnahme für dienstliche Telemediennutzungen ... 741
III. Verhältnis zum BDSG ... 742
IV. Zentrale Vorschriften ... 743
1. Datenverarbeitungsverbot mit Erlaubnisvorbehalt ... 743

Seite
2. Spezielle Erlaubnisvorschriften ... 743
3. Einwilligung des Nutzers ... 744
4. Sonstige Sonderregelungen ... 744

Kapitel 2. Web 2.0, Mobile Apps und die datenschutzrechtlichen Anforderungen

A. Einführung ... 748
I. Zu den Ergänzungen dieses Kapitels in dieser Auflage ... 748
II. Datenschutzrechtliche Besonderheit des Web 2.0 ... 751

B. Rechtsverhältnisse und Konstellationen ... 752

C. Rechtsgrundlagen ... 752
I. Europäische Rechtsgrundlagen ... 753
II. Deutsche Rechtsgrundlagen ... 755
1. Allgemeines Datenschutzrecht ... 755
2. Besonderes Datenschutzrecht ... 755

D. Rechtliche Einordnung von Web 2.0-Diensten ... 756
I. Telemediendienste ... 756
II. Telekommunikationsdienste ... 757
1. Übertragung lediglich beim selben Provider ... 757
2. Aufspaltung von Web 2.0-Dienstebündeln in Einzeldienste ... 757
3. Klassifizierung einzelner Dienste im Web 2.0 ... 758
III. Telekommunikationsgestützte Dienste (§ 3 Nr. 25 TKG) ... 759
IV. Rundfunk und telemedienrechtliche Vorschriften im RStV ... 760
V. Zusammenfassende Einordnung und Ausblick auf die DS-GVO ... 760
VI. Zivilrechtliche Regelungen ... 761

E. Personenbezogene Daten im Web 2.0 ... 761

F. Datenschutzrechtliche Verantwortlichkeit im Web 2.0 ... 762
I. Erwägungen der Artitel-29-Datenschutzgruppe ... 763
II. Einzelfälle im Web 2.0 ... 765
1. Plattformbetreiber ... 765
2. Plattformnutzer ... 766
3. Dritte (Anbieter von Software/Apps) ... 770

G. Das datenschutzrechtliche Verhältnis zwischen Plattformbetreiber und Nutzer ... 770
I. Die telemedienrechtlichen Anforderungen ... 770
1. Zulässigkeit der Datenverarbeitung durch den Plattformbetreiber ... 771
2. Einwilligung nach bestehender Rechtslage ... 777
3. Einwilligung künftig nach DS-GVO ... 783
4. Nutzungsvertrag, AGB und Privacy Policy (Datenschutzerklärung) ... 785
5. Sonstige Pflichten des Plattformbetreibers ... 786

Seite
II. Die telekommunikationsrechtlichen Anforderungen ... 788
III. Künftiges Recht auf Datenübertragbarkeit nach DS-GVO ... 790
IV. Pflichten des Plattformbetreibers gegenüber Dritten (Betroffenen) ... 791
H. Das datenschutzrechtliche Verhältnis zwischen Nutzern und anderen Nutzern/Dritten ... 791
I. Das datenschutzrechtliche Verhältnis zwischen Dritten und Nutzern (Apps und Mobile Apps) ... 794
J. Ausblick und Würdigung ... 795

Kapitel 3. Social Communities und deren datenschutzrechtliche Auswirkungen auf die Unternehmenspraxis

A. Überblick ... 798
B. Einsatz als Marketing-Instrument ... 798
I. Technische und wirtschaftliche Rahmenbedingungen ... 798
II. Datenschutzkonforme Erhebung von Nutzerprofilen? ... 799
1. Anwendbarkeit deutschen Datenschutzrechts ... 799
2. Safe Harbor-Urteil des EuGH ... 800
3. Erhebung der Daten/Tracking ... 802
III. Nutzung als Marketing-Instrument ... 803
1. Datenverarbeitung im Auftrag (§ 11 BDSG)/Auftragsverarbeitung ... 803
2. Datenschutzrechtliche Zulässigkeit des „Like-Buttons" ... 804
3. Impressum ... 805
4. Datenschutzerklärung bei eigenen Social Media-Netzwerken ... 805
IV. Inhaltskontrolle ... 805
C. Einsatz von Social Media-Plattformen als Recruiting-Instrument ... 806
I. Rechtliche Rahmenbedingungen ... 806
1. Aktuelle Rechtslage ... 806
2. Frei zugängliche Quellen ... 806
3. Soziale Netzwerke ... 807
II. Zivilrechtliche Zugehörigkeit des Xing-Accounts ... 807
D. Schutz des Unternehmens vor Meinungsäußerungen Dritter ... 808
I. Rechtliche Rahmenbedingungen ... 808
II. Datenschutzrechtliche Aspekte ... 808
III. Social Media Policy ... 809

Kapitel 4. Datenschutz in der Telekommunikation

A. Vorbemerkung ... 812
B. Wesentliche Regelungen des TKG zum Datenschutz ... 813
I. Grundsätzliche Anwendung (§ 91 TKG) ... 816
1. Einleitung ... 816

Seite

2. Adressaten des § 91 TKG ... 817
3. Lex specialis TKG ... 819
4. Zusammenfassung zu § 91 TKG ... 819

II. Datenübermittlung an ausländische nicht öffentliche Stellen (vormals § 92 TKG 2004, aufgehoben) ... 820

III. Informationspflichten (§ 93 TKG) ... 820
1. Grundsätze der Informationspflichten ... 820
2. Inhalt der Informationspflichten nach Abs. 1 ... 821
3. Wahlrecht bei Verkehrsdaten ... 821
4. Informationspflicht in Risikofällen ... 822
5. Auskunftsrecht juristischer Personen ... 823
6. Unentgeltlichkeit und Schriftlichkeit der Auskunft ... 823
7. Unrechtmäßige Erlangung von Daten ... 823

