

Inhaltsverzeichnis

Vorwort	5
Inhaltsverzeichnis	7
Literaturverzeichnis	23

§ 1 Von der Richtlinie zur Verordnung – Europäisches Datenschutzrecht de lege lata

33

A. Vorbemerkungen	33
B. Allgemeines Datenschutzrecht der Europäischen Union	34
I. Ausgangspunkt	34
II. Grundrechtecharta	35
III. Datenschutzgrundrecht als allgemeiner Grundsatz des Unionsrechts	42
IV. Besonderer Schutz gegenüber dem Handeln der Europäische Union	44
1. Schutzbereich	44
2. Beeinträchtigungen und Rechtfertigung	45
C. Richtlinie 95/46/EG	45
D. Defizite des Richtlinienkonzeptes	48
E. Die Richtlinie geht, die Verordnung kommt	49
I. Rechtsnatur einer Verordnung auf EU-Ebene	49
II. Zielsetzungen der DSGVO	50
III. Aufbau der DSGVO	52

§ 2 Zentrale Begriffe

55

A. Vorbemerkung	55
B. Die Akteure des Datenschutzrechtes	55
I. Verantwortlicher	55
II. Betroffene Personen	58
III. Dritter	61
IV. Empfänger	62
V. Auftragsverarbeiter	62
VI. Vertreter	63
VII. Unternehmen und Unternehmensgruppe	63
VIII. Aufsichtsbehörde	64
C. Gegenstand des Datenschutzrechtes	64
I. Personenbezogene Daten	64
II. Besondere Kategorien von personenbezogenen Daten – „sensible Daten“	70
1. Allgemeines	70
2. Genetische Daten	72
3. Biometrische Daten	72
4. Gesundheitsdaten	72
D. Umgang mit Daten	73
I. Verarbeitung	73
1. Erheben	74
2. Erfassen	75
3. Organisation	75
4. Ordnen	76

5. Speicherung	77
6. Anpassung	77
7. Veränderung	78
8. Auslesen	78
9. Abfragen	78
10. Verwendung	78
11. Offenlegung [durch Übermittlung & Verarbeitung]	79
12. Abgleich oder Verknüpfung	80
13. Einschränkung	81
14. Löschen oder Vernichten	81
15. Pseudonymisierung	82
16. Anonymisierung	83
II. Automatisierte Verarbeitung	84
III. Nicht automatisierte Verarbeitung	84
E. Sonstige Legaldefinitionen	85

§ 3 Allgemeine Verarbeitungsgrundsätze 87

A. Vorbemerkung	87
B. Rechtmäßigkeit, Treu und Glauben und Transparenz	87
I. Rechtmäßigkeit der Datenverarbeitung	87
II. Verarbeitung nach Treu und Glauben	88
III. Transparenz	90
C. Zweckbindungsgrundsatz	92
I. Festgelegter Zweck	93
II. Eindeutiger Zweck	94
III. Legitimer Zweck	95
IV. Weiterverarbeitung	95
D. Datenminimierung	97
E. Richtigkeit	98
F. Speicherbegrenzung	99
G. Integrität und Vertraulichkeit	99
H. Rechenschaftspflicht	100

§ 4 Rechtsgrundlagen der Verarbeitung 105

A. Datenverarbeitung aufgrund einer Einwilligung, Art. 6 Abs. 1 lit. a) DSGVO	105
I. Inhaltliche Anforderungen an die Einwilligung des Betroffenen	105
1. Freiwilligkeit	106
a) Freiwilligkeit im Beschäftigungsverhältnis	106
b) Freiwilligkeit bei Auslobung finanzieller Anreize	109
c) Freiwilligkeit bei Verhandlungsungleichgewicht	112
d) Erzwungene Einwilligungen	112
2. Zweckbindung „für den konkreten Fall“	113
3. Informierte Einwilligung	113
4. Unmissverständlich	115
II. Formerfordernisse, „eindeutig bestätigende Handlung“	115
III. Vorformulierte Erklärungen	116
IV. Einwilligungsfähigkeit von Kindern, Art. 8 DSGVO	117

