

# Inhaltsverzeichnis

	Seite
Vorwort .....	V
Inhaltsübersicht .....	VII
Bearbeiterverzeichnis .....	LXI
Abkürzungsverzeichnis .....	LXV

## Teil I. Allgemeine datenschutzrechtliche Grundlagen und Strukturen

### Kapitel 1. Vom Volkszählungsurteil zur Datenschutz-Grundverordnung

<b>A. Entwicklung des Datenschutzes .....</b>	<b>4</b>
I. Vom BDSG zur DS-GVO .....	4
II. Weitere Kodifikationen und europäische Regelungen .....	7
1. Grundrechte und Grundfreiheiten .....	7
2. Kompetenz zu BDSG .....	10
3. Errungenschaften .....	10
III. Recht auf informationelle Selbstbestimmung und dessen Weiterent- wicklung .....	11
<b>B. Zum Stand des Datenschutzrechts .....</b>	<b>14</b>
I. Allgemeines .....	14
II. BDSG .....	15
1. Anwendung .....	15
2. Adressat .....	15
3. Begriffe, Definitionen .....	15
4. Verbotsprinzip .....	17
III. DS-GVO .....	18
<b>C. Modernisierungsbedarf .....</b>	<b>23</b>
I. Modernisierungsbedarf aufgrund der Rechtsprechung .....	23
1. Innerer Bereich der Zurückgezogenheit .....	24
2. Zweckbindung .....	24
3. Recht auf informationelle Selbstbestimmung .....	24
II. Modernisierungsbedarf aufgrund der sonstigen Entwicklung .....	31
1. Ansätze, Materialien .....	31
2. EU: Digitale Agenda .....	32
3. USA-Impulse .....	32
4. Europarat .....	33
5. ePrivacy-VO .....	34
III. Beschäftigtendatenschutz BDSG (2009 und 2018) .....	34

	Seite
IV. Datenschutz-Grundverordnung .....	36
1. Grundbausteine .....	36
2. Neue Instrumente .....	37
3. Nicht eingelöste Vorgaben vom 4.11.2010 .....	37
4. Kritik .....	38
V. Einzelne Aspekte von Verbesserungen durch die DS-GVO .....	40
1. Intransparenz .....	40
2. Technisch veraltet .....	40
3. Berücksichtigung der Rechtsprechung .....	40
4. Zahnloses Gesetz, schwache Sanktion .....	41
5. BDSG keine Marktverhaltensregelung? .....	42
D. Netzzugang, Netzwerkdurchsetzungsgesetz (NetzDG) .....	43
E. Informationsethik und Datenschutz .....	47
 <b>Kapitel 2. Die Europäische Dimension des Datenschutzes</b> 	
A. Europarechtlicher Rahmen .....	54
I. Motivation .....	54
II. Gegenwärtiger Rechtszustand .....	55
1. Unmittelbar einschlägiges Sekundärrecht .....	55
2. Sonstiges Sekundärrecht .....	56
3. Primärrecht .....	57
4. Weitere Normen und „Softlaw“ .....	61
III. Sekundärrechtlich determinierte europäische datenschutzrechtliche Grundsätze .....	62
1. Anwendbarkeit nur bei Personenbezug und nur bei natürlichen Personen .....	62
2. Verarbeitung nach Treu und Glauben (Art. 5 Abs. 1 lit. a DS-GVO) .....	63
3. Zweckbindungsgrundsatz (Art. 5 Abs. 1 lit. b DS-GVO) .....	63
4. Richtigkeit (Art. 6 Abs. 1 lit. d DS-GVO) .....	63
5. Datenvermeidung und Datensparsamkeit (Art. 6 Abs. 1 lit. c und lit. e DS-GVO) .....	63
6. Unterscheidung sensible/nicht sensible Daten (Art. 9 DS-GVO) .....	63
7. Verbot mit Erlaubnisvorbehalt .....	64
8. Betroffenenrechte .....	64
9. Unabhängige Vorabkontrolle .....	65
10. Accountability und Informationssicherheit als Neuerungen .....	65
11. Stärkung der Verantwortlichkeit .....	65
B. Judikatur .....	66
I. Lindqvist (C-101/01) .....	66
II. Österreichischer Rundfunk (C-465/00, C-138/01, C-139/01) .....	66
III. Vorratsdatenspeicherung I (C-201/06) .....	67
IV. Markkinapörssi (C-73/07) .....	67



	Seite
V. Datenschutzbeauftragter I (C-518/07) .....	67
VI. Rijkeboer (C-553/07) .....	67
VII. Datenschutzbeauftragter II (C-614/10) .....	67
VIII. Bavarian Lager (C-28/08 P) .....	67
IX. Agrarbeihilfen (C-92/09, 93/09) .....	68
X. ASNEF (C-468/10, C-469/10) .....	68
XI. Promusicae (C-275/06) .....	68
XII. Scarlet (C-70/10) .....	68
XIII. Vorratsdatenspeicherung II (C-293/12, C-594/12, C-46/13) .....	68
XIV. Google Spain (C-131/12) .....	68
XV. Ungarische Datenschutzbehörde – Jóri (C-288/12) .....	69
XVI. Safe Harbor (C-362/14) .....	69
XVII. Dynamische Internetadressen (C-582/14) .....	69
XVIII. Tele 2 Sverige (C-203/15) .....	69
XIX. Facebook Fanpages (C-210/16) .....	70
C. Internationale Vorgaben .....	70

**Kapitel 3. Internationale Anwendbarkeit der DS-GVO und  
Zuständigkeit der Aufsichtsbehörden**

A. Einführung .....	75
I. Die Struktur der kollisionsrechtlichen Prüfung .....	75
II. Rechtsquellen des Datenschutzkollisionsrechts.....	76
III. Die Bedeutung der internationalen Zuständigkeit der Aufsichtsbe- hörden .....	77
IV. Gang der Darstellung .....	78
B. Internationale Anwendbarkeit der DS-GVO .....	78
I. Die maßgeblichen Grundsätze .....	78
1. Die Kollisionsnormen des Art. 3 DS-GVO .....	78
2. Die EuGH-Rechtsprechung zum Datenschutzkollisionsrecht .....	79
II. Die Anknüpfung an die Niederlassung (Art. 3 Abs. 1 DS-GVO) .....	85
1. Begriff und Belegenheit der Niederlassung .....	85
2. Die Zuordnung der Datenverarbeitung zur Niederlassung .....	90
3. Zusammenfassung: Niederlassungsbegriff und Zuordnung der Datenverarbeitung zur Niederlassung .....	94
4. Zuordnung der Datenverarbeitung zu mehreren Niederlassun- gen .....	94
5. Einzelfälle zur Niederlassung .....	95
6. Niederlassungen in Drittstaaten .....	97
III. Die Anknüpfung an die Verarbeitung von Daten Betroffener in der Union (Art. 3 Abs. 2 DS-GVO) .....	99
1. Das Marktortprinzip .....	99



	Seite
2. Daten Betroffener in der Union .....	99
3. Anbieten von Waren oder Dienstleistungen .....	101
4. Datenverarbeitung zum Zweck der Beobachtung .....	104
IV. Das anwendbare Datenschutzrecht bei der Auftragsverarbeitung .....	106
1. Maßgeblichkeit des Art. 3 DS-GVO für Auftragsverarbeiter .....	106
2. Anwendbarkeit der DS-GVO auf Auftragsverarbeiter .....	107
V. Änderung von Anknüpfungspunkten .....	108
C. Die internationale Zuständigkeit der Aufsichtsbehörden .....	108
I. Einführung .....	108
II. Die Zuständigkeitsregelung des Art. 55 DS-GVO .....	110
1. Die Grundlagen der Zuständigkeit .....	110
2. Die Anknüpfung an die Niederlassung .....	110
3. Auswirkungen auf Betroffene und weitere Zuständigkeits- gründe .....	111
4. Internationale Zuständigkeit aufgrund mitgliedstaatlichen Rechts .....	112
III. Zuständigkeit bei grenzüberschreitender Datenverarbeitung .....	112
1. Das Konzept der federführenden Zuständigkeit .....	112
2. Der Anwendungsbereich der Regeln zur federführenden Auf- sichtsbehörde .....	114
3. Die Bestimmung der federführenden Aufsichtsbehörde .....	118
IV. Die Kooperation der Aufsichtsbehörden .....	121
1. Die Zusammenarbeit der Aufsichtsbehörden .....	121
2. Die Modifikation der Zuständigkeit (Art. 56 Abs. 2–5 DS-GVO) .....	122
V. Zuständigkeit der Aufsichtsbehörden in Fallgruppen .....	124
1. Unternehmen mit (Haupt-)Niederlassung in Deutschland .....	124
2. Unternehmen mit (Haupt-)Niederlassung in anderen EU- Staaten .....	125
3. Unternehmen mit (Haupt-)Niederlassung im Drittstaat .....	126

#### Kapitel 4. Internationaler Datenschutz

A. Einführung .....	128
B. Nordamerika .....	129
I. USA .....	129
II. Einige Konsequenzen .....	133
III. Kanada .....	135
C. Asien .....	136
I. Indien .....	136
II. Volksrepublik China/Hongkong/Singapur .....	137
III. Japan/Südkorea .....	138
D. Südamerika .....	139



E. Australien/Neuseeland .....	141
--------------------------------	-----

Kapitel 5. Grundsätze der datenschutzrechtlichen Prüfung

A. Woran erkennt man die datenschutzrechtliche Relevanz? .....	144
--	-----

B. Welche Regelungen sind heranzuziehen? .....	145
--	-----

I. Verhältnis der DS-GVO zu nationalen Datenschutzbestimmungen .....	145
--	-----

II. Liegen besondere Verarbeitungssituationen vor, die sogleich in das nationale Recht verweisen? .....	147
---	-----

1. Freiheit der Meinungsäußerung und Informationsfreiheit .....	147
---	-----

2. Beschäftigtendatenschutz .....	148
-----------------------------------	-----

III. „Personenbezogene Daten“ als Voraussetzung für die Anwendung des Datenschutzrechts .....	148
---	-----

1. Begriff des „personenbezogenen Datums“ .....	148
---	-----

2. Abgrenzung zu anonymen Daten .....	149
---------------------------------------	-----

3. Pseudonymisierung .....	149
----------------------------	-----

IV. „Private Nutzung“ – Ausschluss des Datenschutzrechts? .....	150
---	-----

1. Abgrenzung von privater und familiärer Nutzung zu „sonstiger Nutzung“ personenbezogener Daten .....	150
--	-----

2. Problem der „gemischten Nutzung“ .....	151
---	-----

V. Das „Marktortprinzip“ und der räumliche Anwendungsbereich der DS-GVO .....	151
---	-----

VI. „Verarbeitung“ personenbezogener Daten .....	151
--	-----

1. Begriff der „Verarbeitung“ .....	151
-------------------------------------	-----

2. Folgerung .....	152
--------------------	-----

VII. „Verantwortlicher für die Verarbeitung“ – an wen richtet sich die DS-GVO? .....	152
--	-----

1. Begriff des „Verantwortlichen“ .....	152
---	-----

2. Abgrenzung zu „Auftragsverarbeiter“ .....	153
--	-----

3. „Dritter“ .....	153
--------------------	-----

VIII. Grundsätze und Bedingungen für die Rechtmäßigkeit der Verarbeitung .....	153
--	-----

1. Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 DS-GVO) .....	153
--	-----

2. Rechtmäßigkeit der Verarbeitung (Art. 6 DS-GVO) .....	154
--	-----

IX. Pflichten des Verantwortlichen .....	157
--	-----

1. Gegenüber dem Betroffenen .....	157
------------------------------------	-----

2. Datenschutzmanagement .....	164
--------------------------------	-----

X. Rechte des Betroffenen .....	168
---------------------------------	-----

1. Pflichten des Verantwortlichen, die zugleich Rechten des Betroffenen entsprechen .....	168
---	-----

2. Widerspruch gegen die Verarbeitung .....	169
---	-----

3. Kontakt zum Datenschutzbeauftragten .....	169
--	-----

4. Beschwerderecht (Art. 77 DS-GVO) .....	169
---	-----



<b>Annex: Rechtslage in Österreich</b>	<b>Seite</b>
A. Die hartnäckige Natur des österreichischen Datenschutzrechts im Verfassungsrang .....	171
B. Das österreichische Grundrecht auf Datenschutz für juristische Personen .....	172
C. Die eingeschränkte legislative Kompetenz des Bundes für Fragen des Datenschutzes .....	174
D. Der eingeschränkte räumliche Anwendungsbereich des österreichischen Datenschutzgesetzes .....	174
E. Zusammenfassung .....	175

## Teil II. Datenschutzorganisation

### Kapitel 1. Nachweispflichten/Accountability

A. Bedeutung des Themas .....	179
B. Rechtsgrundlagen .....	181
I. Allgemeiner Hinweis .....	181
II. Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO .....	182
III. Nachweispflichten gemäß Art. 24 Abs. 1 DS-GVO .....	182
IV. Weitere spezielle Nachweispflichten .....	182
C. Umfang und Reichweite der Nachweispflichten .....	183
I. Wortlautauslegung .....	184
II. Historische Auslegung .....	184
III. Teleologische Auslegung .....	185
IV. Systematische Auslegung .....	185
V. Zwischenergebnis .....	186
D. Rechtsstaatliche Bedenken gegen zu weit verstandene Nachweispflichten .....	187
I. Verhältnismäßigkeitsgrundsatz .....	187
II. Bestimmtheitsgrundsatz .....	187
III. Bedeutung der Nachweispflichten im Verwaltungsverfahren .....	187
IV. Bedeutung der Nachweispflichten im Bußgeld- und Strafverfahren ..	189
V. Nachweispflichten gegenüber dem Betroffenen? .....	191
VI. Bedeutung der Nachweispflichten im zivilrechtlichen Schadensersatzverfahren .....	192
E. Risikoadäquate Reduktion der Nachweispflichten .....	194
I. Nachweispflichten als risikoferner „Vor-Vorfeldschutz“ .....	194
II. Gewichtungsp Parameter des risikobasierten Ansatzes .....	195
1. Art der Verarbeitung .....	195
2. Umfang der Verarbeitung .....	195
3. Umstände der Verarbeitung .....	195
4. Zwecke der Verarbeitung .....	195



	Seite
III. Risiko für den Betroffenen, fehlendes Schutzgut .....	198
IV. Eintrittswahrscheinlichkeit und Schwere der Risiken .....	199
F. Empfehlungen für die Praxis .....	199