IV. Einwilligung im elektronischen Verfahren gemäß § 94 TKG ... 823

V. Nutzung von Bestandsdaten gemäß § 95 TKG ... 823
1. Bestandsdatennutzung ... 824
2. Bestandsdaten ... 824
3. Speicherung von Bestandsdaten ... 825
4. Speicherung für Werbung, Marketing ... 825
5. Datenspeicherung nach Vertragsende gemäß § 95 Abs. 3 TKG ... 825
6. Vorlage eines amtlichen Ausweises ... 825

VI. Verkehrsdaten (§ 96 TKG) ... 826
1. Fernmeldegeheimnis ... 826
2. Auswertung von Verkehrsdaten ... 827
3. Verwendung von Verkehrsdaten ... 827
4. Sonderproblem des § 101 UrhG ... 829

VII. Entgeltermittlung und -abrechnung (§ 97 TKG) ... 830
1. Grundsätze ... 830
2. Faktische Beweislastumkehr bei Löschung von Verkehrsdaten ... 831
3. Austausch von Daten zwischen Anbietern (Interconnection) ... 831

VIII. Standortdaten (§ 98 TKG) ... 831
1. Einleitung ... 831
2. Notrufnummern und Standortdaten ... 832

IX. Einzelverbindungsnachweis (§ 99 TKG) ... 832
1. EVN im Haushalt und in Betrieben/Behörden ... 833
2. Wahlrecht des Teilnehmers ... 833

X. Störung von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten (§ 100 TKG) ... 833

XI. Mitteilen ankommender Verbindungen (§ 101 TKG) ... 834
1. Einleitung ... 834
2. Verfahren „Fangen“ ... 835

XII. Rufnummernanzeige und -unterdrückung (§ 102 TKG) ... 836

XIII. Automatische Anrufweiterschaltung (§ 103 TKG) ... 836

XIV. Teilnehmerverzeichnisse (§ 104 TKG) ... 836

Seite

XV. Auskunftserteilung (§ 105 TKG) 837
XVI. Telegrammdienst (§ 106 TKG) und Nachrichtenübermittlungssysteme mit Zwischenspeicherung (§ 107 TKG) 838

C. Regelungen zur öffentlichen Sicherheit im Zusammenhang mit Datenschutz in der Kommunikation 839
I. Technische Schutzmaßnahmen (§ 109 TKG) 839
II. Datensicherheit (§ 109a TKG) 840
III. Überwachungsmaßnahmen (§ 110 TKG) 841
IV. Daten für Auskunftsersuchen (§ 111 TKG) und automatisiertes Auskunftsverfahren (§ 112 TKG) 841
V. Manuelles Auskunftsverfahren (§ 113 TKG) 842
VI. Regelungen zur Vorratsdatenspeicherung (§§ 113a–113g TKG) 842
1. § 113a TKG 842
2. § 113b TKG 842
3. § 113c TKG 843
4. § 113d TKG 843
5. § 113e TKG 843
6. § 113f TKG 844
7. § 113g TKG 844
VII. Kontrolle und Durchsetzung von Verpflichtungen (§ 115 TKG) 844

D. Perspektiven 845

Kapitel 5. Pflichten zur Herausgabe von und zur Auskunftserteilung über Daten

A. Einleitung 848

B. Herausgabe von Daten für Auskunfts- und Verzeichnisdienste 849
I. Inhalt des Herausgabeanspruchs 849
II. Arten der herauszugebenden Daten 849
III. Beachtung der Datenschutzvorschriften 850

C. Auskünfte über Urheberrechtsverletzungen 851
I. Voraussetzungen des Auskunftsanspruchs 852
1. Anspruchsberechtigte 852
2. Klageerhebung oder offensichtliche Rechtsverletzung 853
3. Tätigkeit in gewerblichem Ausmaß 853
4. Gerichtliche Anordnung bezüglich Verwendung von Verkehrsdaten 854
II. Verpflichtung zur Vorhaltung der Verkehrsdaten 858
1. Divergierende Judikatur zur Frage der Speicherpflicht auf Zuruf 858
2. Stellungnahme 859
3. Unvereinbarkeit der Speicherung von Verkehrsdaten auf Zuruf mit datenschutzrechtlichen Vorschriften 862

Seite

4. Beschränkung des Datenspeicherungsanspruchs auf konkrete Verbindungen ... 864

D. Auskünfte an Sicherheitsbehörden ... 865
I. Datenerhebungspflicht ... 865
II. Beauskunftung der Daten ... 866
1. Automatisiertes Auskunftsverfahren ... 866
2. Manuelles Auskunftsverfahren ... 866
III. Vorratsdatenspeicherung und -herausgabe ... 868

Teil VIII. E-Commerce

Kapitel 1. Kundendatenschutz

A. Einleitung ... 870
I. Begriffsdefinition ... 870
II. Überblick ... 870

B. Einzelne Regelungsbereiche ... 871
I. Adresshandel und Werbung ... 871
1. Allgemeines ... 871
2. Regelungsüberblick ... 871
II. CRM-Systeme, Profilbildung und Data-Mining ... 871
1. Allgemeines/Problemstellung ... 871
2. Regelungsbereiche ... 872
III. Online-Datenschutz und Webtracking ... 874
1. Online-Datenschutz ... 874
2. Webtracking ... 876