1. Dienste der Informationsgesellschaft	117
2. Einwilligung bei Diensten der Informationsgesellschaft	118
a) Mindestens 13, höchstens 16 Jahre	118
b) Direktes Angebot an Kinder	119
c) Erforderlichkeit der Einwilligung des Trägers der elterlichen Verantwortung	121
aa) Träger der elterlichen Verantwortung – Ein Elternteil ausreichend?	121
bb) Nachweis der Elterneinwilligung bzw. Zustimmung	124
cc) Keine Auswirkungen auf das Vertragsrecht	125
3. Anforderungen außerhalb der Dienste der Informationsgesellschaft	125
V. Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten	126
VI. Einwilligungserleichterungen für Forschung und Wissenschaft	126
VII. Einwilligung für Cookies, Web-Bugs und Co.	127
1. Cookies	127
a) Begrifflichkeit und Funktion	127
b) Rechtliche Beurteilung	128
aa) Einwilligung anhand der Browser-Einstellungen des jeweiligen Nutzers	129
bb) Keine Anwendung der Bestimmungen in §§ 14, 15 TMG	130
cc) Session-Cookies	130
dd) Permanent-Cookies	130
ee) Flash-Cookies	131
2. Web-Bugs	131
3. Verwendung sogenannter Web-Logs	132
4. Behavioral targeting und Online-Werbung	133
5. Kontrollüberlegungen aus der Richtlinie 2002/58/EG	134
6. Anforderungen an die Einwilligung	136
7. Zukünftige Neuregelung – die ePrivacy-Verordnung	136
VIII. Geltungsdauer einer Einwilligung	137
IX. Widerruflichkeit der Einwilligung	138
X. Keine Vertretung	138
XI. Sonderproblem: Einwilligung trotz bestehendem sonstigen Erlaubnistatbestand ..	138
XII. Fortbestand von Alt-Einwilligungen	139
B. Datenverarbeitung in Erfüllung eines Vertrags, Art. 6 I lit. b) DSGVO	139
I. Vertrag	140
II. Durchführung/Erfüllung	142
III. Erforderlichkeit der Verarbeitung	142
C. Datenverarbeitung in Erfüllung einer rechtlichen Verpflichtung, Art. 6 I lit. c) DSGVO ...	146
D. Datenverarbeitung zum Schutz lebenswichtiger Interessen, Art. 6 Abs. 1 lit. d) DSGVO ...	148
E. Datenverarbeitung in Wahrnehmung einer öffentlichen Aufgabe/im öffentlichen Interesse, Art. 6 Abs. 1 lit. e) DSGVO	148
F. Datenverarbeitung zur Wahrung berechtigten Interessen des Verantwortlichen oder eines Dritten, Art. 6 Abs. 1 lit. f) DSGVO	150
I. Allgemeines und Hintergründe	150
II. Begriff des „berechtigten Interesses“	154
III. Betroffeneninteressen	156
IV. Interessenabwägung	157
1. Allgemeine Anforderungen	157