**Kapitel 2. Datenschutzmanagement und Datenschutzprozesse**

A. Allgemeines .....	201
B. Rechtliche Grundlagen .....	202
C. Datenschutzaudit und Bewertung des Datenschutzrisikos .....	202
I. Erfassung aller datenschutzrelevanten Prozesse .....	203
II. Rechtliche Bewertung und Risikoanalyse .....	204
D. Verzeichnis von Verarbeitungstätigkeiten .....	205
I. Rechtliche Anforderungen .....	205
1. Erforderliche Inhalte .....	205
2. Form und Sprache des Verzeichnisses .....	206
3. Zuständigkeit .....	207
II. Aufbau und Pflege des Verzeichnisses von Verarbeitungstätigkeiten .....	207
1. Erfassung von Verarbeitungstätigkeiten und Prozesseignern .....	207
2. Detailerfassung für einzelne Verarbeitungstätigkeiten .....	208
III. Ausnahme für KMU .....	208
E. Datenschutzrichtlinie und wesentliche Prozesse .....	210
I. Datenschutzrichtlinie .....	210
II. Prozess: Einbindung des Datenschutzbeauftragten .....	210
III. Prozess: Datenschutzrechtliche Prüfung .....	211
IV. Prozess: Sensibilisierung der Mitarbeiter .....	211
V. Weitere Prozesse .....	212
F. Datenschutzmanagement-System .....	212

**Kapitel 3. Betrieblicher Datenschutzbeauftragter**

A. Benennung eines Datenschutzbeauftragten .....	215
I. Pflicht zur Benennung .....	215
1. Allgemeines .....	215
2. Zehn-Personen-Grenze .....	215
3. Anderweitige Pflicht zur Benennung .....	216
II. Formelle Anforderungen an die Benennung .....	217
1. Nachweisbarkeit .....	217
2. Veröffentlichung der Kontaktdaten .....	217
3. Mitteilung an die Aufsichtsbehörde .....	218
4. Benennung eines externen Datenschutzbeauftragten .....	218
5. Benennung zum Konzerndatenschutzbeauftragten .....	219
6. Befristung der Benennung zum Datenschutzbeauftragten .....	219
7. Mitbestimmung des Betriebsrats .....	220



	Seite
III. Abberufung eines Datenschutzbeauftragten .....	220
1. Wichtiger Grund für die Abberufung .....	220
2. Arbeitsrechtliche Anforderungen an die Abberufung .....	221
3. Abberufung eines externen Datenschutzbeauftragten .....	221
4. Sonderfall: Fusionen und Übernahmen (M&A) .....	222
IV. Sanktionen .....	223
<b>B. Qualifikation des Datenschutzbeauftragten .....</b>	<b>223</b>
I. Risikobasierter Ansatz .....	223
II. Berufliche Qualifikation .....	223
1. Juristische Qualifikation .....	224
2. IT-Wissen .....	224
3. Sonstige Fähigkeiten .....	224
III. Persönliche Eignung .....	225
<b>C. Die rechtliche Stellung des Datenschutzbeauftragten im Unternehmen ....</b>	<b>225</b>
I. Weisungsfreiheit .....	225
II. Besonderer Kündigungsschutz und Benachteiligungsverbot .....	226
III. Unterstützung des Datenschutzbeauftragten .....	226
IV. Anbindung an die höchste Managementebene .....	227
V. Kein Interessenkonflikt .....	227
<b>D. Aufgaben des Datenschutzbeauftragten .....</b>	<b>230</b>
I. Unterrichtung und Beratung .....	230
II. Überwachung der Einhaltung .....	231
III. Zusammenarbeit mit der Aufsichtsbehörde .....	231
IV. Verschwiegenheitspflicht .....	232
<b>E. Haftung des Datenschutzbeauftragten .....</b>	<b>232</b>
<b>Kapitel 4. Selbstkontrolle und Datenschutzaufsicht</b>	
<b>A. Allgemeines, Aufgaben .....</b>	<b>235</b>
<b>B. Verhältnis der beiden Einrichtungen zueinander .....</b>	<b>237</b>
I. Unterstützung des Beauftragten .....	237
II. Befugnis der Aufsichtsbehörde zu Anordnungen .....	238
III. Abberufung .....	238
IV. Betretungsrechte .....	238
<b>C. Weitere Formen der Selbstkontrolle und der Fremdkontrolle .....</b>	<b>239</b>
<b>D. Grundsätze, Instrumente .....</b>	<b>240</b>
<b>E. Der Betriebsrat als datenschutzrechtliche „Kontrollinstanz“ .....</b>	<b>241</b>
<b>Kapitel 5. Compliance und Datenschutz</b>	
<b>A. Der Begriff Compliance .....</b>	<b>245</b>
I. Verwendung in Normen .....	245
II. Definition Compliance und Abgrenzung zu Governance .....	247



	Seite
<b>B. Compliance und Datenschutz</b> .....	249
I. Rechtsgrundlagen: Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 DS-GVO) und Rechtmäßigkeit der Verarbeitung (Art. 6 DS-GVO) .....	250
II. Rechenschaftspflicht/Dokumentation .....	252
III. Verantwortlichkeit .....	254
1. Unternehmensgruppen (Konzernregelungen) .....	254
2. Verarbeitungsgrundlagen .....	255
3. Maßnahmen zur Einhaltung der Verantwortlichkeiten .....	255
<b>C. Folgen fehlender Beachtung datenschutzrechtlicher Regelungen und Einhaltung der Compliance-Vorgaben</b> .....	262
I. Bußgelder .....	262
II. Straftat .....	265
III. Schadensersatz .....	265
IV. Sonstige Folgen – Verwertungsverbot .....	266
 <b>Kapitel 6. Datenschutz und Zertifizierung</b>	
<b>A. Einführung</b> .....	269
<b>B. Selbstregulierung</b> .....	272
<b>C. Datenschutzaudit</b> .....	275
<b>D. Besonderheiten bei Cloud Computing</b> .....	277
<b>E. Verhaltensregeln, Branchenregeln</b> .....	279
<b>F. Safe Harbor – eine Art Test, Privacy Shield</b> .....	281
<b>G. Zertifizierung und Verhaltensregeln, Verfahren</b> .....	285
I. Zertifizierung .....	285
II. Verhaltensregeln .....	288
 <b>Annex: Rechtslage in Österreich</b>	
<b>A. Der Datenschutzbeauftragte</b> .....	292
I. Einleitung .....	292
II. Bestellung .....	292
III. Position .....	293
<b>B. Befugnis der Aufsichtsbehörde (Datenschutzaufsicht)</b> .....	295
<b>C. Compliance und Datenschutz</b> .....	295
<b>D. Österreichischer Datenschutzrat</b> .....	296
 <b>Teil III. Informationspflichten</b>	
<b>A. Einleitung</b> .....	299
I. Hintergrund und Bedeutung .....	299
II. Überblick über die Systematik der Informationspflichten .....	301



	Seite
<b>B. Inhaltliche Anforderungen an die Informationspflichten .....</b>	<b>303</b>
I. Art. 13 DS-GVO .....	303
1. Systematik .....	303
2. Informationspflichten nach Abs. 1, 2 .....	304
3. Zweckänderung .....	309
4. Zeitpunkt und Form der Informationserteilung .....	311
II. Art. 14 DS-GVO .....	313
<b>C. Sonderfälle .....</b>	<b>314</b>
I. Werbung und Interessenabwägung (Art. 6 Abs. 1 lit. f DS-GVO) .....	314
II. Nachweispflichten .....	316
<b>D. Zusammenfassung .....</b>	<b>317</b>

#### Annex: Rechtslage in Österreich

<b>A. Datenschutzgesetz .....</b>	<b>318</b>
<b>B. Gewerberecht .....</b>	<b>318</b>
<b>C. E-Commerce-Gesetz .....</b>	<b>319</b>
<b>D. Unterstützung durch die Datenschutzbehörde .....</b>	<b>319</b>
<b>E. Rechtsanwendung .....</b>	<b>320</b>

### Teil IV. Archivierung und Entsorgung

#### Kapitel 1. Datenschutzkonzepte

<b>A. Speicherpraxis zwischen Aufbewahrungs- und Löschpflicht .....</b>	<b>327</b>
I. Fortschreitende Digitalisierung, billiger Speicherplatz und Auslagerung als Herausforderungen an die betriebliche Gedächtnisorganisation .....	327
II. Begriffe: Aufbewahrung, Archivierung, Speicherung, Ablage, Löschung, Vernichtung, Entsorgung .....	328
III. Schwierigkeiten der Phasenabgrenzung .....	333
IV. Praxis der Datenschutzbehörden .....	333
V. Rechtsprechungspraxis .....	341
<b>B. Archivierung .....</b>	<b>344</b>
I. Bedeutung: Revisions- und IT-Sicherheit, IT-Compliance, E-Discovery, Beweisqualität von E-Mails .....	344
II. Rechtsgrundlagen .....	345
1. Datenschutzrechtliche Speicherbefugnis .....	345
2. Handels- und steuerrechtliche Anforderungen, GoB, GoBD .....	347
3. Papierloses Büro, ersetzendes Scannen .....	353
4. Betriebliche Mitbestimmung .....	356



	Seite
<b>C. Entsorgung</b> .....	356
I. Bedeutung .....	356
II. Gesetzliche Anforderungen an Löschung und Entsorgung von personenbezogenen Daten .....	358
1. Begriff des Löschens .....	358
2. Differenzierung nach Art des Datenträgers .....	359
3. Datenschutzrechtlicher Löschanpruch .....	360
 <b>Kapitel 2. Technische und organisatorische Maßnahmen</b>	
<b>A. Archivierung</b> .....	365
I. Zentrale/dezentrale Archivierung .....	365
II. Langzeitarchivierung .....	367
1. Archivierung von Arbeitsprozessdaten .....	367
2. Archivierung digitaler Signaturen .....	368
III. Dokumentenmanagementsysteme .....	369
IV. Externe Archivierung .....	370
<b>B. Entsorgung</b> .....	371
I. Technische Lösungsverfahren .....	371
1. Löschen durch Überschreiben .....	371
2. Magnetische Durchflutung und thermische Zerstörung .....	373
3. Mechanische Zerstörung .....	373
II. Datenschutzgerechte Entsorgungskonzepte .....	375
1. Technische und organisatorische Maßnahmen nach DS-GVO ...	375
2. Datenschutzkonformes Löschkonzept nach DIN 66398:2016-05	376
III. Entsorgung durch Dienstleister .....	379
1. Auftragsverarbeitung .....	379
2. Herrschaftstheorie .....	382
 <b>Kapitel 3. Archivierung und Protokollierung als Problem des betrieblichen Datenschutzes</b>	
<b>A. Konflikt zwischen IT-Sicherheit/Revisionssicherheit und Datenschutz</b> ....	386
I. Erlaubte Privatnutzung .....	387
II. Rückgabe von Firmengeräten/Ausscheidensregelung .....	390
<b>B. Urheberrechtliche Zulässigkeit der Archivierung</b> .....	390
<b>C. Umgang mit Datenbeständen, insbesondere mit Altbeständen</b> .....	392
I. Cloud-Storage und Dokumentenmanagementsysteme in der Cloud	392
II. Big Data – Datenbanken, Datenportabilität und Doublettenvermeidung .....	394
 <b>Annex: Rechtslage in Österreich</b>	
<b>A. Archivierung</b> .....	398
I. Allgemeines zur Archivierung und Datensicherung .....	398



	Seite
II. Rechtliche Anforderungen an die Archivierung und Datensicherung	399
1. Relevante Rechtsgrundlagen .....	399
2. Elektronische Buchführung .....	400
3. Bedeutung von Archivierung und Back-ups für das IKS .....	401
B. Das Löschen von Daten .....	401
I. Umfang der Löschung .....	402
II. Keine unbefristete Aufbewahrung .....	403
III. Speicherung über die Aufbewahrungspflichten hinaus .....	

## Teil V. Datenschutz und Personal

### Kapitel 1. Beschäftigtendatenschutz

A. Einleitung .....	407
B. Beschäftigtendatenschutz unter der DS-GVO .....	408
I. Regelungsspielraum nach Art. 88 Abs. 1 DS-GVO .....	411
1. Bestimmung des mitgliedstaatlichen Regelungsspielraums .....	411
2. Abgrenzung der Spezifizierung zur Auslegung und zu Beschränkungen, Abweichungen und Ausnahmen .....	416
II. Regelungsspielräume nach Art. 6 Abs. 2 und Abs. 3 DS-GVO .....	417
1. Datenverarbeitung zur Erfüllung einer gesetzlichen Verpflichtung .....	418
2. Bestimmung des mitgliedstaatlichen Regelungsspielraums nach Art. 6 Abs. 2 DS-GVO .....	420
3. Bestimmung des mitgliedstaatlichen Regelungsspielraums nach Art. 6 Abs. 3 UAbs. 2 DS-GVO .....	422
III. Konkurrenzen .....	424
C. Kodifikation des Beschäftigtendatenschutzes .....	425
D. Datenschutzbezogene Betriebsvereinbarungen .....	429
I. Datenschutzbezogene Betriebsvereinbarungen nach bisherigem Recht .....	429
II. Datenschutzbezogene Betriebsvereinbarungen unter der DS-GVO ...	431
E. Fragerecht des Arbeitgebers .....	433
I. Arbeitsrecht .....	433
II. Datenschutzrecht .....	434
1. Einwilligung .....	434
2. Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO .....	435
3. Art. 9 Abs. 2 lit. b, f und h DS-GVO .....	435
4. Einzelfälle .....	437
F. Datenabgleich zu Compliance-Zwecken .....	439
I. Datenabgleich nach bisherigem Recht .....	441
1. Aufdeckung von Ordnungswidrigkeiten und schwerwiegenden Pflichtverletzungen statt von Straftaten .....	442



	Seite
2. Präventive Kontrollen; Verhinderung statt Aufdeckung .....	443
II. Datenabgleich unter der DS-GVO .....	443
<b>G. Videoüberwachung am Arbeitsplatz .....</b>	<b>445</b>
I. Videoüberwachung nach bisherigem Recht .....	445
1. Videoüberwachung von Arbeitsplätzen in öffentlich zugängli- chen Bereichen .....	445
2. Videoüberwachung von Arbeitsplätzen in öffentlich nicht zu- gänglichen Betriebsbereichen .....	445
3. Videoüberwachung im öffentlichen Raum außerhalb des Ar- beitsplatzes .....	446
II. Videoüberwachung unter der DS-GVO .....	446