C. Änderungen nach der Datenschutz-Grundverordnung ... 877
I. Allgemeines ... 877
II. CRM-Systeme, Profilbildung und Data-Mining ... 877
III. Profilbildung ... 878
1. Allgemeines ... 878
2. Zulässigkeit ... 878
IV. Online-Datenschutz und Webtracking ... 879
V. Zusammenfassung ... 880

Kapitel 2. Bonitätsbewertung

A. Kreditwesengesetz ... 882
I. Bonitätsbewertung und Risikosteuerung ... 883
1. Scoring, Rating, Adressausfallrisiko, Bonitätsbewertung ... 884
2. Verfahren der Bonitätsbewertung ... 884
II. Scorewert – ein personenbezogenes Datum ... 884
1. Bildung einer Vergleichsgruppe und der Bezug zum Betroffenen ... 884
2. Prognosedaten und deren Personenbezug ... 885

Seite

III. Abgrenzung zwischen BDSG und KWG ... 885
1. Anwendung Scoring-Vorschrift des BDSG ... 885
2. Subsidiaritätsprinzip des § 1 Abs. 3 BDSG ... 886
3. § 10 KWG als bereichsspezifische Vorschrift ... 886
IV. Anwendungsbereich des § 10 Abs. 1 S. 3–8 KWG ... 887
1. Verbot mit Erlaubnisvorbehalt und die Bedeutung des § 10 Abs. 1 S. 3 KWG ... 887
2. Adressausfallrisiko ... 887
3. Interne Ratingsysteme ... 887
V. Normative Voraussetzungen für die Datenerhebung und -verwendung ... 888
1. Verantwortliche Stellen ... 888
2. Betroffener Personenkreis ... 888
3. Zweckbindung ... 888
4. Privilegierung der Entwicklung und Weiterentwicklung von Ratingsystemen ... 888
VI. Datenarten und Erhebungsquellen ... 889
1. Datenarten ... 889
2. Erhebungsquellen ... 890
3. Internet als allgemein zugängliche Quelle ... 890
4. Benachrichtigungspflicht ... 891
VII. Datenübermittlung ... 891
VIII. Zusammenfassung ... 892

B. Bonitätsbewertung im Rahmen des BDSG ... 892
I. Bedeutung und Wesen der Bonitätsbewertung im gegenwärtigen sozioökonomischen Rahmen ... 893
II. Rechtliche Beurteilung der Bonitätsbewertung aufgrund des BDSG ... 894
1. Persönlicher Anwendungsbereich ... 894
2. Überblick über die Rechtsgrundlagen ... 895
3. Einwilligung (§§ 4, 4a BDSG) ... 896
4. Zulässigkeitstatbestände für einen der Bonitätsbewertung dienenden Datenumgang (§§ 28 ff. BDSG) ... 897
5. Rechte des Betroffenen (§§ 33 ff. BDSG) ... 901
III. Ausblick auf die DS-GVO ... 901

Kapitel 3. Opt-in/Opt-out

A. Bedeutung des Themas ... 905
I. Schlagwortfunktion der Begriffe ... 905
II. Allgemeine Charakterisierung der Begriffe ... 905
III. Datenschutzrechtliche Relevanz des Themas ... 906
IV. Wirtschaftliche Relevanz des Themas ... 906
1. Kundenbindungs- und Rabattsysteme ... 906
2. Soziale Netzwerke ... 907
V. Rechtspolitische Aspekte des Themas ... 907

Seite

B. Rechtsgrundlagen ... 908
I. Allgemeiner Hinweis ... 908
II. Regelungen des BDSG ... 908
1. Einwilligung als Zulässigkeitstatbestand ... 908
2. Die Regelung des § 28 Abs. 3 BDSG ... 909
3. § 4a Abs. 1 S. 1 BDSG als Sedes Materiae der Diskussion ... 909
III. § 7 Abs. 2 UWG ... 909
IV. Einwilligungserklärung als AGB-Klausel ... 910

C. Gang der BGH-Rechtsprechung ... 910
I. Überblick ... 910
II. Wesentliche Erkenntnisse der „Payback"-Entscheidung ... 911
1. Darstellung der strittigen Klausel ... 911
2. Bewertung als „Opt-out"-Klausel ... 911
3. Unterscheidung zwischen datenschutzrechtlicher und wettbewerbsrechtlicher Einwilligung ... 912
4. Bewertung der datenschutzrechtlichen Einwilligung ... 913
5. Bewertung der wettbewerbsrechtlichen Einwilligung ... 914
6. Hinweis für die Praxis ... 914
III. Wesentliche Erkenntnisse der „Happy Digits"-Entscheidung ... 914
1. Darstellung der strittigen Klausel ... 914
2. Bewertung anhand der Regelungen des BDSG ... 915
IV. Konsequenzen der BGH-Rechtsprechung ... 915

D. Meldungen an die SCHUFA ... 916

E. Verfahrensrechtliche Fragen ... 916
I. Klagemöglichkeiten nach dem UKlaG ... 916
II. Nachweis des Vorliegens einer Einwilligung durch „Double-Opt-in" ... 917
III. Unsicherheiten aufgrund des Urteils des OLG München vom 27.9.2012 ... 919