2. In die Abwägung einzustellende Kriterien	157
a) Stellenwert, Charakter und Quelle des berechtigten Interesses	158
aa) Wahrnehmung eigener Grundrechtspositionen oder Grundfreiheiten ...	158
bb) Öffentliche Interessen	159
(1) Informationsvermittlungen durch Verbraucherzentralen	159
(2) Presseinformationen durch Wettbewerber	160
(3) Identifizierende Presseberichterstattungen	160
(4) Politischer Meinungskampf	162
cc) Verarbeitungen innerhalb einer Unternehmensgruppe (Konzerndaten- verarbeitung)	162
dd) Sonstige Konkretisierungen	163
b) Stellenwert, Charakter und Quelle des Betroffeneninteresses	163
aa) Kinder	164
bb) Kranke und sonst „verletzliche“ Personen	164
cc) Öffentliche Funktion und Bekanntheit der betroffenen Person	164
dd) Sozial- vs. Privatsphäre	165
c) Von der Verarbeitung betroffene Daten – Kategorisierung und Standard- Datenschutzmodell	165
aa) Normaler Schutzbedarf	166
bb) Hoher Schutzbedarf	166
cc) Sehr hoher Schutzbedarf	167
dd) „Öffentliche Daten“	167
d) Form der beabsichtigten Verarbeitung	170
e) Etablierte Schutzmaßnahmen – Garantien	170
f) Mögliche Folgen der Verarbeitung für den Betroffenen	170
g) Anleitung der Art. 29-Datenschutzgruppe	171
h) Scoring außerhalb eines konkreten Entscheidungsprozesses	171
i) Informationsrechte im Verein	173
G. Schematische Darstellung der Verarbeitung	175
H. Zweckändernde Weiterverarbeitung	176
I. Art. 6 Abs. 4 DSGVO	176
II. Weiterverarbeitungsbefugnisse im BDSG-Neu	176
1. Weiterverarbeitung durch öffentliche Stellen, § 23 BDSG-Neu	177
a) Offensichtlich „mutmaßliche“ Einwilligung in die Weiterverarbeitung, § 23 Abs. 1 Nr. 1 BDSG-Neu	177
b) Überprüfung von Angaben der betroffenen Person, § 23 Abs. 1 Nr. 2 BDSG-Neu	178
c) Abwehr erheblicher Nachteile für das Gemeinwohl oder Gefahr für die öf- fentliche Sicherheit, § 23 Abs. 1 Nr. 3 BDSG-Neu	178
d) Verfolgung von Straftaten, Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen, § 23 Abs. 1 Nr. 4 BDSG-Neu	178
e) Abwehr schwerwiegender Beeinträchtigung der Rechte einer anderen Per- son	179
f) Wahrnehmung von Aufsichts- und Kontrollbefugnissen usw., § 23 Abs. 1 Nr. 6	179
g) Besondere Anforderungen an die Weiterverarbeitung besonderer Katego- rien personenbezogener Daten, § 23 Abs. 2 BDSG-Neu	179
2. § 24 BDSG-Neu	179

a) Weiterverarbeitung zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten, § 24 Abs. 1 Nr. 1 BDSG-Neu	179
b) Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche, § 24 Abs. 1 Nr. 2 BDSG-Neu	180
c) Besondere Anforderung bei Weiterverarbeitung besonderer Kategorien personenbezogener Daten, § 24 Abs. 2 BDSG-Neu	181
I. Verarbeitung besonderer Kategorien personenbezogener Daten, Art. 9 DSGVO	181
I. Verarbeitung aufgrund einer Einwilligung	181
II. Verarbeitung im Zusammenhang mit dem Arbeitsrecht, dem Recht der sozialen Sicherheit und dem Sozialschutz	182
III. Verarbeitung zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person	182
IV. Verarbeitung durch politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation	183
V. Verarbeitung von durch den Betroffenen offensichtlich öffentlich gemachten Daten	183
VI. Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte	184
VII. Verarbeitung auf Grundlage eines erheblichen öffentlichen Interesses	184
VIII. Verarbeitung auf dem Gebiet der Gesundheitsvorsorge und der Arbeitsmedizin ..	185
IX. Verarbeitung zu Zwecken der öffentlichen Gesundheit oder der Abwendung schwerwiegender Gesundheitsgefahren	187
X. Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke	187
XI. Verarbeitungsbefugnisse in § 22 BDSG-Neu	188
1. Allgemeines	188
2. Ausnahmen zugunsten öffentlicher und nicht öffentlicher Stellen, § 22 Abs. 1 Nr. 1 BDSG-Neu	188
a) Ausübung von Rechten und Pflichterfüllung im Zusammenhang mit der sozialen Sicherheit und dem Sozialschutz, § 22 Abs. 1 Nr. 1 lit. a) BDSG-Neu	188
b) Gesundheitsvorsorge, Beurteilung der Arbeitsfähigkeit, medizinische Diagnostik und Behandlung, § 22 Abs. 1 Nr. 1 lit. b) DSGVO	188
c) Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, § 22 Abs. 1 Nr. 1 lit. c) DSGVO	189
3. Ausnahmen zugunsten öffentlicher Stellen, § 22 Abs. 1 Nr. 2 BDSG-Neu	189
4. Besondere Schutzvorkehrungen im Rahmen der Verarbeitung besonderer Kategorien personenbezogener Daten, § 22 Abs. 2 BDSG-Neu	189
J. Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten, Art. 10 DSGVO	194
K. Profiling und automatisierte Einzelfallentscheidungen	194
I. Profiling	194
1. Legaldefinition, Art. 4 Nr. 4 DSGVO und Anwendungsbereich	194
2. Anwendungsbeispiele	195
a) Big Data, Data Mining	195
b) Scoring	196
c) Nutzerprofile im Internet	198