**Kapitel 2. „Bring Your Own Device“ und Datenschutz**

<b>A. Einleitung .....</b>	<b>449</b>
<b>B. BYOD und die rechtlichen Implikationen .....</b>	<b>449</b>
I. Erscheinungsformen des BYOD .....	449
1. Nutzung privater IT zu dienstlichen Zwecken .....	449
2. Unechtes BYOD .....	451
II. BYOD im rechtlichen Kontext .....	451
1. Gewerbliche Schutzrechte .....	451
2. Arbeitsrecht .....	452
3. Handels- und steuerrechtliche Dokumentations- und Aufbewah- rungspflichten .....	453
4. Datenschutz .....	453
III. BYOD und Datenschutz .....	453
1. Anwendbarkeit datenschutzrechtlicher Vorschriften .....	453
2. Kontrollrechte und -pflichten .....	456
3. Einführung des BYOD im Unternehmen .....	459
4. Skandalisierungspflicht .....	460
<b>C. Zusammenfassung .....</b>	<b>461</b>

**Kapitel 3. Datenschutz und Mitbestimmung**

<b>A. Einleitung .....</b>	<b>466</b>
<b>B. Überblick über die Gesetzessituation .....</b>	<b>467</b>
I. Mitbestimmungsregelungen im Datenschutzrecht? .....	467
1. Begriffe: „Verdatungsschutz“ und Datensicherheit .....	467
2. Was regelt die DS-GVO zum Umgang mit Beschäftigtendaten? .....	468
II. Datenschutzregelungen im Mitbestimmungsrecht? .....	471
1. Überblick .....	471
2. § 87 Abs. 1 Nr. 6 BetrVG: Mitbestimmung (nur) bei Leistungs- oder Verhaltensdaten .....	472
3. Anwendungsbereich des BetrVG .....	475



	Seite
4. Ergänzend: Individualrechte im BetrVG .....	475
III. Wo liegt die Schnittmenge zwischen Datenschutz und Mitbestimmung? .....	476
<b>C. Datenschutz in Betriebsvereinbarungen</b> .....	478
I. Überblick .....	478
II. Datenschutzregelungen in Betriebsvereinbarungen: Was ist zu beachten? .....	479
1. Was sind „spezifischere Vorschriften“ gemäß Art. 88 Abs. 1 DS-GVO? .....	479
2. Dürfen „spezifischere Vorschriften“ das Schutzniveau der DS-GVO unterschreiten? .....	480
3. Dürfen „spezifischere Vorschriften“ das Schutzniveau der DS-GVO überschreiten? .....	481
4. Spezifischere Vorschriften als Rechtsgrundlage für Datenverarbeitung? .....	482
5. Schaffen von „geeigneten und besonderen Maßnahmen“ nach Art. 88 Abs. 2 DS-GVO .....	485
III. Sonderfall: Einigungsstellenspruch .....	489
IV. Sind bestehende Betriebsvereinbarungen anzupassen? .....	490
V. Checkliste .....	491
<b>D. Datenschutz bei der Datenverarbeitung durch den Betriebsrat</b> .....	492
I. Datenschutzrechtliche Erlaubnis für die Datenverarbeitung durch den Betriebsrat .....	492
II. Vom Betriebsrat einzuhaltende datenschutzrechtliche Begleitpflichten .....	494
<b>E. Kontrollrechte des Datenschutzbeauftragten beim Betriebsrat</b> .....	495

## Kapitel 4. Sozialdatenschutz

<b>A. Bedeutung des Sozialdatenschutzes für Arbeitnehmer</b> .....	501
<b>B. Das System des Sozialdatenschutzes</b> .....	501
I. Rechtsgrundlagen .....	501
1. Nationales Verfassungsrecht .....	501
2. EU-Rechtsrahmen .....	502
3. Nationale Rechtsgrundlagen .....	505
II. Sozialgeheimnis .....	511
III. Änderungen der Terminologie .....	512
1. Verarbeiten .....	512
2. Erheben, Übermitteln und Nutzen .....	513
IV. Begriff der Sozialdaten .....	513
1. Allgemeines .....	513
2. In § 35 SGB I genannte Stellen .....	514
3. Zweckbindung .....	515



	Seite
4. Betriebs- und Geschäftsgeheimnisse .....	515
5. Anonymisierte und pseudonymisierte Daten .....	516
6. Gutachten als Sozialdaten .....	516
V. Verlängerter Sozialdatenschutz .....	517
VI. Zweckändernde Datenverarbeitung .....	518
1. Zweckbindungsgrundsatz .....	518
2. Zweckändernde Verarbeitung .....	518
VII. Technische Vorkehrungen .....	521
<b>C. Verarbeitung auf Grundlage einer Einwilligung .....</b>	<b>522</b>
I. Bedeutung der Einwilligung nach DS-GVO .....	522
II. Höchstpersönlichkeit, Mindestalter .....	523
III. Form der Einwilligung .....	524
IV. Freiwilligkeit .....	524
V. Auswirkungen auf Mitwirkungspflichten .....	525
<b>D. Erheben von Sozialdaten .....</b>	<b>527</b>
I. Begriff des Erhebens .....	527
II. Erforderlichkeit der Erhebung .....	529
1. Allgemeines .....	529
2. Gebot der Transparenz und der Direkterhebung .....	529
3. Erhebung auf Vorrat .....	534
4. Die Erhebung spezifischer Daten .....	535
5. Unzulässige Erhebungsmethoden .....	537
<b>E. Speichern, Verändern, Übermitteln, Einschränkung der Verarbeitung     oder Löschen .....</b>	<b>538</b>
I. Allgemeines .....	538
II. Übermitteln von Daten .....	539
1. Abgrenzung Übermittlung/Nutzung .....	539
2. Voraussetzungen einer Übermittlungsbefugnis .....	540
3. Verhältnismäßigkeit der Übermittlung .....	543
4. Aktenübersendung an Sozialgerichte .....	544
5. Übermittlung ohne Einwilligung oder normative Befugnis .....	544
6. Verantwortung für die Übermittlung .....	545
7. Übermittlungsbeschränkung bei der Geheimhaltung unterlie- genden Daten .....	545
8. Übermittlungen ohne Ersuchen .....	546
<b>F. Verarbeitung von Sozialdaten im Auftrag .....</b>	<b>548</b>
<b>G. Betroffenenrechte und Einschränkungen .....</b>	<b>553</b>
I. Systematik .....	553
II. Informationspflichten .....	553
1. Anlass und Inhalt der Pflicht .....	553
2. Beschränkungen bei Direkterhebung .....	554
3. Beschränkung bei Dritterhebung .....	555



	Seite
III. Auskunftsrecht .....	556
1. Inhalt .....	556
2. Beschränkungen .....	556
IV. Widerspruchsrecht .....	557
1. Voraussetzungen .....	557
2. Beschränkungen .....	557
V. Recht auf Berichtigung .....	558
VI. Recht auf „Vergessenwerden“ .....	558
VII. Recht auf Einschränkung der Verarbeitung .....	559
1. Voraussetzungen .....	559
2. Beschränkungen .....	559
VIII. Recht auf Datenübertragbarkeit .....	560
H. Aufsichtsbehörden .....	560
I. Allgemeines .....	560
II. Befugnisse der datenschutzrechtlichen Aufsichtsbehörden .....	560
I. Der Datenschutzbeauftragte .....	561
J. Sanktionsnormen .....	562
K. Datenschutz im sozialgerichtlichen Verfahren .....	562
I. Geltung des Datenschutzes auch im Gerichtsverfahren .....	562
II. Geltung der DS-GVO im Gerichtsverfahren .....	563
III. Die in Betracht kommenden Datenschutznormen .....	563
IV. Datenschutz innerhalb desselben Gerichts .....	564
V. Übermittlung von Daten außerhalb des Sozialgerichtsprozesses .....	565
VI. Konsequenzen von Verstößen gegen das Recht auf informationelle Selbstbestimmung .....	566
VII. Neue Zuständigkeiten der Sozialgerichtsbarkeit .....	567
1. Fallgestaltungen .....	567
2. Sachliche Zuständigkeit der Sozialgerichtsbarkeit .....	567
3. Örtliche Zuständigkeit .....	568
<b>Annex: Rechtslage in Österreich</b>	
A. Ausgangslage .....	570
B. Überwachungs- und Einsichtsrechte .....	571
C. Betriebliche Mitbestimmung .....	571

## Teil VI. Datenschutz in Betrieb, Unternehmen und Konzern

### Kapitel 1. Konzerndatenschutz

A. Fehlendes Konzernprivileg .....	576
I. Konzern, Unternehmensgruppe, Relevanz für Aufsicht .....	576



	Seite
II. Datenverarbeitung im Konzern, Zulässigkeitsnorm .....	579
III. Alternativen, Erweiterungen .....	581
1. Auftragsverarbeitung im Konzern, außerhalb der EU .....	581
2. Gemeinsame Verantwortlichkeit (Art. 26 DS-GVO) .....	582
3. Einwilligung .....	586
4. Konzernbetriebsvereinbarung und Zuständigkeit des Konzernbetriebsrats .....	588
<b>B. Der Weg zur Zulässigkeit über Art. 6 Abs. 1 lit. f DS-GVO, Abwägungsmodell .....</b>	<b>589</b>
I. Art. 5 DS-GVO .....	589
II. Art. 6 DS-GVO .....	590
III. Das Problem des Art. 9 DS-GVO, § 26 Abs. 3 BDSG .....	590
<b>C. Besondere Situationen .....</b>	<b>591</b>
I. Zentrale Personalverwaltung, Matrix .....	591
II. Umwandlungen, Verschmelzungen, M&A/Due Diligence .....	593
III. Revisionen .....	593
IV. Compliance für IT-Sicherheit .....	596
<b>D. Neue Technologien, Industrie 4.0, Social Media und Ähnliches .....</b>	<b>597</b>
<b>E. Konzerndatenschutzbeauftragter .....</b>	<b>597</b>

## Kapitel 2. Internationaler Datenverkehr

<b>A. EU-Datenschutz für den Datentransfer ins Ausland .....</b>	<b>600</b>
<b>B. Datenschutz im Geschäftsverkehr mit den Vereinigten Staaten/außerhalb der EU .....</b>	<b>603</b>
I. EU-US Privacy Shield .....	604
II. Standardvertragsklauseln .....	608
III. Binding Corporate Rules (BCR) .....	610
<b>C. Outsourcing .....</b>	<b>611</b>
<b>D. Vertragsgestaltung im internationalen Datenverkehr .....</b>	<b>612</b>

## Kapitel 3. Präventive Compliance und Whistleblowing im Konzern

<b>A. Einleitung .....</b>	<b>620</b>
<b>B. Allgemeine Vorgaben für eine Compliance-Organisation .....</b>	<b>620</b>
<b>C. Elektronische Systeme zur präventiven Compliance .....</b>	<b>622</b>
I. Verpflichtung zur Vorhaltung von Systemen und Daten? .....	622
1. Allgemeine Compliance-Vorgaben .....	622
2. Vorgaben für Banken, Versicherungen und Wertpapierdienstleistungsunternehmen .....	623
II. Allgemeine Vorgaben zum Zugriff auf Daten bei Datenabgleichen ...	624



	Seite
1. Allgemeine Vorgaben der DS-GVO und des BDSG zur präventiven Compliance .....	624
2. Datenabgleiche beschränkende Sondernormen .....	628
3. Mitbestimmungsrecht des Betriebsrats .....	630
4. Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung und zur Information des betrieblichen Datenschutzbeauftragten .....	630
5. Pflicht zur Information der Betroffenen .....	631
6. Sanktionen bei Verletzung des Datenschutzrechts .....	631
III. Empfehlungen für die Praxis .....	632
1. Begrenzungen des automatisierten Datenabgleichs .....	632
2. Trennung von dienstlichen und privaten E-Mails .....	634
3. Abschluss von Betriebsvereinbarungen .....	635
D. Whistleblowing-Systeme .....	636
I. Einleitung .....	636
II. Aufbau eines Whistleblowing-Systems .....	636
III. Inhaltlicher Anwendungsbereich .....	637
IV. Datenschutzrechtliche Vorgaben .....	638
1. Einwilligung .....	638
2. Anforderungen an Aufnahme und Verarbeitung von Hinweisen außerhalb der Einholung von Einwilligungen .....	639
3. Anonymität des Hinweisgebers .....	641
4. Einbindung eines externen Ombudsmanns .....	642
5. Übermittlung an andere Konzerngesellschaften .....	642
6. Sonstige datenschutzrechtliche Anforderungen .....	643
7. Einbindung des Datenschutzbeauftragten und Durchführung einer Datenschutz-Folgenabschätzung .....	645
8. Einbindung des Betriebsrats und Betriebsvereinbarung .....	645
V. Empfehlungen für die Praxis .....	645
E. System zur Data Breach Notification nach Art. 33 f. DS-GVO .....	646
F. Stellung des Datenschutzbeauftragten im Verhältnis zum Compliance-Beauftragten .....	648
I. Einleitung .....	648
II. Rechtliche Anforderungen an Aufgabe und Stellung des Datenschutzbeauftragten .....	649
III. Rechtliche Anforderungen an Aufgabe und Stellung des Compliance-Beauftragten .....	650
IV. Bewertung .....	651
<b>Kapitel 4. Datenschutz in der Unternehmenstransaktion</b>	
A. Einleitung .....	656
B. Datenschutzrechtlicher Rahmen für die Übermittlung von personenbezogenen Daten an Interessenten und deren Berater .....	657
I. Beschäftigtendaten .....	657



	Seite
1. Einwilligung .....	657
2. Betriebsvereinbarungen .....	659
3. Zulässigkeit nach Art. 6 DS-GVO, § 26 BDSG .....	660
II. Kunden- und Lieferantendaten .....	663
III. Besondere personenbezogene Daten .....	663
IV. Durch Sondernormen geschützte Daten .....	664
V. Sanktionen bei Verletzung des Datenschutzrechts .....	664
<b>C. Übermittlung von personenbezogenen Daten im Rahmen der Due Diligence und Verhandlungen .....</b>	<b>664</b>
I. Grundsätze der Zulässigkeitsprüfung .....	665
II. Daten der Vorstände bzw. Geschäftsführer .....	666
III. Beschäftigtendaten .....	667
IV. Kunden- und Lieferantendaten .....	667
<b>D. Übermittlung von personenbezogenen Daten in der Phase zwischen Signing und Closing .....</b>	<b>668</b>
<b>E. Übermittlungen von personenbezogenen Daten nach dem Closing .....</b>	<b>669</b>
I. Share Deal .....	669
II. Asset Deal .....	670
III. Unternehmenserwerb durch Verschmelzung oder Abspaltung .....	672
<b>F. Vorbereitung der Unternehmenstransaktion .....</b>	<b>673</b>
I. Vorbereitung von Listen .....	674
II. Abschluss von Vertraulichkeitsvereinbarungen .....	674
1. Allgemeines .....	674
2. Drittlandtransfer .....	675
III. Abschluss eines Auftragsverarbeitungsvertrags mit Datenraum- anbietern .....	676
IV. Einbindung des betrieblichen Datenschutzbeauftragten .....	676
V. Einbindung des Betriebsrats .....	677
VI. Benachrichtigung der Betroffenen .....	677
1. Allgemeines .....	677
2. Informationspflichten der Zielgesellschaft .....	677
3. Informationspflichten der Interessenten bzw. des Erwerbers .....	678
4. Ausnahmen der DS-GVO von den Informationspflichten .....	678
5. Ausnahmen des BDSG von den Informationspflichten .....	680