F. Erkenntnisse aus der Rechtsprechung zu Opt-in-Konstellationen ... 920

G. Ausblick auf die Datenschutz-Grundverordnung ... 922
I. Unterscheidung von datenschutzrechtlicher und wettbewerbsrechtlicher Einwilligung ... 922
II. Tatsache des Vorliegens einer Einwilligung ... 922
III. Freiwilligkeit einer Einwilligung ... 923
IV. Gesetzlicher Erlaubnistatbestand für eine Verarbeitung zum Zwecke der Direktwerbung ... 924
V. Widerspruchsrecht im Bereich der Direktwerbung ... 925

Seite

Kapitel 4. Datenweitergabe an Handelspartner und Offenlegungspflichten; Shophosting

A. Webshop-Lösungen als datenschutzrechtliche Herausforderung 928
I. Thematische Einordnung und Herausforderungen der DS-GVO 928
II. Shophosting und Webshop-Outsourcing als Geschäftsmodell 930
III. Möglichkeiten und Grenzen von Auftragsdatenverarbeitung 931
IV. Datenschutzrechtliche Vorgaben an Offenlegungspflichten 934
1. Nachbesserungsbedarf bei Auftragsdatenverarbeitungsverträgen zwischen Online-Händlern und ihren Dienstleistern 934
2. Nutzereinwilligungen selten wirksam 936
3. Unterrichtung gemäß § 13 Abs. 1 TMG („Datenschutzerklärung") 944
4. Externe Links 948
5. Niederlassungsprinzip 949
6. Internationale Ausrichtung von Websites 950
7. Datenübermittlung in die USA 952
8. Dynamische IP-Adressen als personenbezogenes Datum 952

B. Typische Beispiele für Datenweitergabe an Partnerunternehmen im Rahmen von Webshops 953
I. Datenübermittlung an Versanddienstleister 953
II. Datenübermittlung im Rahmen von Financial Supply Chain Management 955
1. Zahlungsdienstleister 956
2. Datenübermittlung an Auskunfteien und Scoring-Anbieter 956
3. Betrugsprävention mittels Device Profiling und Tippverhaltensprofilen 957
4. Debitorenmanagement, Datenübermittlung an Inkassoanbieter 959
III. Datenübermittlung zu Werbezwecken 960
1. E-Mail-Marketing durch Full-Service-Dienstleister 960
2. Web-Analyse mit Hilfe von Web-Analysediensten 961
3. Behavioral Targeting und Retargeting durch Werbenetzwerke 962
4. Social Media Plugins 963

C. Best Practice-Ansätze; Gütesiegel 964
I. Datenschutzsiegel 965
II. Shop-Gütesiegel 965

Kapitel 5. Online-Zahlungsverkehr

A. Anwendbarkeit des Bundesdatenschutzgesetzes 968
I. Subsidiarität des BDSG 968
II. Telemediengesetz 969
1. Anwendungsbereich 969
2. Abgrenzung zum BDSG 969
III. Telekommunikationsgesetz 970
IV. Ausblick: Datenschutz-Grundverordnung 971

Seite

B. Personenbezogene Daten im Zahlungsverkehr ... 971
I. Personenbezogene Daten ... 971
II. Maßstab für Bestimmbarkeit ... 972
III. Ausblick: Personenbezogene Daten nach der DS-GVO ... 972

C. Integration einer Zahlungsmethode ... 973
I. Angebot der Zahlungsart durch den Händler direkt ... 974
1. Datenschutzhinweis und Einwilligung ... 975
2. Erstellung Datenschutzhinweis bzw. Einwilligung ... 977
3. Bestimmtheit/Transparenz/Hinweispflichten ... 978
4. Aufbau eines Datenschutzhinweises ... 980
5. Zeitpunkt ... 981
6. Form ... 981
7. AGB-Kontrolle ... 983
8. Freiwilligkeit der Einwilligung ... 983
9. Datenkommunikation mit Auskunfteien ... 984
10. Verbot automatisierter Entscheidungen ... 984
11. Scoring-Maßnahmen ... 986
12. Zusammenarbeit mit Dienstleistern und Auskunfteien ... 987
II. Einsatz von Fremdsystemen ... 987
1. Keine Auftragsdatenverarbeitung ... 988
2. Hinweispflichten des Händlers ... 988

D. Rechtsfolgen bei Verstoß ... 989

E. Zuständigkeit der Datenschutzbehörde ... 989

Teil IX. Datenschutz im Gesundheitssektor

Kapitel 1. Umgang mit Patientendaten

A. Besondere Schutzbedürftigkeit von Patientendaten ... 994

B. Die ärztliche Schweigepflicht ... 995

C. Datenerhebung, Verarbeitung und Nutzung durch den Arzt ... 997
I. Allgemeines ... 997
II. Speicherung ... 999
III. Datenveränderung und -nutzung ... 1000

D. Erhebung, Verarbeitung und Nutzung von ärztlichen Daten durch Dritte ... 1000
I. Erhebung durch Sozialversicherungsträger ... 1001
II. Erhebung ärztlicher Daten durch Gerichte, insbesondere Sozialgerichte 1005
1. Die Einholung ärztlicher Befundunterlagen bzw. Vernehmung von Ärzten als Zeugen ... 1005
2. Einholung medizinischer Sachverständigengutachten ... 1005
III. Erhebung von Patientendaten durch sonstige Dritte ... 1008
1. Erhebung durch öffentliche Stellen ... 1008
2. Erhebung durch nicht öffentliche Stellen ... 1009