II. Automatisierte Entscheidungen im Einzelfall	198
III. Ausnahmen vom Verbot des Profiling und automatisierter Einzelfallentscheidungen	199
1. Abschluss oder die Erfüllung eines Vertrags	199
2. Ausdrückliche Einwilligung der betroffenen Person	200
3. Zulässigkeit im Rahmen der Leistungserbringung nach einem Versicherungsvertrag, § 37 BDSG-Neu	200
a) Vollumfänglich stattgebende Entscheidung über einen Leistungsantrag der betroffenen Person, § 37 Abs. 1 Nr. 1 BDSG-Neu	200
b) Entscheidung auf Grundlage von verbindlichen Entgeltregelungen für Heilbehandlungen	201
c) Keine Beschränkung auf bestimmte Datenkategorien	202
4. Einschränkung der Verarbeitungsbefugnisse in Bezug auf Scoring- und Bonitätsauskünfte, § 31 BDSG-Neu	202
a) Regelungsgegenstand und Regelungsbefugnis	202
b) Verwendung von Wahrscheinlichkeitswerten zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses, § 31 Abs. 1 BDSG-Neu	204
c) Verwendung eines von Auskunftsebenen ermittelten Wahrscheinlichkeitswerts über die Zahlungsfähig- und Zahlungswilligkeit einer natürlichen Person ..	206
IV. Wahrung von Betroffeneninteressen, Art. 22 Abs. 3 DSGVO	207

§ 5 Informations- und Mitteilungspflichten des Verantwortlichen

A. Gang der Darstellung	209
B. Wesen der neuen Informationspflichten bei Datenerhebung – Warum und wie?	209
I. Zielsetzung und Zweck – Warum?	209
II. Formvorgaben der Informationspflicht – Wie?	210
1. Präzise, transparent, verständlich und leicht zugänglich	210
a) Allgemeine Anforderungen	210
b) Bildsymbole	213
c) Gesteigerte Anforderungen bei Informationen gegenüber Kindern	214
2. Formerfordernisse	214
3. Kosten	215
C. Informationspflichten im Rahmen der Datenerhebung beim Betroffenen (Direkterhebung)	216
I. Aufbau der Norm	216
1. Verhältnis zwischen Informationen nach Absatz 1 und Absatz 2	216
2. Information nur bei erstmaliger Erhebung oder bei jeder Erhebung	218
II. Informationspflichten nach Art. 13 Abs. 1 DSGVO	219
1. Name und Kontaktdaten	219
2. Kontaktdaten des Datenschutzbeauftragten	219
3. Zwecke und Rechtsgrundlagen der Verarbeitung	220
4. Berechtigte Interessen	220
5. Empfänger oder Kategorien von Empfängern	220
6. Übermittlung in Drittländer oder an internationale Organisationen	221
III. Informationspflichten nach Art. 13 Abs. 2 DSGVO („Informationen auf Abruf“) ..	221
1. Dauer der Speicherung bzw. Kriterien zur Festlegung der Speicherdauer	221
2. Betroffenenrechte	222