### Annex: Rechtslage in Österreich

<b>A. Konzerndatenschutz .....</b>	<b>681</b>
I. Grundlagen des Konzerndatenschutzes .....	681
II. Konzerninteresse .....	682
III. Datenverarbeitung im Konzern auf Basis von Betriebsvereinbarungen .....	683
IV. Entfall der Meldepflicht .....	684



	Seite
<b>B. Präventive Compliance</b> .....	684
I. Interne Compliance-Untersuchungen .....	684
II. Whistleblowing-Hotlines .....	685
<b>C. Datenschutz in der Unternehmenstransaktion</b> .....	686

## Teil VII. Outsourcing und neue Technologien als Herausforderung für den Datenschutz

### Kapitel 1. Outsourcing

<b>A. Vergabe von Aufträgen</b> .....	690
I. Begriff .....	690
II. Formen .....	691
III. Verhandlung, Auftragserteilung, Vergabe .....	693
IV. Cloud-Besonderheiten .....	695
V. Big Data .....	698
<b>B. SLA-Gestaltung im Hinblick auf den Datenschutz</b> .....	700
<b>C. Transition und Betriebsübergang, Retransition</b> .....	705

### Kapitel 2. Auftrags(daten)verarbeitung

<b>A. Vorbemerkung, Übergang, Wegfall der „Privilegierung“?</b> .....	710
I. Einführung .....	710
II. Neue Aspekte .....	711
III. Fragen der Umstellung, Konkretisierung .....	713
IV. Definitionen, Anwendung .....	714
V. Übergang/Delta .....	716
1. Abrupter Übergang .....	716
2. Überarbeitungsbedarf .....	717
VI. Wegfall oder Verringerung der „Privilegierung“? .....	718
1. Was wird aus der „Funktionsübertragung“? .....	718
2. Keine direkte Übertragung der BDSG-Interpretation .....	720
3. Grundlage: der Vertrag .....	720
<b>B. Auftragsverarbeitung gemäß DS-GVO</b> .....	721
I. Anwendungsbereich .....	721
II. Beispielsfälle .....	724
III. Auswahlverantwortung des Verantwortlichen .....	728
1. Hauptkriterium: technische und organisatorische Maßnahmen, Garantien .....	728
2. Garantien (Art. 28 Abs. 5 DS-GVO), Verhaltensregeln und Zer- tifizierungsverfahren .....	729
3. Technische und organisatorische Maßnahmen .....	730



	Seite
4. Verbleibende Verantwortlichkeit des Auftragsverarbeiters .....	732
5. Auftragskette, Subunternehmer .....	732
<b>C. Der Vertrag .....</b>	<b>733</b>
I. Vertragsthemen, Vertragsinhalte, „Minimum“ .....	733
1. Kerninhalt des Vertrags .....	733
2. Form .....	734
II. Mindestinhalt des Vertrags .....	734
1. Verarbeitung auf Basis dokumentierter Weisung (Art. 28 Abs. 3 S. 2 lit. a DS-GVO) .....	734
2. Verpflichtung zur Vertraulichkeit bzw. Verschwiegenheit (Art. 28 Abs. 3 S. 2 lit. b DS-GVO) .....	735
3. Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 S. 2 lit. c DS-GVO) .....	735
4. Einhaltung der Vorgaben zum Unterauftrag (Art. 28 Abs. 3 S. 2 lit. d DS-GVO) .....	737
5. Unterstützung bei der Beantwortung von Anträgen (Art. 28 Abs. 3 S. 2 lit. e DS-GVO) .....	738
6. Unterstützung bei den Pflichten nach Art. 32–36 DS-GVO (Art. 28 Abs. 3 S. 2 lit. f DS-GVO) .....	739
7. Löschung oder Rückgabe nach dem Ende der Verarbeitungsleistung (Art. 28 Abs. 3 S. 2 lit. g DS-GVO) .....	739
8. Zurverfügungstellung von Informationen und Unterstützung von Überprüfungen (Art. 28 Abs. 3 S. 2 lit. h DS-GVO) .....	740
<b>D. Weitere Pflichten im Vertragsverhältnis .....</b>	<b>740</b>
I. Hinweise, Prüfung .....	740
II. Datenschutzbeauftragter .....	741
III. Aufsicht .....	743
IV. Haftung, Bußgeld .....	744
<b>E. Auslandsübermittlung .....</b>	<b>746</b>
I. Nicht-EU-Ausland .....	746
II. EU-Standardvertragsklauseln .....	747
III. Binding Corporate Rules (BCR) .....	748
IV. Safe Harbor, Privacy Shield (Adäquanz-Entscheidung), Cloud-Besonderheiten .....	750
<b>F. Spezialthema Cloud .....</b>	<b>752</b>
 <b>Kapitel 3. Customer Relationship Management und Datenschutz</b>	
<b>A. Customer Relationship Management – Pflege und Profilbildung als betriebswirtschaftliches Instrument .....</b>	<b>756</b>
<b>B. CRM und Datenschutz .....</b>	<b>757</b>
I. Grundsatz .....	757
II. Gegenstand des CRM – personenbezogene Daten .....	758



	Seite
III. Erfordernis der Einwilligung .....	759
IV. Hinweispflicht .....	762
V. Gesetzlicher Erlaubnistatbestand .....	762
1. Einwilligung .....	763
2. Erfüllung eines Vertrags .....	764
3. Durchführung vorvertraglicher Maßnahmen .....	764
4. Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten .....	768
5. Allgemein zugängliche Daten .....	768
VI. Verarbeitung oder Nutzung zu Werbezwecken .....	768
1. CRM als Kundenbindungs- und Akquisemittel .....	769
2. Listenprivileg .....	769
VII. Datenpflege und -veredelung .....	770
C. CRM im Konzern .....	770

## Kapitel 4. Cloud Computing

A. Cloud Computing und Datenschutz .....	776
I. Einführung, Definition, technische Hintergründe .....	776
1. Definition und Abgrenzung .....	776
2. Basis des Cloud Computing: Virtualisierung .....	777
3. Cloud-Modelle .....	777
4. Cloud Service-Typen .....	779
5. Aspekte der Datensicherheit .....	780
II. Cloud Computing und die DS-GVO .....	782
1. Anwendungsbereich .....	782
2. Auftragsverarbeiter und Joint Controller .....	783
3. Anforderungen an die Informationssicherheit .....	786
4. Besondere Kategorien personenbezogener Daten in der Cloud ...	787
5. Haftung für Datenschutzverstöße .....	787
6. Datenübermittlung in Drittländer .....	787
7. Notwendigkeit von Datenschutz-Folgenabschätzungen .....	788
8. Löschung von Daten und Einschränkung der Verarbeitung .....	789
9. Recht auf Datenübertragbarkeit .....	790
10. Meldepflichten .....	790
III. Lösungsansätze .....	791
1. Bedeutung von Zertifikaten und Verhaltensregeln .....	791
2. Verschlüsselung von personenbezogenen Daten in der Cloud ....	792
3. Nutzung von Trusted Computing-Technologien .....	794
4. Löschen von Daten in der Cloud .....	795
5. Nutzung von Private Clouds .....	795
IV. Fazit .....	796
B. Transnationale Clouds .....	797
I. Die transnationale Dimension des Cloud Computing .....	799



	Seite
II. Anwendbares Datenschutzrecht bei transnationalen Clouds .....	799
1. Cloud Provider mit Niederlassung im Inland .....	801
2. In einem anderen EU-Mitgliedstaat belegener Cloud Provider ...	803
3. In einem Drittland belegener Cloud Provider .....	803
III. Auftragsdatenverarbeitung unter Beteiligung von Cloud Providern in Drittländern .....	805
1. Cloud Provider als Auftragnehmer in einem Drittland .....	805
2. Cloud Provider oder Nutzer als Auftraggeber in einem Dritt- land .....	805
IV. Weitergabe personenbezogener Daten an Cloud Provider im Aus- land .....	806
1. Voraussetzungen .....	806
2. Angemessenes Datenschutzniveau im Empfängerland .....	806
3. Kein angemessenes Datenschutzniveau im Empfängerland .....	806
4. Zulässigkeit der Übermittlung .....	814

Kapitel 5. Cyberwar und Datenschutz

A. Vernetzung .....	817
I. Einführung .....	817
II. Gesetzliche Grundlagen .....	818
III. Code is Law .....	820
IV. Cyber-Terrorismus .....	821
B. Der Datenschutzbezug, vor allem über Sicherheit und Prävention .....	822
I. Informationssicherheit .....	822
II. Datenbevorratung .....	823
III. Cyberwar- und Spionageabwehr .....	824
IV. Aufgabenstellung .....	825
V. Sensible Schwachstellen .....	826
VI. Mitarbeiter .....	827
VII. Whistleblowing .....	829
VIII. Auftragsverarbeitung .....	830
IX. Sicherheitsüberprüfungen .....	831
X. Datenschutz-Folgenabschätzung (DS-GVO) .....	834
C. Haftung, sicherheitsrechtlicher Rahmen .....	836

Kapitel 6. Smart Metering und E-Mobility

A. Einleitung .....	846
B. Grundlagen des Smart Metering und der E-Mobility .....	847
I. Technische Grundlagen und Begriffsbestimmungen des Smart Metering und der E-Mobility .....	847



	Seite
II. Wesentliche Anwendungsgebiete des Smart Metering und der E-Mobility .....	849
III. Sektorspezifische rechtliche Grundlagen des Smart Metering und der E-Mobility .....	849
<b>C. Datenschutz beim Smart Metering und der E-Mobility .....</b>	<b>850</b>
I. Verhältnis des MsbG zur DS-GVO .....	850
II. Art und Umfang der betroffenen personenbezogenen Daten .....	852
1. Art der betroffenen personenbezogenen Daten .....	852
2. Umfang der betroffenen personenbezogenen Daten .....	853
III. Berechtigte Stellen .....	854
IV. Anwendbare allgemeine datenschutzrechtliche Grundsätze, insbesondere Datenminimierung .....	855
V. Sektorspezifische datenschutzrechtliche Regelungen im Bereich des Smart Metering .....	856
1. Verarbeitung personenbezogener Daten in bestimmten Anwendungsfällen .....	856
2. Auskunft-, Einsichts- und Informationspflichten .....	861
3. Löschungspflichten und weitere Betroffenenrechte .....	863
4. Datenschutz-Folgenabschätzung .....	864
5. Sanktionen .....	865
VI. Besondere datenschutzrechtliche Probleme der E-Mobility .....	865
1. Bewegungsprofile .....	866
2. Authentifizierung und Datenübermittlung .....	866
<b>D. Datensicherheit beim Smart Metering und der E-Mobility .....</b>	<b>867</b>
I. Allgemein zu berücksichtigende Grundsätze der Datensicherheit .....	869
II. Zertifizierungspflichten .....	870
1. Zertifizierungspflicht des Smart-Meter-Gateways .....	870
2. Zertifizierungspflicht des Smart-Meter-Gateway-Administrators .....	871
III. Spezielle Anforderungen an das Smart-Meter-Gateway .....	872
IV. Spezielle Anforderungen an das Sicherheitsmodul .....	873
<b>Annex: Rechtslage in Österreich</b>	
<b>A. Smart Metering und E-Mobility .....</b>	<b>875</b>
I. Übermittlung und Verarbeitung der erhobenen Verbrauchsdaten .....	876
II. Auftragsdatenverarbeitung .....	878
<b>B. Cyberwar und Datenschutz .....</b>	<b>878</b>
<b>Teil VIII. Datenschutz in verschiedenen Kommunikationsformen</b>	
<b>Kapitel 1. Datenschutz im Internet</b>	
<b>A. Internetregulierung in Deutschland .....</b>	<b>882</b>
I. Vom IuKDG zum TMG .....	883



	Seite
II. Personenbezug von IP-Adressen .....	884
1. Objektiver Personenbezug .....	884
2. Relativität des Personenbezugs .....	885
3. Infektionstheorie .....	887
4. Bewertung durch den EuGH .....	888
5. IP-Adressen von internen Rechnern .....	888
6. Bewertung von IPv6.....	888
7. Personenbezug von IP-Adressen in der DS-GVO.....	889
<b>B. Das Telemediengesetz .....</b>	<b>889</b>
I. Überblick .....	890
II. Anwendungsbereich .....	890
1. Begriff der Telemedien .....	890
2. Ausnahme für dienstliche Telemediennutzungen .....	891
III. Zentrale Vorschriften .....	892
1. Datenverarbeitungsverbot mit Erlaubnisvorbehalt .....	892
2. Spezielle Erlaubnisvorschriften .....	892
3. Einwilligung des Nutzers .....	893
4. Sonstige Sonderregelungen .....	893
 <b>Kapitel 2. Web 2.0, Mobile Apps und die datenschutzrechtlichen Anforderungen</b>	
<b>A. Einführung .....</b>	<b>896</b>
I. Zu den Ergänzungen dieses Kapitels in dieser Auflage .....	896
II. Datenschutzrechtliche Besonderheit plattformbetriebener Inhalte ....	898
<b>B. Rechtsverhältnisse und Konstellationen .....</b>	<b>901</b>
<b>C. Rechtsgrundlagen .....</b>	<b>901</b>
I. Europäische Rechtsgrundlagen .....	901
II. Deutsche Rechtsgrundlagen .....	903
1. Allgemeines Datenschutzrecht .....	903
2. Besonderes Datenschutzrecht .....	903
<b>D. Rechtliche Einordnung von Web 2.0-Diensten .....</b>	<b>905</b>
I. Telemediendienste .....	905
II. Telekommunikationsdienste .....	905
1. Übertragung lediglich beim selben Provider .....	905
2. Aufspaltung von Web 2.0-Dienstebündeln in Einzeldienste .....	906
3. Klassifizierung einzelner Dienste im Web 2.0 .....	907
III. Telekommunikationsgestützte Dienste (§ 3 Nr. 25 TKG) .....	907
IV. Rundfunk und telemedienrechtliche Vorschriften im RStV .....	908
V. Zusammenfassende Einordnung und Ausblick auf die DS-GVO .....	909
VI. Zivilrechtliche Regelungen .....	909
<b>E. Personenbezogene Daten im Web 2.0 .....</b>	<b>909</b>
<b>F. Datenschutzrechtliche Verantwortlichkeit im Web 2.0 .....</b>	<b>910</b>