Seite
IV. Datenspeicherung, -veränderung und -nutzung ... 1010
V. Übermittlung ärztlicher Daten ... 1012
1. Übermittlung von (einfachen) Patientendaten ... 1012
2. Übermittlung von medizinischen Sozialdaten ... 1013
VI. Übermittlung von medizinischen Sozialdaten für Forschung und Planung ... 1016
VII. Erhebung, Verarbeitung und Nutzung von Patientendaten als Sozialdaten durch private Dritte ... 1020
VIII. Erhebung und Verarbeitung auf Grundlage einer Einwilligung? ... 1021
IX. Übermittlung ohne Einwilligung oder normative Befugnis ... 1024
X. Problem des § 200 SGB VII ... 1026

Kapitel 2. Elektronische Patientenakte

A. Elektronische Patientenakte ... 1028
I. Ziele ... 1029
II. Prinzipien ... 1030
III. Gesundheitsdaten als sensible Daten ... 1031
IV. Verantwortliche Stelle ... 1032
V. Gesetzliche Erlaubnis ... 1033
VI. Einwilligung ... 1037
VII. Datensicherheit ... 1038

B. Ausblick auf die Datenschutz-Grundverordnung ... 1040

C. Fazit ... 1041

Kapitel 3. Telemonitoring

A. Datenschutzrechtliche Rahmenbedingungen bei Telemonitoring ... 1043
I. Einführung ... 1043
II. Anwendungsgebiete ... 1043
III. Rechtlicher Kontext ... 1044
1. Grundsätzlicher rechtlicher Rahmen ... 1044
2. Relevante datenschutzrechtliche Gesetzgebung ... 1045
IV. Verarbeitung personenbezogener Daten im Rahmen des Telemonitorings ... 1046
V. Anforderungen an die Einhaltung des Datenschutzes beim Telemonitoring ... 1048
1. Zulässigkeit des Verfahrens ... 1048
2. Datenverarbeitung im Auftrag ... 1050
3. Rechte des Betroffenen ... 1053
VI. Würdigung und Ausblick ... 1053

Seite

B. Technische und organisatorische Anforderungen im Bereich der Gesundheitstelematik ... 1054
I. Einführung ... 1055
II. Anwendungsgebiete ... 1055
III. Bewertung des Schutzbedarfs ... 1055
1. E-Health Gesetz ... 1056
2. IT-Sicherheitsgesetz ... 1056
3. Datenschutzgesetzgebung ... 1056
4. Schutzniveau ... 1056
IV. Technische Infrastruktur ... 1057
V. Technische und organisatorische Maßnahmen ... 1057
1. Gesetzlicher Rahmen ... 1057
2. Riskoanalyse ... 1058
3. Umsetzung der Hauptziele am Beispiel der eGK sowie deren Telematikinfrastruktur ... 1059
VI. Ausblick Cloud Computing und Big Data im Gesundheitswesen ... 1059

Teil X. Information als Wirtschaftsgut

Kapitel 1. Adresshandel

A. Einleitung ... 1062
B. Definition des Begriffs Adresshandel ... 1063
I. Adressdaten ... 1063
II. Sonstige Daten ... 1063
C. Erlaubnistatbestände ... 1064
I. Grundsatz ... 1064
1. Rechtsgrundlagen ... 1064
2. Praktische Umsetzung/Nutzung der Adressdaten zu Werbezwecken 1064
II. Adresshandel gemäß § 28 Abs. 3 BDSG ... 1066
1. Voraussetzung ... 1066
2. (Berechtigter) Empfängerkreis ... 1066
III. Adresshandel gemäß § 29 BDSG ... 1071
1. Allgemeines ... 1071
2. Grundsätze ... 1072
3. Besonderheiten des Adresshandels nach § 29 BDSG ... 1072
D. Änderungen aufgrund der DS-GVO ... 1074
I. Allgemeines ... 1074
II. Adresshandel unter der DS-GVO ... 1074
1. Rechtsgrundlagen ... 1074
2. Informationspflicht ... 1076
3. Weitergabe von Adressdaten innerhalb eines Unternehmens ... 1076
E. Fazit ... 1077

Seite

Kapitel 2. RFID, Smartcards und Cookies

A. RFID-Chips und Smartcards 1080
I. Funktionsweise von RFID-Chips und Smartcards 1081
1. RFID 1081
2. Smartcards 1081
3. Anwendungsgebiete 1082
II. Datenschutzrechtliche Zulässigkeit des Einsatzes von RFID und Smartcards sowie damit verbundene Sicherheitsrisiken 1082
1. Verarbeitung personenbezogener Daten 1082
2. Einwilligung oder gesetzliche Erlaubnis für die Datenverarbeitung ... 1083
3. Direkterhebungsgrundsatz 1084
4. Datenschutzrechtliche Zulässigkeit typischer Anwendungsfälle 1086
5. Aufklärungspflichten (insbesondere aus § 6c BDSG) und Haftungsrisiken 1089
6. Technisch-organisatorische Maßnahmen gemäß § 9 BDSG 1092
III. Aktuelle Entwicklungen 1092
1. Selbstverpflichtung von RFID-Anwendungsbetreibern zur Datenschutz-Folgenabschätzung 1092
2. Kennzeichnungspflicht nach der Textilkennzeichnungsverordnung 1092
3. Reform des Beschäftigtendatenschutzes 1093
IV. Ausblick Datenschutz-Grundverordnung 1093

B. Cookies 1094
I. Definition: Cookies 1094
II. Informationspflichten nach § 13 Abs. 1 TMG 1094
III. Einwilligung in das Setzen von Cookies – Umsetzung der Datenschutzrichtlinie für elektronische Kommunikation 1095
1. Einwilligungserfordernis und Ausnahmen 1095
2. Einholung der Einwilligung 1097
IV. Verwendung personenbezogener Daten 1100
V. Zulässigkeit der Datenverwendung 1102
VI. Ausblick Datenschutz-Grundverordnung 1102