	Seite
I. Erwägungen der Artikel-29-Datenschutzgruppe .....	911
II. Erwägungen des EuGH .....	913
III. Einzelfälle im Web 2.0 .....	913
1. Plattformbetreiber .....	914
2. Plattformnutzer .....	914
3. Dritte (Anbieter von Software/Apps) .....	917
<b>G. Das datenschutzrechtliche Verhältnis zwischen Plattformbetreiber und Nutzer .....</b>	<b>917</b>
I. Die telemedienrechtlichen Anforderungen .....	917
1. Zulässigkeit der Datenverarbeitung durch den Plattformbetreiber .....	917
2. Einwilligung .....	922
3. Nutzungsvertrag, AGB und Privacy Policy (Datenschutzerklärung) .....	928
4. Sonstige Pflichten des Plattformbetreibers .....	929
II. Die telekommunikationsrechtlichen Anforderungen .....	930
III. Recht auf Datenportabilität .....	931
IV. Pflichten des Plattformbetreibers gegenüber Dritten (Betroffenen) ...	932
<b>H. Das datenschutzrechtliche Verhältnis zwischen Nutzern und anderen Nutzern/Dritten .....</b>	<b>932</b>
<b>I. Ausblick und Würdigung .....</b>	<b>933</b>
 <b>Kapitel 3. Datenschutz in der Telekommunikation</b>	
<b>A. Vorbemerkung .....</b>	<b>937</b>
<b>B. Wesentliche Regelungen des TKG zum Datenschutz .....</b>	<b>938</b>
I. Grundsätzliche Anwendung (§ 91 TKG) .....	939
1. Einleitung .....	939
2. Adressaten des § 91 TKG .....	940
3. Lex specialis TKG .....	941
4. Zusammenfassung zu § 91 TKG .....	942
II. Datenübermittlung an ausländische nicht öffentliche Stellen (vormals § 92 TKG 2004, aufgehoben) .....	942
III. Informationspflichten (§ 93 TKG) .....	942
1. Grundsätze der Informationspflichten .....	942
2. Inhalt der Informationspflichten nach Abs. 1 .....	943
3. Wahlrecht bei Verkehrsdaten .....	943
4. Informationspflicht in Risikofällen .....	944
5. Auskunftsrecht juristischer Personen .....	945
6. Unentgeltlichkeit und Schriftlichkeit der Auskunft .....	945
7. Unrechtmäßige Erlangung von Daten .....	945
IV. Einwilligung im elektronischen Verfahren gemäß § 94 TKG .....	945
V. Nutzung von Bestandsdaten gemäß § 95 TKG .....	946



	Seite
1. Bestandsdatennutzung .....	946
2. Bestandsdaten .....	946
3. Speicherung von Bestandsdaten .....	947
4. Speicherung für Werbung, Marketing .....	947
5. Datenspeicherung nach Vertragsende gemäß § 95 Abs. 3 TKG ..	947
6. Vorlage eines amtlichen Ausweises .....	947
VI. Verkehrsdaten (§ 96 TKG) .....	948
1. Fernmeldegeheimnis .....	948
2. Auswertung von Verkehrsdaten .....	949
3. Verwendung von Verkehrsdaten .....	949
4. Sonderproblem des § 101 UrhG .....	950
VII. Entgeltermittlung und -abrechnung (§ 97 TKG) .....	951
1. Grundsätze .....	951
2. Faktische Beweislastumkehr bei Löschung von Verkehrsdaten ...	953
3. Austausch von Daten zwischen Anbietern (Interconnection) .....	953
VIII. Standortdaten (§ 98 TKG) .....	953
1. Einleitung .....	953
2. Notrufnummern und Standortdaten .....	954
IX. Einzelverbindungs nachweis (§ 99 TKG) .....	954
1. Einzelverbindungs nachweise im Haushalt und in Betrieben/ Behörden .....	954
2. Wahlrecht des Teilnehmers .....	955
X. Störung von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten (§ 100 TKG) .....	955
XI. Mitteilen ankommender Verbindungen (§ 101 TKG) .....	956
1. Einleitung .....	956
2. Verfahren „Fangen“ .....	957
XII. Rufnummernanzeige und -unterdrückung (§ 102 TKG) .....	957
XIII. Automatische Anrufweiterschaltung (§ 103 TKG) .....	958
XIV. Teilnehmerverzeichnisse (§ 104 TKG) .....	958
XV. Auskunftserteilung (§ 105 TKG) .....	959
XVI. Telegrammdienst (§ 106 TKG) und Nachrichtenübermittlungssys- teme mit Zwischenspeicherung (§ 107 TKG) .....	960
<b>C. Regelungen zur öffentlichen Sicherheit im Zusammenhang mit Daten- schutz in der Kommunikation .....</b>	<b>960</b>
I. Technische Schutzmaßnahmen (§ 109 TKG) .....	961
II. Datensicherheit (§ 109a TKG) .....	962
III. Überwachungsmaßnahmen (§ 110 TKG) .....	963
IV. Daten für Auskunftersuchen (§ 111 TKG) und automatisiertes Auskunftsverfahren (§ 112 TKG) .....	963
V. Manuelles Auskunftsverfahren (§ 113 TKG) .....	963
VI. Regelungen zur Vorratsdatenspeicherung (§§ 113a–113g TKG) .....	964
1. § 113a TKG .....	964
2. § 113b TKG .....	964



	Seite
3. § 113c TKG .....	965
4. § 113d TKG .....	965
5. § 113e TKG .....	965
6. § 113f TKG .....	965
7. § 113g TKG .....	966
VII. Kontrolle und Durchsetzung von Verpflichtungen (§ 115 TKG) .....	966
D. Perspektiven .....	966

#### Kapitel 4. Pflichten zur Herausgabe von und zur Auskunftserteilung über Daten

A. Einleitung .....	970
B. Herausgabe von Daten für Auskunfts- und Verzeichnisdienste .....	971
I. Inhalt des Herausgabeanspruchs .....	972
II. Arten der herauszugebenden Daten .....	972
III. Beachtung der Datenschutzvorschriften .....	973
C. Auskünfte über Urheberrechtsverletzungen .....	974
I. Voraussetzungen des Auskunftsanspruchs .....	975
1. Anspruchsberechtigte .....	976
2. Klageerhebung oder offensichtliche Rechtsverletzung .....	977
3. Tätigkeit in gewerblichem Ausmaß .....	977
4. Gerichtliche Anordnung bezüglich Verwendung von Verkehrsdaten .....	978
II. Verpflichtung zur Vorhaltung der Verkehrsdaten .....	982
1. Divergierende Judikatur zur Frage der Speicherpflicht auf Zuruf .....	983
2. Stellungnahme .....	984
3. Unvereinbarkeit der Speicherung von Verkehrsdaten auf Zuruf mit datenschutzrechtlichen Vorschriften .....	986
4. Beschränkung des Datenspeicherungsanspruchs auf konkrete Verbindungen .....	989
D. Auskünfte an Sicherheitsbehörden .....	990
I. Datenerhebungspflicht .....	990
II. Beauskunftung der Daten .....	991
1. Automatisiertes Auskunftsverfahren .....	991
2. Manuelles Auskunftsverfahren .....	992
III. Vorratsdatenspeicherung und -herausgabe .....	993

#### Kapitel 5. Social Communities und deren datenschutzrechtliche Auswirkungen auf die Unternehmenspraxis

A. Überblick .....	997
B. Einsatz als Marketing-Instrument .....	997
I. Technische und wirtschaftliche Rahmenbedingungen .....	997
II. Datenschutzkonforme Erhebung von Nutzerprofilen? .....	998



	Seite
1. Anwendbarkeit des Datenschutzrechts .....	998
2. Safe Harbor-Urteil des EuGH .....	998
3. Erhebung der Daten/Tracking .....	1001
III. Nutzung als Marketing-Instrument .....	1001
1. Auftragsverarbeitung (Art. 28 DS-GVO) .....	1002
2. Datenschutzrechtliche Zulässigkeit des „Like-Buttons“ .....	1003
3. Impressum .....	1004
4. Datenschutzerklärung bei eigenen Social Media-Netzwerken ....	1004
IV. Inhaltskontrolle .....	1004
C. Einsatz von Social Media-Plattformen als Recruiting-Instrument .....	1004
I. Rechtliche Rahmenbedingungen .....	1005
1. Aktuelle Rechtslage .....	1005
2. Frei zugängliche Quellen .....	1005
3. Soziale Netzwerke .....	1006
II. Zivilrechtliche Zugehörigkeit des Xing-Accounts .....	1006
D. Schutz des Unternehmens vor Meinungsäußerungen Dritter .....	1007
I. Rechtliche Rahmenbedingungen .....	1007
II. Datenschutzrechtliche Aspekte .....	1008
III. Social Media Policy .....	1008

**Annex: Rechtslage in Österreich**

A. Datenschutz im Internet .....	1011
B. Web 2.0, Mobile Apps und die datenschutzrechtlichen Anforderungen ...	1012
C. Social Communities und deren datenschutzrechtliche Auswirkungen auf die Unternehmenspraxis .....	1013
D. Datenschutz in der Telekommunikation .....	1014
E. Pflichten zur Herausgabe von und zur Auskunftserteilung über Daten .....	1015

**Teil IX. E-Commerce**

**Kapitel 1. Opt-in/Opt-out**

A. Bedeutung des Themas .....	1018
I. Schlagwortfunktion der Begriffe .....	1018
II. Allgemeine Charakterisierung der Begriffe .....	1019
III. Datenschutzrechtliche Relevanz des Themas .....	1020
IV. Wirtschaftliche Relevanz des Themas .....	1020
1. Kundenbindungs- und Rabattsysteme .....	1020
2. Soziale Netzwerke .....	1021
V. Rechtspolitische Aspekte des Themas .....	1022
B. Rechtsgrundlagen .....	1022



	Seite
I. Allgemeiner Hinweis .....	1022
II. Regelungen der DS-GVO .....	1022
1. Einwilligung als Zulässigkeitstatbestand .....	1022
2. Keine Sonderregelungen für Werbung und Adresshandel .....	1023
3. Art. 4 Nr. 11 DS-GVO als sedes materiae der Diskussion .....	1023
III. § 7 Abs. 2 UWG .....	1024
IV. Einwilligungserklärung als AGB-Klausel .....	1025
C. Gang der BGH-Rechtsprechung unter Geltung des BDSG a.F. ....	1026
I. Überblick .....	1026
II. Wesentliche Erkenntnisse der „Payback“-Entscheidung .....	1027
1. Darstellung der strittigen Klausel .....	1027
2. Bewertung als „Opt-out“-Klausel .....	1027
3. Unterscheidung zwischen datenschutzrechtlicher und wettbe- werbsrechtlicher Einwilligung .....	1028
4. Bewertung der datenschutzrechtlichen Einwilligung .....	1029
5. Bewertung der wettbewerbsrechtlichen Einwilligung .....	1029
6. Hinweis für die Praxis .....	1030
III. Wesentliche Erkenntnisse der „Happy Digits“-Entscheidung .....	1030
1. Darstellung der strittigen Klausel .....	1030
2. Bewertung anhand der Regelungen des BDSG a.F. ....	1030
IV. Konsequenzen der BGH-Rechtsprechung .....	1031
D. Vorlageentscheidung des BGH zur Rechtslage ab Geltung der DS-GVO	1031
I. Inhalt der Vorlageentscheidung .....	1031
II. Wesentliche Fragen im Verfahren vor dem EuGH .....	1032
1. Unterscheidung von datenschutzrechtlicher und wettbewerbs- rechtlicher Einwilligung .....	1032
2. Tatsache des Vorliegens einer Einwilligung .....	1032
3. Freiwilligkeit einer Einwilligung .....	1034
E. Gesetzlicher Erlaubnistatbestand für eine Verarbeitung zum Zwecke der Direktwerbung .....	1034
F. Widerspruchsrecht im Bereich der Direktwerbung .....	1035

## Kapitel 2. Datenweitergabe an Handelspartner und Offenlegungspflichten; Shophosting

A. Webshop-Lösungen als datenschutzrechtliche Herausforderung .....	1039
I. Thematische Einordnung und Herausforderungen der DS-GVO .....	1039
II. Shophosting und Webshop-Outsourcing als Geschäftsmodell .....	1040
III. Möglichkeiten und Grenzen von Auftragsverarbeitung .....	1042
IV. Datenschutzrechtliche Vorgaben an Offenlegungspflichten .....	1044
1. Nachbesserungsbedarf bei Auftragsverarbeitungsverträgen zwischen Online-Händlern und ihren Dienstleistern .....	1044
2. Nutzereinwilligungen selten wirksam .....	1046



	Seite
3. Informationspflicht gemäß Art. 13 DS-GVO („Datenschutzerklärung“)	1055
4. Externe Links	1062
5. Niederlassungsprinzip	1062
6. Marktortprinzip	1063
7. Datenübermittlung in die USA	1065
8. Dynamische IP-Adresse als personenbezogenes Datum	1067
<b>B. Typische Beispiele für Datenweitergabe an Partnerunternehmen im Rahmen von Webshops</b>	1068
I. Datenübermittlung an Versanddienstleister	1068
II. Datenübermittlung im Rahmen von Financial Supply Chain Management	1070
1. Zahlungsdienstleister	1071
2. Datenübermittlung an Auskunftsteien und Scoring-Anbieter	1071
3. Betrugsprävention mittels Device Profiling und Tippverhaltensprofilen	1072
4. Debitorenmanagement, Datenübermittlung an Inkassoanbieter	1074
III. Datenübermittlung zu Werbezwecken	1075
1. E-Mail-Marketing durch Full-Service-Dienstleister	1075
2. Web-Analyse mit Hilfe von Web-Analysediensten	1075
3. Behavioral Targeting und Retargeting durch Werbenetzwerke	1077
4. Social Media Plugins	1078
<b>C. Best Practice-Ansätze; Gütesiegel</b>	1080
I. Datenschutzsiegel	1080
II. Shop-Gütesiegel	1081
 <b>Kapitel 3. Bonitätsbewertung</b>	
<b>A. Kreditwesengesetz</b>	1084
I. Bonitätsbewertung und Risikosteuerung	1085
1. Scoring, Rating, Adressausfallrisiko, Bonitätsbewertung	1085
2. Verfahren der Bonitätsbewertung	1086
II. Scorewert – ein personenbezogenes Datum	1086
1. Bildung einer Vergleichsgruppe und der Bezug zum Betroffenen	1086
2. Prognosedaten und deren Personenbezug	1086
III. Abgrenzung zwischen DS-GVO, BDSG und KWG	1087
1. Scoring im Rahmen der DS-GVO	1087
2. Anwendung der Scoring-Vorschrift des BDSG	1089
3. Subsidiaritätsprinzip des § 1 Abs. 2 BDSG	1091
4. § 10 KWG als bereichsspezifische Vorschrift	1091
IV. Anwendungsbereich des § 10 Abs. 2 KWG	1092
1. Verbot mit Erlaubnisvorbehalt und die Bedeutung des § 10 Abs. 2 KWG	1092
2. Adressausfallrisiko	1092



	Seite
3. Interne Ratingsysteme .....	1092
V. Normative Voraussetzungen für die Datenerhebung und -verwendung .....	1093
1. Verantwortliche Stellen .....	1093
2. Betroffener Personenkreis .....	1093
3. Zweckbindung .....	1093
4. Privilegierung der Entwicklung und Weiterentwicklung von Ra- tingsystemen .....	1094
VI. Datenarten und Erhebungsquellen .....	1094
1. Datenarten .....	1095
2. Erhebungsquellen .....	1095
3. Internet als allgemein zugängliche Quelle .....	1096
4. Benachrichtigungspflicht .....	1097
VII. Datenübermittlung .....	1097
VIII. Zusammenfassung .....	1097
<b>B. Bonitätsbewertung im Rahmen des BDSG .....</b>	<b>1097</b>
I. Bedeutung und Wesen der Bonitätsbewertung im gegenwärtigen so- zioökonomischen Rahmen .....	1097
II. Rechtliche Beurteilung der Bonitätsbewertung aufgrund des BDSG .....	1099
1. Persönlicher Anwendungsbereich .....	1099
2. Überblick über die Rechtsgrundlagen .....	1099
3. Zulässigkeitstatbestände für einen der Bonitätsbewertung die- nenden Datenumgang .....	1100
<b>Kapitel 4. Online-Zahlungsverkehr</b>	
<b>A. Datenschutzrechtliche Normen im Online-Zahlungsverkehr .....</b>	<b>1105</b>
I. Anwendungsvorrang der Datenschutz-Grundverordnung .....	1106
II. Subsidiarität des Bundesdatenschutzgesetzes .....	1106
III. Anwendbarkeit bereichsspezifischer datenschutzrechtlicher Normen .....	1106
1. Telemediengesetz .....	1107
2. Telekommunikationsgesetz .....	1107
3. Payment Service Directive II und nationale Umsetzungsnormen .....	1107
<b>B. Personenbezogene Daten im Zahlungsverkehr .....</b>	<b>1108</b>
I. Personenbezogene Daten .....	1108
II. Maßstab für Identifizierbarkeit .....	1108
<b>C. Integration einer Zahlungsmethode .....</b>	<b>1109</b>
I. Angebot der Zahlungsart durch den Händler direkt .....	1110
1. Datenschutzhinweis und Einwilligung .....	1111
2. Erstellung Datenschutzhinweis bzw. Einwilligung .....	1113
3. Bestimmtheit/Transparenz/Hinweispflichten .....	1113
4. Aufbau eines Datenschutzhinweises .....	1115
5. Zeitpunkt .....	1117



	Seite
6. Form .....	1117
7. AGB-Kontrolle .....	1118
8. Freiwilligkeit der Einwilligung .....	1119
9. Datenkommunikation mit Auskunftfeien .....	1119
10. Verbot automatisierter Entscheidungen .....	1120
11. Scoring-Maßnahmen .....	1121
12. Zusammenarbeit mit Dienstleistern und Auskunftfeien .....	1122
II. Einsatz von Fremdsystemen .....	1123
1. Keine Auftragsverarbeitung .....	1123
2. Hinweispflichten des Händlers .....	1123
D. Rechtsfolgen bei Verstoß .....	1124
E. Zuständigkeit der Datenschutzbehörde .....	1124

Annex: Rechtslage in Österreich

A. Bonitätsprüfung .....	1125
B. Opt-in/Opt-out .....	1126
I. Unerbetene Nachrichten .....	1126
II. Zurverfügungstellung von Adressen zur Benachrichtigung und Be- fragung von betroffenen Personen .....	1127
C. Online-Zahlungsverkehr .....	1128

Teil X. Datenschutz im Gesundheitssektor

Kapitel 1. Umgang mit Patientendaten

A. Besondere Schutzbedürftigkeit von Patientendaten .....	1134
B. Die ärztliche Schweigepflicht .....	1135
C. DS-GVO und Patientendaten .....	1138
I. Allgemeines .....	1138
II. Verarbeitung besonderer Kategorien von Daten .....	1139
III. Die Funktion der nationalen Datenschutzregeln.....	1141
D. Datenverarbeitung durch den Arzt .....	1141
I. Allgemeines .....	1141
II. Erheben von Daten .....	1141
III. Speicherung .....	1144
IV. Zweckändernde Datenverarbeitung .....	1144
E. Verarbeiten von ärztlichen Daten durch Dritte .....	1147
I. Erhebung durch Sozialversicherungsträger .....	1148
II. Erhebung ärztlicher Daten durch Gerichte, insbesondere Sozialge- richte .....	1152



	Seite
1. Die Einholung ärztlicher Befundunterlagen bzw. Vernehmung von Ärzten als Zeugen .....	1152
2. Einholung medizinischer Sachverständigengutachten .....	1152
III. Erhebung von Patientendaten durch sonstige Dritte .....	1155
1. Erhebung durch öffentliche Stellen .....	1155
2. Erhebung durch nichtöffentliche Stellen .....	1155
IV. Datenspeicherung und -nutzung .....	1156
V. Übermittlung ärztlicher Daten .....	1158
1. Übermittlung von (einfachen) Patientendaten .....	1158
2. Übermittlung von medizinischen Sozialdaten .....	1159
VI. Übermittlung von medizinischen Sozialdaten für Forschung und Planung .....	1162
VII. Erhebung, Verarbeitung und Nutzung von Patientendaten als Sozialdaten durch private Dritte .....	1166
VIII. Verarbeitung auf Grundlage einer Einwilligung? .....	1168
IX. Übermittlung ohne Einwilligung oder normative Befugnis .....	1172
X. Problem des § 200 SGB VII .....	1173

## Kapitel 2. Elektronische Patientenakte

A. Elektronische Patientenakte .....	1176
I. Ziele der ePA .....	1177
II. Grundsätze bei der Verarbeitung personenbezogener Daten im Rahmen einer ePA .....	1177
III. Gesundheitsdaten als besondere Kategorie personenbezogener Daten .....	1178
IV. Verantwortlicher für die Datenverarbeitung .....	1180
V. Gesetzliche Erlaubnis für die Datenverarbeitung im Rahmen einer ePA .....	1181
1. Verarbeitung auf Grundlage von Art. 9 Abs. 2 lit. h DS-GVO und § 22 Abs. 1 Nr. 1 lit. b BDSG .....	1182
2. Verarbeitung auf Grundlage von Art. 9 Abs. 2 lit. c DS-GVO ....	1185
3. Verarbeitung auf Grundlage von Art. 9 Abs. 2 lit. g oder lit. i DS-GVO .....	1186
4. Verschwiegenheitspflicht .....	1187
VI. Einwilligung zur Verarbeitung von Daten im Rahmen einer ePA .....	1187
VII. Datensicherheit .....	1189
VIII. Weitere Anforderungen nach der DS-GVO .....	1191
B. Fazit .....	1193

## Kapitel 3. Telemonitoring

A. Datenschutzrechtliche Rahmenbedingungen bei Telemonitoring .....	1196
I. Einführung .....	1196



	Seite
II. Anwendungsgebiete .....	1196
III. Rechtlicher Kontext .....	1197
1. Grundsätzlicher rechtlicher Rahmen .....	1197
2. Relevante datenschutzrechtliche Gesetzgebung .....	1198
IV. Verarbeitung personenbezogener Daten im Rahmen des Telemonito- rings .....	1199
V. Anforderungen an die Einhaltung des Datenschutzes beim Telemoni- toring .....	1201
1. Zulässigkeit des Verfahrens .....	1201
2. Auftragsverarbeitung .....	1202
3. Rechte des Betroffenen .....	1205
VI. Würdigung und Ausblick .....	1205
<b>B. Technische und organisatorische Anforderungen im Bereich der Gesund- heitstelematik .....</b>	<b>1206</b>
I. Einführung .....	1206
II. Anwendungsgebiete .....	1207
III. Technische Infrastruktur .....	1207
IV. Schutzniveau und Datenschutz-Folgenabschätzung .....	1208
V. Sicherheit der Verarbeitung .....	1208
1. Gesetzlicher Rahmen .....	1208
2. Risikoanalyse .....	1209
3. Evaluation und Nachweis .....	1210
VI. Umsetzung der Risikobewertung .....	1210
VII. Ausblick auf die weitere Entwicklung .....	1212
<b>Annex: Rechtslage in Österreich</b>	
A. Rechtliche Grundlagen .....	1213
B. Datengeheimnis und Übermittlung von Gesundheitsdaten .....	1213
C. Elektronische Gesundheitsakten (ELGA) .....	1215
D. Amtshilfe .....	1216
E. Forschungszwecke .....	1217

## Teil XI. Information als Wirtschaftsgut

### Kapitel 1. Kundendatenschutz, Adresshandel und Direktmarketing

<b>A. Einleitung .....</b>	<b>1220</b>
I. Begriffsdefinition Kundendatenschutz .....	1220
II. Überblick .....	1221
<b>B. Definition des Begriffs „Adresshandel“ .....</b>	<b>1221</b>
I. Adressdaten .....	1222
II. Sonstige Daten .....	1222



	Seite
<b>C. Erlaubnistatbestände .....</b>	<b>1223</b>
I. Allgemeines .....	1223
II. Grundsätze .....	1223
1. Rechtsgrundlagen .....	1223
2. Praktische Umsetzung zur Nutzung von Adressdaten zu Werbe- zwecken .....	1225
III. Adresshandel des Verantwortlichen .....	1226
1. Voraussetzung .....	1226
2. (Berechtigter) Empfängerkreis .....	1227
IV. Geschäftsmäßiger Adresshandel .....	1234
1. Allgemeines .....	1234
2. Grundsätze .....	1234
3. Ergebnis .....	1235
<b>D. Direktmarketing .....</b>	<b>1235</b>
I. CRM-Systeme und Profiling .....	1235
1. CRM-Systeme .....	1235
2. Profiling .....	1236
II. Online-Marketing und Webtracking .....	1237
1. Online-Marketing .....	1237
2. Webtracking .....	1238
3. Cross-Device-Tracking und Online Behavioural Targeting .....	1238
<b>E. Fazit .....</b>	<b>1239</b>

## Kapitel 2. RFID, Smartcards und Cookies

<b>A. RFID-Chips und Smartcards .....</b>	<b>1242</b>
I. Funktionsweise von RFID-Chips und Smartcards .....	1243
1. RFID .....	1243
2. Smartcards .....	1243
3. Anwendungsgebiete .....	1243
II. Datenschutzrechtliche Zulässigkeit des Einsatzes von RFID und Smartcards sowie damit verbundene Sicherheitsrisiken .....	1244
1. Verarbeitung personenbezogener Daten .....	1244
2. Einwilligung oder gesetzliche Erlaubnis für die Datenverarbei- tung .....	1245
3. Datenschutz durch Technikgestaltung und durch datenschutz- freundliche Voreinstellungen .....	1247
4. Datenschutz-Folgenabschätzung .....	1248
5. Informationspflichten .....	1249
6. Datenschutzrechtliche Zulässigkeit typischer Anwendungsfälle ..	1250
7. Missbrauchsgefahr, Aufklärungspflichten und Haftungsrisiken ..	1253
8. Technisch-organisatorische Maßnahmen gemäß Art. 32 und Art. 5 Abs. 1 lit. f DS-GVO .....	1255
III. Aktuelle Entwicklungen und Ausblick .....	1255



	Seite
1. Kennzeichnungspflicht nach der Textilkennzeichnungsverordnung .....	1255
2. ePrivacy-Verordnung .....	1256
<b>B. Cookies</b> .....	1256
I. Cookies und der Zugriff auf Informationen, die bereits im Endgerät gespeichert sind .....	1256
II. Einwilligung in das Setzen von Cookies und den Zugriff auf Informationen, die bereits im Endgerät gespeichert sind – Umsetzung der Datenschutzrichtlinie für elektronische Kommunikation .....	1257
1. Einwilligungserfordernis und Ausnahmen .....	1257
2. Auf die Einholung der Einwilligung anwendbare Regelungen ....	1259
3. Einwilligung in der Praxis .....	1259
4. Voraussetzungen einer wirksamen Einwilligung .....	1260
5. Weitere Informationspflichten gemäß DS-GVO .....	1265
6. Sanktionen bei Verstößen gegen Vorgaben zu Cookies und Co. ....	1265
III. Verarbeitung personenbezogener Daten im Zusammenhang mit dem Einsatz von Cookies und vergleichbaren Technologien .....	1266
IV. Zulässigkeit der Verarbeitung personenbezogener Daten im Zusammenhang mit dem Einsatz von Cookies und vergleichbaren Technologien .....	1269
V. Ausblick ePrivacy-Verordnung .....	1270

### Kapitel 3. Bewertungsportale

<b>A. „Click-mich-an“: die neue soziale Währung</b> .....	1273
<b>B. Bewertung im Internet in den Grenzen des Datenschutzes</b> .....	1274
I. Allgemeine rechtliche Rahmenbedingungen .....	1274
1. Meinungsfreiheit .....	1274
2. Wettbewerbsrecht .....	1274
3. Telemedienrecht .....	1275
II. Datenschutz .....	1276
1. Anwendbarkeit datenschutzrechtlicher Vorschriften .....	1276
2. Verhältnis von TMG und datenschutzrechtlichen Regelungen ...	1277
3. Datenerhebung .....	1278
4. Berichtigung, Sperrung, Löschung .....	1279