Kapitel 3. Werbung im Internet

A. Beispielhafte Darstellung einzelner Konzepte 1106
I. Vorbemerkung 1106
II. Konzepte für eine werbliche Nutzung personenbezogener Daten 1106
1. Nutzung eines vorhandenen Kundendatenbestandes 1106
2. Anforderungen bei der Nutzung vorhandener Daten 1110
3. Angebote zur Anreicherung vorhandener Daten 1111
III. Methoden zur Umsetzung der Konzepte 1111
1. Soziale Netzwerke am Beispiel von Facebook und Google+ 1111
2. Webstatistik am Beispiel von Google Analytics 1113
3. Der Fall easycash: Kundenprofile auf Basis von Zahlungsdaten 1115

Seite

B. Rechtliche Schwerpunkte aus der Sicht des Werbenden ... 1117
I. Werbung im Anwendungsbereich der Datenschutz-Grundverordnung ... 1117
1. Grundlagen ... 1117
2. Einwilligung/Vertragserfüllung/Erlaubnisnorm/berechtigtes Interesse ... 1118
3. Zweckbindung ... 1119
4. Erforderlichkeit ... 1119
5. Abwägungspflichten/Dokumentationen ... 1120
6. Kernbegriffe, nicht abschließend ... 1120
II. Klarnamen, Pseudonymisierung, Anonymisierung ... 1121
1. Grundlagen ... 1121
2. Rechtliche Konsequenzen ... 1121
III. Werbung als (Mit-)Geschäftszweck von sozialen Netzwerken – die Erlaubnisnorm ... 1122
1. Datenpool ... 1122
2. Art der Daten ... 1122
3. Erlaubnisnorm für Inhaltsdaten ... 1123
4. Informierte Einwilligung ... 1124
5. Grundsatz der Zweckbindung ... 1124
IV. Social Plugin ... 1124
1. Funktionsweise ... 1124
2. Datenschutzrechtliche Problematik bei direkter Einbindung ... 1125
3. Rechtskonforme Gestaltung ... 1126
V. Ausblick ... 1128

Kapitel 4. Bewertungsportale

A. „Click-mich-an": die neue soziale Währung ... 1130

B. Bewertung im Internet in den Grenzen des Datenschutzes ... 1131
I. Allgemeine rechtliche Rahmenbedingungen ... 1131
1. Meinungsfreiheit ... 1131
2. Wettbewerbsrecht ... 1131
3. Telemedienrecht ... 1132
II. Datenschutz ... 1133
1. Anwendbarkeit datenschutzrechtlicher Vorschriften ... 1133
2. Verhältnis von TMG und BDSG ... 1134
3. Datenerhebung ... 1134
4. Berichtigung, Sperrung, Löschung ... 1135

Kapitel 5. Datenschutzkonformer Einsatz von Suchmaschinen im Unternehmen

A. Einführung ... 1138

B. Geschäftsmodell ... 1139

Seite

C. Vorbemerkungen zum Datenschutz bei Suchmaschinen ... 1141
I. Anwendbarkeit der europäischen Datenschutzbestimmungen ... 1141
II. Der Klassiker: Personenbezug der IP-Adresse ... 1142

D. Einzelne Fallgestaltungen ... 1143
I. Personenbezogene Mitarbeiterdaten auf der Website eines Unternehmens ... 1143
1. Veröffentlichung von Mitarbeiterdaten auf der Website ... 1144
2. Auffindbarkeit von Mitarbeiterdaten bei Suchmaschinen ... 1146
II. Google Hacking ... 1147
III. Googeln von Bewerbern ... 1148
IV. Web-Analyse ... 1149
1. Sinn, Anbieter und Funktionsweise ... 1149
2. Rechtliche Rahmenbedingungen ... 1149
V. Bereitstellen von Werbeflächen auf der Website eines Unternehmens ... 1154

E. Ergebnis ... 1154

Teil XI. Datensicherheit

Kapitel 1. Technische und organisatorische Maßnahmen

A. Einleitung ... 1156

B. Erläuterungen ... 1158
I. Begrifflichkeiten ... 1158
II. Anforderungen aus § 9 BDSG ... 1159
1. Grundsatz der Erforderlichkeit ... 1159
2. Grundsatz der Verhältnismäßigkeit ... 1159
3. Datenschutzgerechte Organisation ... 1159
4. Kontrollmaßnahmen der Anlage zu § 9 BDSG ... 1159
5. Empfehlung der Verschlüsselung ... 1171
III. Anforderungen nach der DS-GVO ... 1171

C. Rechtsschutz und Verfahrensfragen ... 1172

D. Kritische Würdigung ... 1173
I. Unbestimmtheit des Datenschutzgesetzes ... 1173
II. Komplexität und Inkompatibilität der Kontrollmaßnahmen ... 1175
III. Datenschutz als Managementaufgabe ... 1176
IV. Datenschutzkonzepte und Datenschutzmanagement („Datenschutzprozess") ... 1176