### Kapitel 4. Datenschutzkonformer Einsatz von Suchmaschinen im Unternehmen

<b>A. Einführung</b> .....	1282
<b>B. Geschäftsmodell</b> .....	1283
<b>C. Vorbemerkungen zum Datenschutz bei Suchmaschinen</b> .....	1285
I. Anwendbarkeit der europäischen Datenschutzbestimmungen .....	1285
II. Der Klassiker: Personenbezug der IP-Adresse .....	1285



	Seite
<b>D. Einzelne Fallgestaltungen</b> .....	1287
I. Personenbezogene Mitarbeiterdaten auf der Website eines Unternehmens .....	1287
1. Veröffentlichung von Mitarbeiterdaten auf der Website .....	1287
2. Auffindbarkeit von Mitarbeiterdaten bei Suchmaschinen .....	1289
II. Google Hacking .....	1290
III. „Googeln“ von Bewerbern .....	1291
IV. Webanalyse .....	1292
1. Sinn, Anbieter und Funktionsweise .....	1292
2. Rechtliche Rahmenbedingungen .....	1292
V. Bereitstellen von Werbeflächen auf der Website eines Unternehmens .....	1296
VI. Suchmaschinen und das „Recht auf Vergessenwerden“ .....	1296
<b>E. Ergebnis</b> .....	1298

### Annex: Rechtslage in Österreich

<b>A. Adresshandel</b> .....	1299
<b>B. RFID, Smartcards und Cookies</b> .....	1300
I. RFID-Anwendungen und Smartcards .....	1300
II. Cookies .....	1301
<b>C. Werbung im Internet</b> .....	1302
<b>D. Bewertungsportale</b> .....	1303

## Teil XII. Datensicherheit

### Kapitel 1. Anforderungen an die IT-Sicherheit und deren rechtliche Grundlage

<b>A. Was bedeutet IT-Sicherheit?</b> .....	1306
I. IT-Sicherheit und Datenschutz .....	1306
II. IT-Sicherheit im Zeitalter Industrie 4.0 .....	1307
III. Komponenten einer IT-Infrastruktur .....	1307
1. Objekte .....	1308
2. Hardware .....	1308
3. Software .....	1308
4. Exkurs: Open Source Software und proprietäre Software .....	1309
5. Informations-Management .....	1309
6. Exkurs: Cloud .....	1309
<b>B. Anforderungen an die IT-Sicherheit</b> .....	1310
I. Das Informations-Sicherheits-Management-System .....	1310
II. Wesentliche Elemente eines ISMS .....	1312
1. Bedrohungsanalyse .....	1312
2. Definition der Schutzziele .....	1313



	Seite
3. Analyse der Verwundbarkeit – Risikoanalyse .....	1313
4. Definition der Maßnahmen .....	1314
5. Aufrechterhaltung der Maßnahmen im laufenden Betrieb .....	1315
<b>C. IT-Sicherheit in der DS-GVO .....</b>	<b>1316</b>
I. Einflussfaktoren .....	1317
1. Stand der Technik .....	1317
2. Implementierungskosten .....	1318
3. Art, Umfang, Umstände und Zweck der Verarbeitung .....	1318
4. Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen .....	1318
5. Mit der Verarbeitung verbundene Risiken .....	1319
II. Kategorisierung technischer und organisatorischer Maßnahmen .....	1320
<b>Kapitel 2. Technische und organisatorische Maßnahmen</b>	
<b>A. Einleitung .....</b>	<b>1322</b>
<b>B. Erläuterungen .....</b>	<b>1323</b>
I. Begrifflichkeiten .....	1323
II. Neuerungen durch die DS-GVO .....	1324
1. Risikoorientierung .....	1324
2. Datenschutz durch Technikgestaltung („data protection by design“) .....	1324
3. Datenschutz durch Voreinstellung („data protection by default“) .....	1324
III. Allgemeine Anforderungen an die Verarbeitung .....	1325
IV. Datenschutz durch Technikgestaltung und Voreinstellung .....	1326
1. Datenschutz durch Technikgestaltung .....	1326
2. Datenschutz durch Voreinstellung .....	1326
V. Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO .....	1327
VI. Sicherheit der Verarbeitung (Art. 32 DS-GVO) .....	1328
<b>C. Rechtsschutz und Verfahrensfragen .....</b>	<b>1330</b>
I. Bußgelder .....	1330
II. Schadensersatz .....	1331
III. Aufsichtsbehördliche Maßnahmen .....	1331
IV. Melde- und Benachrichtigungspflicht .....	1331
<b>D. Kritische Würdigung .....</b>	<b>1332</b>
I. Unbestimmtheit der Regelungen zur Datensicherheit .....	1332
II. Unübersichtliche Struktur der Regelungen zur Datensicherheit .....	1333
III. Risikoorientierung der DS-GVO und einheitliches Vorgehen .....	1334
IV. Durchsetzung des technisch-organisatorischen Datenschutzes .....	1335
<b>E. Datensicherheitsmaßnahmen .....</b>	<b>1335</b>
I. Zutrittskontrolle .....	1336



	Seite
II. Zugangskontrolle .....	1336
III. Zugriffskontrolle .....	1338
1. Maßnahmen der Zugriffskontrolle .....	1338
2. Maßnahmen der Speicherkontrolle .....	1339
IV. Weitergabekontrolle .....	1340
1. Maßnahmen während der Übermittlung .....	1341
2. Maßnahmen während des Transports und der Speicherung .....	1341
3. Maßnahmen zur Feststellung der Datenübermittlung .....	1342
V. Eingabekontrolle .....	1342
VI. Auftragskontrolle .....	1343
VII. Verfügbarkeitskontrolle .....	1344
VIII. Trennungsgebot .....	1345

### Kapitel 3. Schutz von Betriebs- und Geschäftsgeheimnissen

A. Einleitung .....	1348
B. Erläuterungen .....	1350
I. Entstehung des Geheimnisschutzes .....	1350
II. Mögliche Pflicht zum Geheimnisschutz aus § 91 AktG, § 43 GmbHG und § 25a KWG .....	1351
III. Maßnahmen zum Schutz von Betriebs- und Geschäftsgeheimnissen .....	1351
1. Risikoanalyse .....	1351
2. Technisch-organisatorische Maßnahmen .....	1352
3. Geheimnisträger im Unternehmen .....	1352
4. Geheimnisträger außerhalb des Unternehmens .....	1352
5. Öffentliche Auslegungsverfahren und Behördenakte .....	1352
IV. Rechtsschutz und Verfahrensfragen .....	1353
1. Strafrechtlicher Schutz .....	1353
2. Zivilrechtlicher Schutz .....	1353
V. Kritische Würdigung .....	1353
1. Konflikte mit dem Datenschutz .....	1353
2. Zusammenspiel mit dem Datenschutz .....	1355
3. Berufsgeheimnisträger .....	1355

### Kapitel 4. Überblick zu Risikomanagement unter BSIG, BSI-KritisV, NIS-RL i. V. m. DS-GVO

A. Gesetzlicher Rahmen .....	1358
I. Einführung über DS-GVO .....	1358
II. Betrieblicher und volkswirtschaftlicher Aspekt .....	1358
III. BSIG, BSI-KritisV, NIS-RL .....	1359
IV. Regulierter Bereich, v. a. Banken und Versicherungen, insbesondere Maßgaben bei Auslagerung .....	1362
B. IT-(Sicherheits-)Compliance .....	1363



	Seite
<b>C. Mittelbare Anforderungen über Ordnungsmäßigkeit und Haftung der Organe .....</b>	<b>1365</b>
<b>D. DS-GVO .....</b>	<b>1366</b>
I. Art. 24 DS-GVO .....	1366
II. Art. 32 DS-GVO .....	1366
III. Art. 35 DS-GVO – Datenschutz-Folgenabschätzung .....	1367
IV. Art. 5 Abs. 2 DS-GVO – Rechenschaftspflicht und weitere Funktionen .....	1368
1. Portabilität .....	1368
2. Informationspflichten, Widerspruchsrecht .....	1369
3. Automatisierte Entscheidungen .....	1369
4. Weitere Technikgestaltungen, Art. 24 und 25 DS-GVO .....	1369
<b>E. Konzernweite Compliance-Pflicht .....</b>	<b>1370</b>
<b>F. IT-Anwendung, typische Risikobeispiele .....</b>	<b>1371</b>
I. Auftragsverarbeitung .....	1371
II. Softwarelizenzierung .....	1371
III. Wartung, Pflege .....	1372
<b>G. Beauftragte .....</b>	<b>1373</b>

### Annex: Rechtslage in Österreich

<b>A. Allgemeines zur Datensicherheit in Österreich nach bisheriger Rechtslage .....</b>	<b>1375</b>
<b>B. Rechtliche Anforderungen an technische und organisatorische Maßnahmen .....</b>	<b>1376</b>
I. Fortführung der bisherigen Datensicherheitsmaßnahmen .....	1376
II. Datengeheimnis .....	1377
<b>C. Durchsetzung von Verletzungen der Datensicherheit .....</b>	<b>1378</b>
I. Rechtsanspruch des Betroffenen .....	1378
II. Rechtsanspruch des Mitbewerbers .....	1380

## Teil XIII. Konfliktmanagement im Datenschutz

### Kapitel 1. Umgang mit Datenschutzverletzungen

<b>A. Einleitung .....</b>	<b>1383</b>
<b>B. Bruch der Datensicherheit .....</b>	<b>1384</b>
I. Anwendungsbereich .....	1384
II. Inhalt und Form der Information .....	1385
III. Ordnungswidrigkeiten, Straftatbestand und Haftung .....	1387
<b>C. Missachtung des Datenschutzes .....</b>	<b>1387</b>
I. Straftatbestände und Ordnungswidrigkeiten .....	1387



	Seite
II. Screening und Whistleblowing .....	1389
1. Screening .....	1389
2. Whistleblowing .....	1390
D. Compliance, interne Revision und Datenschutzorganisation .....	1390
E. Kommunikation bei Datenschutzkonflikten .....	1391
I. Überblick und Empfehlungen .....	1391
II. Kommunikationsschema .....	1392
F. Fazit des Konfliktmanagements im Datenschutz .....	1393

## Kapitel 2. E-Discovery

A. Einführung .....	1395
B. Wichtige Begriffe .....	1396
C. Praktische Durchführung der E-Discovery .....	1401
I. Identifizierungsphase .....	1401
II. Sicherungsphase .....	1401
III. Sichtungsphase .....	1401
IV. Vorlegungsphase .....	1402
D. Rechtskonflikte und deren Lösung .....	1402
I. Ausgangslage: Interessens- und Rechtskonflikt für internationale Unternehmen .....	1402
II. Artikel-29-Datenschutzgruppe: Stellungnahmen WP 1/2009 und WP 262/2018 .....	1404
III. Lösungsansätze der französischen Datenschutzbehörde CNIL .....	1405
IV. Lösungsansätze der Sedona Conference .....	1405
V. Datenexporte aus Deutschland an eine US-Muttergesellschaft .....	1407
VI. E-Discovery und Schiedsverfahren .....	1409
VII. Auswirkungen der DS-GVO auf die E-Discovery .....	1409
E. Handlungsstrategien für Unternehmen in der EU .....	1411
F. Beispielfälle aus der US-Rechtsprechung .....	1414
I. Volkswagen AG v. Valdez, Texas Supreme Court, 16.11.1995 .....	1414
II. Access Data Corporation v. ALSTE Technologies GmbH, U.S. District Court for the District of Utah, 21.1.2010 .....	1415
III. In re Air Cargo Shipping Services Antitrust Litigation, Eastern District of New York, 29.3.2010 .....	1415
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 .....	1416
V. Sofaer Global Hedge Fund v. Brightpoint, Inc. and Robert J. Laikin, U.S. District Court, Southern District of Indiana, 12.11.2010 .....	1416



	Seite
VI. MeadWestvaco Corp. v. Rexam PLC, U.S. District Court, Eastern District of Virginia, 14.12.2010 .....	1416
VII. SunTrust v. United Guaranty Residential Insurance Co., U.S. District Court, Richmond, VA, 29.3.2011 .....	1417
VIII. Heraeus Kulzer GmbH v. Biomet, Inc., U.S. Court of Appeals for the 7th Circuit, 24.1.2011 .....	1417
IX. Pershing Pacific West v. Marinemax, U.S. District Court, Southern District of California, 11.3.2013 .....	1418
X. Microsoft v. United States of America, 29.8.2014 .....	1418
XI. Knight v. Henkel, U.S. District Court, Southern District of Michigan, 30.11.2017 .....	1420

### Kapitel 3. Haftungsrisiken und deren Versicherung

A. Das Schadenspotential bei Datenschutzverstößen in der modernen Wirtschaftsordnung .....	1424
B. Bedeutung der Haftung .....	1426
C. Haftung nach der DS-GVO .....	1426
I. Einleitung .....	1426
II. Sachlicher Anwendungsbereich .....	1429
III. Räumlicher Anwendungsbereich .....	1429
IV. Persönlicher Anwendungsbereich .....	1430
V. Haftung des Verantwortlichen .....	1430
1. Anspruchsvoraussetzungen .....	1430
2. Haftungsbefreiung .....	1433
3. Beweislast .....	1435
VI. Haftung des Auftragsverarbeiters .....	1435
1. Anspruchsvoraussetzungen .....	1435
2. Haftungsbefreiung .....	1436
3. Beweislast .....	1436
VII. Rechtsfolge .....	1436
VIII. Mehrheit von Schädigern .....	1436
IX. Verjährung .....	1438
X. Freizeichnung – Verzicht .....	1438
XI. Streitigkeiten .....	1438
D. Weitere Anspruchsgrundlagen .....	1439
I. Haftung aus schuldhaftem Rechtsverstoß nach § 44 Abs. 1 S. 1 i. V.m. S. 4 TKG .....	1439
1. Allgemeines: Kurzcharakteristik der Regelung – Rechtsnatur der Haftung .....	1439
2. Persönlicher Anwendungsbereich .....	1439
3. Anspruchsvoraussetzungen .....	1439



	Seite
4. Rechtsfolge: Schadensersatz – Einschränkung der Schadensersatzpflicht aufgrund von § 44a TKG .....	1440
II. Haftung aus schuldhafter Datenschutzverletzung nach den allgemeinen Regeln über unerlaubte Handlungen (§§ 823, 824, 826 BGB) ...	1441
III. Zusammentreffen mehrerer Haftungsgründe – vorvertragliche, vertragliche und nachvertragliche Haftung .....	1442
IV. Negatorische Haftung (Beseitigungs- und Unterlassungsanspruch) ...	1443
<b>E. Haftung nach BDSG a.F.</b> .....	1444
I. Haftung aus schuldhafter gesetzeswidriger Datenverwendung nach § 7 BDSG a.F. ....	1444
1. Allgemeines: Kurzcharakteristik von § 7 BDSG a.F. – Rechtsnatur der Haftung .....	1444
2. Persönlicher Anwendungsbereich .....	1445
3. Anspruchsvoraussetzungen .....	1446
4. Beweislast .....	1449
5. Rechtsfolge: Schadensersatz .....	1450
II. Haftung aus gesetzeswidriger automatisierter Datenverwendung durch öffentlich-rechtliche Unternehmen nach § 8 BDSG a.F. ....	1450
1. Allgemeines: Kurzcharakteristik von § 8 BDSG a.F. – Rechtsnatur der Haftung .....	1450
2. Persönlicher Anwendungsbereich .....	1451
3. Anspruchsvoraussetzungen .....	1451
4. Mitverschulden (§ 8 Abs. 5 BDSG a.F.) .....	1452
5. Beweislast .....	1453
6. Rechtsfolge: Schadensersatz – Einschränkung der Schadensersatzpflicht aufgrund von Abs. 2 und 3 .....	1453
7. Haftung bei vernetzten und zentralisierten Verarbeitungssystemen (§ 8 Abs. 4 BDSG a.F.) .....	1454
8. Verjährung (§ 8 Abs. 6 BDSG a.F.) .....	1454
III. Praktische Bedeutung der allgemeinen Anspruchsgrundlagen des BGB .....	1454
<b>F. Versicherung</b> .....	1455
<b>Annex: Rechtslage in Österreich</b>	
<b>A. Strategie und Taktik im Umgang mit Datenschutzverletzungen</b> .....	1457
I. „Data Breach Notification“ .....	1457
II. Straftatbestände .....	1458
<b>B. E-Discovery</b> .....	1459
<b>C. Haftungsrisiken und deren Versicherung</b> .....	1460
<b>Teil XIV. Straf- und Ordnungswidrigkeitenvorschriften im Bereich des betrieblichen Datenschutzes</b>	
<b>A. Grundlagen</b> .....	1466



	Seite
I. Überblick .....	1466
II. Blankettmerkmal vs. normatives Tatbestandsmerkmal bei § 42 BDSG .....	1469
1. Differenzierungskriterien .....	1469
2. Rechtsfolgen .....	1470
III. Gesetzlichkeitsprinzip und Bestimmtheitsgrundsatz .....	1471
1. Unionsrechtlicher Bestimmtheitsgrundsatz .....	1472
2. Nationaler Bestimmtheitsgrundsatz .....	1472
3. Anwendungsvorrang des Unionsrechts gegenüber nationalen Grundrechtsstandards? .....	1474
4. Schlussfolgerungen .....	1476
IV. Lex-mitior-Grundsatz .....	1477
V. Irrtumsproblematik .....	1478
VI. Adressaten .....	1479
VII. Besonderheiten bei Blanketten .....	1479
1. Gesetzlichkeitsprinzip. ....	1479
2. Änderung der Ausfüllungsnorm .....	1480
<b>B. Datenschutz-Grundverordnung .....</b>	<b>1480</b>
I. Bußgeldverstöße nach Art. 83 Abs. 4 DS-GVO .....	1480
1. Verstöße von Verantwortlichen und Auftragsverarbeitern (Art. 83 Abs. 4 lit. a DS-GVO) .....	1480
2. Verstöße von Zertifizierungsstellen (Art. 83 Abs. 4 lit. b DS-GVO) .....	1482
3. Verstöße der Überwachungsstelle (Art. 83 Abs. 4 lit. c DS-GVO) .....	1482
II. Bußgeldverstöße nach Art. 83 Abs. 5 DS-GVO .....	1482
1. Verstöße gegen die Grundsätze der Datenverarbeitung (Art. 83 Abs. 5 lit. a DS-GVO) .....	1482
2. Verstöße gegen die Rechte der betroffenen Person (Art. 83 Abs. 5 lit. b DS-GVO) .....	1482
3. Verstöße bei der Datenübermittlung an Drittländer oder inter- nationale Organisationen (Art. 83 Abs. 5 lit. c DS-GVO) .....	1483
4. Verstöße gegen Vorschriften für besondere Verarbeitungssitua- tionen nach Kapitel IX (Art. 83 Abs. 5 lit. d DS-GVO) .....	1483
5. Verstöße gegen Anweisungen der Aufsichtsbehörde (Art. 83 Abs. 5 lit. e und Abs. 6 DS-GVO) .....	1484
III. Vorgaben für die Verhängung von Geldbußen .....	1484
1. Allgemeines .....	1484
2. Kriterien bei der Bemessung der Höhe der Geldbuße .....	1485
IV. Unmittelbare Verbandshaftung .....	1486
1. Begriff des Unternehmens nach Art. 101 und Art. 102 AEUV ....	1487
2. Anpassung an das Datenschutzrecht .....	1489
<b>C. Sanktionen nach nationalem Recht (§§ 41 ff. BDSG) .....</b>	<b>1493</b>
I. Anwendbarkeit des OWiG nach § 41 Abs. 1 BDSG .....	1493



	Seite
II. Bußgeldtatbestände nach § 43 BDSG .....	1493
III. Kriminalstrafe nach nationalem Recht .....	1494
1. Keine allgemeine Zugänglichkeit personenbezogener Daten .....	1494
2. Strafbarkeit nach § 42 Abs. 1 BDSG .....	1495
3. Strafbarkeit nach § 42 Abs. 2 BDSG .....	1495
4. Strafantrag .....	1498
5. Rechtswidrigkeit .....	1498
6. Verschulden .....	1498
<b>D. Verfahren</b> .....	1499
I. Anwendbare Verfahrensvorschriften .....	1499
II. Beweislast .....	1500
III. Opportunitätsprinzip .....	1500
<b>E. Sanktionsvorschriften des BDSG in der Fassung bis 24.5.2018 (a.F.)</b> .....	1501
I. Anwendbarkeit .....	1501
II. Tatbestandsstrukturen und Rechtsfolgen .....	1503
1. Ordnungswidrigkeiten nach § 43 Abs. 1 BDSG a.F. ....	1503
2. Ordnungswidrigkeiten nach § 43 Abs. 2 BDSG a.F. ....	1503
3. Adressat der Bußgeldanordnung .....	1504
4. Bemessung der Geldbuße .....	1504
5. Straftatbestand des § 44 BDSG a.F. ....	1505
6. Keine allgemeine Zugänglichkeit personenbezogener Daten .....	1505
7. Verbot mit Erlaubnisvorbehalt .....	1505
III. Die Tatbestände des § 43 Abs. 2 BDSG a.F. ....	1506
1. Nr. 1: Unbefugtes Erheben und Verarbeiten .....	1506
2. Nr. 2: Unbefugtes Bereithalten zum Zwecke des Datenabrufs ....	1506
3. Nr. 3: Unbefugter Datenabruf .....	1506
4. Nr. 4: Erschleichen der Übermittlung von personenbezogenen Daten durch unrichtige Angaben .....	1507
5. Nr. 5: Verstöße gegen die besondere Zweckbindung von Daten	1507
6. Nr. 5a: Verstoß gegen das Koppelungsverbot des § 28 Abs. 3b BDSG a.F. ....	1507
7. Nr. 5b: Verstoß gegen das Verarbeitungs- und Nutzungsverbot des § 28 Abs. 4 BDSG a.F. ....	1508
8. Nr. 6: Deanonymisierung .....	1508
9. Nr. 7: Verstoß gegen die Mitteilungspflicht bei unrechtmäßiger Kenntniserlangung von Daten .....	1508
IV. Die Strafvorschrift des § 44 BDSG a.F. ....	1508
<b>F. Konfliktfelder des betrieblichen Datenschutzes aus strafrechtlicher Sicht</b>	1508
I. Überwachung und Störung des Telefonverkehrs .....	1509
II. Überwachung des Schriftverkehrs .....	1509
III. Überwachung des E-Mail-Verkehrs .....	1510
1. Eingriff in das Fernmeldegeheimnis .....	1510



	Seite
2. Arbeitgeber als Telekommunikationsanbieter nach § 206 StGB und Betreiber von Empfangsanlagen nach § 89 TKG .....	1510
3. Tatsituation bei einem Eingriff in das Fernmeldegeheimnis .....	1511
4. Rechtfertigungsgründe .....	1512
IV. Datenzugriff unter Überwindung einer Zugangssicherung .....	1513
V. Videoüberwachung besonders geschützter Räume .....	1513
VI. GPS-Überwachung .....	1514

**Annex: Rechtslage in Österreich**

A. Bestimmungen im österreichischen Datenschutzgesetz .....	1516
I. Abschwächung durch Verwarnungen .....	1517
II. Verfassungsrechtliche Aspekte .....	1517
B. Zuständigkeit .....	1518
C. Strafadressat .....	1519

**Teil XV. Länderberichte**

**Kapitel 1. Großbritannien**

A. Introduction to data protection in UK .....	1521
B. Recent jurisdiction .....	1522
C. Data Protection Act 2018 .....	1524

**Kapitel 2. Italien**

A. Introduction .....	1525
B. The implementation of the European data protection legislation in Italy .....	1526
C. The Italian personal data protection system and the impact of the GDPR .....	1528
I. Lawfulness of data processing .....	1528
II. Information notice (to be provided to the data subjects, on how and where personal data are collected) .....	1529
III. Data subjects' rights .....	1530
IV. Data Controller, data processor and persons authorized to process personal data under the direct authority of the controller or proces- sor .....	1530
V. Data processing risk approach and accountability measures .....	1531
VI. International data transfers .....	1531
D. Conclusion .....	1531

**Kapitel 3. Schweden**

A. Introduction to data protection in Sweden .....	1532
--	------



	Seite
B. National regulatory response to the General Data Protection Regulation	1533
C. Private sector challenges .....	1534

#### Kapitel 4. Tschechien

A. Data protection discovered .....	1537
B. Transposition .....	1538
C. Transposing metaphors .....	1539
D. Adoptive minimalism .....	1540
E. Data protection in the Czech judiciary .....	1541

#### Kapitel 5. Schweiz

A. Allgemeine datenschutzrechtliche Grundlagen .....	1546
I. Internationaler und europarechtlicher Rahmen .....	1546
II. Entwicklung und Stand der Gesetzgebung .....	1547
III. Rechtsquellen und Anwendungsbereich .....	1548
1. Datenschutzgesetz und Sondergesetze .....	1548
2. Kantonale Rechtsquellen .....	1549
IV. Anwendbares Recht und örtlicher Geltungsbereich .....	1549
B. Zweck, Geltungsbereich und Grundprinzipien .....	1550
I. Zweck und Geltungsbereich .....	1550
II. Gesetzliche Definitionen .....	1551
III. Materielle Grundprinzipien .....	1552
1. Gesetzmäßigkeit .....	1552
2. Verhältnismäßigkeit .....	1552
3. Zweckbindung .....	1552
4. Erkennbarkeit .....	1553
5. Datenminimierung .....	1553
IV. Transparenzanforderungen .....	1553
1. Informationspflichten .....	1553
2. Auskunftsrechte .....	1553
C. Datenschutzkonzepte und Datensicherheit .....	1555
I. Datenschutz durch Technik .....	1555
II. Datensicherheit .....	1555
III. Archivierung und Entsorgung .....	1556
IV. Zertifizierungen .....	1557
D. Datenschutz im Betrieb, Unternehmen und Konzern .....	1558
I. Datenschutz und Personal .....	1558
II. Datenschutz-Compliance und Whistleblowing .....	1558
III. Konzerninterner (grenzüberschreitender) Datenverkehr .....	1560



	Seite
IV. M&A-Transaktionen .....	1561
V. Betrieblicher Datenschutzbeauftragter .....	1561
<b>E. Outsourcing und neue Technologien .....</b>	<b>1562</b>
I. Auftragsdatenbearbeitung .....	1562
II. Cloud Computing .....	1563
III. Smart Metering .....	1563
IV. Cybersecurity .....	1564
<b>F. Datenschutz in besonderen Medien und Märkten .....</b>	<b>1565</b>
I. Datenschutz in einzelnen Kommunikationsformen .....	1565
1. Internet .....	1565
2. Telekommunikation .....	1567
3. Soziale Netzwerke .....	1569
II. Datenschutz im E-Commerce .....	1571
1. Kundendatenschutz .....	1571
2. Bonitätsbewertungen .....	1571
3. Opt-in/Opt-out-Verfahren bzw. Einwilligung .....	1573
4. Online-Zahlungsanbieter .....	1575
III. Information als Wirtschaftsgut .....	1576
1. Adresshandel .....	1576
2. RFID .....	1577
3. Werbung (im Internet) .....	1578
IV. Datenschutz im Gesundheitssektor .....	1580
1. eHealth .....	1580
2. mHealth .....	1581
<b>G. Datenschutzorganisation .....</b>	<b>1583</b>
I. Interne Organisationsvorkehrungen .....	1583
II. Aufsicht durch (öffentlichen) Datenschutzbeauftragten .....	1583
<b>H. Revision des Schweizer Datenschutzrechts .....</b>	<b>1584</b>

## Kapitel 6. Russland

<b>A. Legal Framework .....</b>	<b>1587</b>
<b>B. Scope of application .....</b>	<b>1588</b>
I. Jurisdictional and territorial effect .....	1588
II. Data localisation .....	1589
III. Personal data .....	1589
IV. Data operator .....	1589
V. Data processor .....	1589
VI. Data processing operations .....	1590
<b>C. Main data protection rules and requirements .....</b>	<b>1590</b>



	Seite
I. Principles of data procession .....	1590
II. Main obligations of operators .....	1590
D. Regulator and Notification .....	1591
E. Consent .....	1591
F. Rights of individuals .....	1592
G. Organisational and technical measures .....	1592
H. Information Security .....	1592
I. Enforcement and sanctions .....	1593
J. Cross-border data transfers .....	1594
 Kapitel 7. Ukraine 	
A. Legal Framework .....	1595
B. Scope of application .....	1596
C. Personal data .....	1596
D. Subjects of legal relations in the area of data procession .....	1597
E. Data protection principles and requirements .....	1597
I. Data protection principles .....	1597
II. Procedure for the procession of personal data .....	1598
F. Grounds for the procession of personal data .....	1598
G. Rights of a data subject .....	1599
H. Obligations of data holder .....	1599
I. Notification .....	1600
J. Data Protection Authority .....	1600
K. Cross-border data transfers .....	1601
 Sachverzeichnis .....	 1603