Kapitel 2. Schutz von Betriebs- und Geschäftsgeheimnissen

A. Einleitung ... 1179

Seite

B. Erläuterungen ... 1180
I. Entstehung des Geheimnisschutzes ... 1180
II. Spezielle Anforderungen aus § 91 AktG, § 43 GmbHG und § 25a KWG 1181
III. Maßnahmen zum Schutz von Betriebs- und Geschäftsgeheimnissen ... 1181
1. Risikoanalyse ... 1181
2. Technisch-organisatorische Maßnahmen ... 1181
3. Geheimnisträger im Unternehmen ... 1182
4. Geheimnisträger außerhalb des Unternehmens ... 1182
5. Öffentliche Auslegungsverfahren und Behördenakte ... 1182
IV. Rechtsschutz und Verfahrensfragen ... 1183
1. Strafrechtlicher Schutz ... 1183
2. Zivilrechtlicher Schutz ... 1183
V. Kritische Würdigung ... 1183
1. Konflikte mit dem Datenschutz ... 1183
2. Zusammenspiel mit dem Datenschutz ... 1186

Teil XII. Konfliktmanagement im Datenschutz

Kapitel 1. Strategie und Taktik im Umgang mit Datenschutzverletzungen

A. Einleitung ... 1189

B. Datenpanne ... 1190
I. Anwendungsbereich ... 1190
II. Inhalt und Form der Information ... 1191
III. Ordnungswidrigkeiten, Straftatbestand und Haftung ... 1192

C. Missachtung des Datenschutzes ... 1192
I. Straftatbestände und Ordnungswidrigkeiten ... 1192
II. Screening und Whistleblowing ... 1193
1. Screening ... 1193
2. Whistleblowing ... 1194

D. Compliance, interne Revision und Datenschutzorganisation ... 1194

E. Kommunikation bei Datenschutzkonflikten ... 1195
I. Überblick und Empfehlungen ... 1195
II. Kommunikationsschema ... 1196

F. Fazit des Konfliktmanagements im Datenschutz ... 1197

Kapitel 2. E-Discovery

A. Einführung ... 1199

B. Wichtige Begriffe ... 1200

Seite

C. Praktische Durchführung der E-Discovery 1205
I. Identifizierungsphase 1205
II. Sicherungsphase 1205
III. Sichtungsphase 1205
IV. Vorlegungsphase 1206

D. Rechtskonflikte und deren Lösung 1206
I. Ausgangslage: Interessens- und Rechtskonflikt für internationale Unternehmen 1206
II. Artikel-29-Datenschutzgruppe Stellungnahme 1/2009 1207
III. Lösungsansätze der französischen Datenschutzbehörde CNIL 1209
IV. Lösungsansätze der Sedona Conference 1209
V. Datenexporte aus Deutschland an eine US-Muttergesellschaft 1211
VI. E-Discovery und Schiedsverfahren 1212
VII. Auswirkungen der DS-GVO auf die E-Discovery 1213

E. Handlungsstrategien für Unternehmen in der EU 1215

F. Beispielsfälle aus der US-Rechtsprechung 1218
I. Volkswagen AG v. Valdez, Texas Supreme Court, 16.11.1995 1218
II. Access Data Corporation v. ALSTE Technologies GmbH, U. S. District Court for the District of Utah, 21.1.2010 1219
III. In re Air Cargo Shipping Services Antitrust Litigation, Eastern District of New York, 29.3.2010 1219
IV. In Re Payment Card Interchange Fee and Merchant Discount Antitrust Litigation, U. S. District Court for the Eastern District of New York, 27.8.2010 1219
V. Sofaer Global Hedge Fund, Plaintiff, v. Brightpoint, Inc. and Robert J. Laikin, Defendants, U. S. District Court, Southern District of Indiana, 12.11.2010 1220
VI. Eastern District of Virginia – MeadWestvaco Corp. v. Rexam PLC, U. S. District Court, Eastern District of Virginia, 14.12.2010 1220
VII. SunTrust v. United Guaranty Residential Insurance Co. of North, U. S. District Court, Richmond, VA, 29.3.2011 1220
VIII. Heraeus Kulzer GmbH v. Biomet, Inc., U. S. Court of Appeals for the 7th Circuit, 24.1.2011 1221
IX. Pershing Pacific West v. Marinemax, U. S. District Court, Southern District of California, 11.3.2013 1221
X. Microsoft v. United States of America, 29.8.2014 1222

Kapitel 3. Haftungsrisiken und deren Versicherung

A. Das Schadenspotential bei Datenschutzverstößen in der modernen Wirtschaftsordnung 1227

B. Bedeutung der Haftung 1229

Seite

C. Haftung des Unternehmens ... 1229
I. Rechtsgrundlagen der Haftung (Überblick) ... 1229
II. Deliktsrechtliche Haftung ... 1230
1. Haftung aus schuldhafter gesetzeswidriger Datenverwendung nach § 7 BDSG ... 1230
2. Haftung aus gesetzeswidriger automatisierter Datenverwendung durch öffentlich-rechtliche Unternehmen nach § 8 BDSG ... 1236
3. Haftung aus schuldhaftem Rechtsverstoß nach § 44 Abs. 1 S. 1 i. V. m. S. 4 TKG ... 1241
4. Haftung aus schuldhafter Datenschutzverletzung nach den allgemeinen Regeln über unerlaubte Handlungen (§§ 823, 824, 826 BGB) ... 1243
III. Zusammentreffen mehrerer Haftungsgründe – vorvertragliche, vertragliche und nachvertragliche Haftung ... 1244
IV. Negatorische Haftung (Beseitigungs- und Unterlassungsanspruch) ... 1245
V. Verjährung ... 1246
VI. Mehrheit von Schädigern ... 1247
VII. Freizeichnung – Verzicht ... 1247
VIII. Streitigkeiten ... 1247

D. Haftung des betrieblichen Datenschutzbeauftragten ... 1247

E. Haftung des Arbeitnehmers ... 1248

F. Versicherung ... 1249

G. Exkurs: Haftung nach der Datenschutz-Grundverordnung ... 1250
I. Einleitung ... 1250
II. Sachlicher Anwendungsbereich ... 1252
III. Räumlicher Anwendungsbereich ... 1252
IV. Persönlicher Anwendungsbereich ... 1253
V. Haftung des Verantwortlichen ... 1253
1. Anspruchsvoraussetzungen ... 1253
2. Haftungsbefreiung ... 1255
3. Beweislast ... 1257
VI. Haftung des Auftragsverarbeiters ... 1257
1. Anspruchsvoraussetzungen ... 1257
2. Haftungsbefreiung ... 1258
3. Beweislast ... 1258
VII. Rechtsfolge ... 1258
VIII. Mehrheit von Schädigern ... 1258
IX. Streitigkeiten ... 1260

Seite

Teil XIII. Straf- und Ordnungswidrigkeitenvorschriften im Bereich des betrieblichen Datenschutzes

A. Bedeutung ... 1263

B. Sanktionsvorschriften des BDSG ... 1265
I. Blankettbestimmungen ... 1265
1. Gesetzlichkeitsprinzip ... 1265
2. Änderung der Ausfüllungsnorm ... 1266
3. Irrtumsproblematik ... 1267
II. Anwendbarkeit ... 1267
III. Europäischer Einfluss ... 1269
IV. Tatbestandsstrukturen und Rechtsfolgen ... 1270
1. Ordnungswidrigkeiten nach § 43 Abs. 1 BDSG ... 1270
2. Ordnungswidrigkeiten nach § 43 Abs. 2 BDSG ... 1270
3. Adressat der Bußgeldanordnung ... 1270
4. Bemessung der Geldbuße ... 1271
5. Straftatbestand des § 44 BDSG ... 1271
6. Keine allgemeine Zugänglichkeit personenbezogener Daten ... 1272
7. Präventives Verbot mit Erlaubnisvorbehalt ... 1273
V. Die Tatbestände des § 43 Abs. 2 BDSG ... 1273
1. Nr. 1: Unbefugtes Erheben und Verarbeiten ... 1273
2. Nr. 2: Unbefugtes Bereithalten zum Zwecke des Datenabrufs ... 1273
3. Nr. 3: Unbefugter Datenabruf ... 1274
4. Nr. 4: Erschleichen der Übermittlung von personenbezogenen Daten durch unrichtige Angaben ... 1274
5. Nr. 5: Verstöße gegen die besondere Zweckbindung von Daten ... 1274
6. Nr. 5a: Verstoß gegen das Koppelungsverbot des § 28 Abs. 3b BDSG 1275
7. Nr. 5b: Verstoß gegen das Verarbeitungs- und Nutzungsverbot des § 28 Abs. 4 BDSG ... 1275
8. Nr. 6: Deanonymisierung ... 1275
9. Nr. 7: Verstoß gegen die Mitteilungspflicht bei unrechtmäßiger Kenntniserlangung von Daten ... 1275
VI. Die Strafvorschrift des § 44 BDSG ... 1275

C. Konfliktfelder des betrieblichen Datenschutzes aus strafrechtlicher Sicht ... 1278
I. Überwachung und Störung des Telefonverkehrs ... 1278
II. Überwachung des Schriftverkehrs ... 1278
III. Überwachung des E-Mail-Verkehrs ... 1279
1. Eingriff in das Fernmeldegeheimnis ... 1279
2. Arbeitgeber als Telekommunikationsanbieter nach § 206 StGB und Betreiber von Empfangsanlagen nach § 89 TKG ... 1279
3. Tatsituation bei einem Eingriff in das Fernmeldegeheimnis ... 1280
4. Rechtfertigungsgründe ... 1281
IV. Datenzugriff unter Überwindung einer Zugangssicherung ... 1282

Seite

V. Videoüberwachung besonders geschützter Räume 1283
VI. GPS-Überwachung 1283

D. Datenschutz-Grundverordnung 1285
I. Überblick 1285
II. Bußgeldverstöße nach Art. 83 Abs. 4 DS-GVO 1285
1. Verstöße von Verantwortlichen und Auftrags(daten)verarbeitern (Art. 83 Abs. 4a DS-GVO) 1286
2. Verstöße von Zertifizierungsstellen (Art. 83 Abs. 4b DS-GVO) 1287
3. Verstöße der Überwachungsstelle (Art. 83 Abs. 4c DS-GVO) 1287
III. Bußgeldverstöße nach Art. 83 Abs. 5 DS-GVO 1287
1. Verstöße gegen die Grundsätze der Datenverarbeitung (Art. 83 Abs. 5a DS-GVO) 1287
2. Verstöße gegen die Rechte der betroffenen Person (Art. 83 Abs. 5b DS-GVO) 1287
3. Verstöße bei der Datenübermittlung an Drittländer oder internationale Organisationen (Art. 83 Abs. 5c DS-GVO) 1288
4. Verstöße gegen Vorschriften für besondere Verarbeitungssituationen nach Kapitel IX (Art. 83 Abs. 5d DS-GVO) 1288
5. Verstöße gegen Anweisungen der Aufsichtsbehörde (Art. 83 Abs. 5e DS-GVO) 1289
IV. Kriterien bei der Bestimmung der Geldbuße 1289
V. Begriff des Unternehmens nach Art. 101 und 102 AEUV 1290
VI. Übertragung in das Datenschutzrecht 1291
1. Kritik 1291
2. Schlussfolgerung 1293

Sachverzeichnis 1297