a) Auskunft	222
b) Recht auf Berichtigung	222
c) Recht auf Löschung	222
d) Einschränkung der Verarbeitung	222
e) Widerspruchsrecht	223
f) Recht auf Datenübertragbarkeit	223
g) Einwilligungswiderruf	223
h) Beschwerderecht	223
3. Verpflichtung zur Bereitstellung von Daten	223
a) Bereitstellung von Informationen aufgrund gesetzlicher Verpflichtung	224
b) Bereitstellung von Informationen aufgrund vertraglicher Verpflichtung ...	226
c) Bereitstellung für einen Vertragsabschluss erforderlich	226
d) Bereitstellungspflicht des Betroffenen und Folgen der Nichtbereitstellung .	227
4. Automatisierte Entscheidungsfindung einschließlich Profiling	228
IV. Informationspflicht bei Weiterverarbeitung	229
V. Nichtanwendbarkeit der Informationspflicht	230
1. Kenntnis des Betroffenen, Art. 13 Abs. 4 DSGVO	230
2. Ausnahme bei Weiterverarbeitung in Form der Offenlegung oder Übermitt- lung an Berufsgeheimnisträger, § 29 Abs. 2 BDSG-Neu	230
3. Weitere Ausnahmen von der Informationspflicht bei Weiterverarbeitung, § 32 Abs. 1 BDSG-Neu	231
a) Unverhältnismäßiger Aufwand bei Weiterverarbeitung „analog gespei- chelter Daten“, § 32 Abs. 1 Nr. 1 BDSG-Neu	231
aa) Analog gespeicherte Daten	231
bb) Weiterverarbeitungsvorgang richtet sich unmittelbar an den Betroffe- nen	232
cc) Weiterverarbeitung ist mit dem ursprünglichen Erhebungszweck ver- einbar	232
dd) Keine digitale Kommunikation	232
ee) Geringes Interesse des Betroffenen an Information	232
ff) Fallbeispiel	233
b) Gefährdung der Aufgabenerfüllung nach Art. 23 Abs. 1 lit. a bis e DSGVO, § 32 Abs. 1 Nr. 2 BDSG-Neu	233
c) Gefährdung der öffentlichen Sicherheit oder Ordnung, § 32 Abs. 1 Nr. 3 BDSG-Neu	234
d) Beeinträchtigung der Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche, § 32 Abs. 1 Nr. 4 BDSG-Neu	234
e) Gefährdung der vertraulichen Übermittlung an eine öffentliche Stelle, § 32 Abs. 1 Nr. 5 BDSG-Neu	235
4. Besondere Schutzvorkehrungen bei Wegfall der Informationspflicht, § 32 Abs. 2 u. 3 BDSG-Neu	235
a) Schriftliche Festlegung für ein Absehen von der Information an den Be- troffenen, § 32 Abs. 3 S. 3 BDSG-Neu	235
b) Besondere Schutzmaßnahme für Fälle nach § 32 Abs. 1 Nr. 1–3 BDSG- Neu	236
c) Nachholen der Information bei nur vorübergehender Gefährdung, § 32 Abs. 3 BDSG-Neu	236
D. Informationspflichten im Rahmen der Datenerhebung bei Dritten (Dritterhebung)	237
I. Aufbau der Norm	237

1. Verhältnis zwischen Informationen nach Absatz 1 und Absatz 2	237
2. Information nur bei erstmaliger Erhebung oder bei jeder Erhebung	238
II. Zeitpunkt des Entstehens der Informationspflichten nach Art. 14 Abs. 1 und 2 DSGVO, Art. 14 Abs. 3 DSGVO	238
1. Innerhalb eines Monats nach Erlangung, Art. 14 Abs. 3 lit. a) DSGVO	239
2. Zeitpunkt der ersten Mitteilung an den Betroffenen, Art. 14 Abs. 3 lit. b) DSGVO	239
3. Zum Zeitpunkt der Offenlegung, Art. 14 Abs. 3 lit. c) DSGVO	240
III. Informationspflichten nach Art. 14 Abs. 1 DSGVO	240
1. Name und Kontaktdaten, Art. 14 Abs. 1 lit. a) DSGVO	240
2. Datenschutzbeauftragter, Art. 14 Abs. 1 lit. b) DSGVO	240
3. Zwecke und Rechtsgrundlagen, Art. 14 Abs. 1 lit. c) DSGVO	240
4. Datenkategorien, Art. 14 Abs. 1 lit. d.) DSGVO	240
5. Empfänger oder Kategorien von Empfängern, Art. 14 Abs. 1 lit. e) DSGVO ..	241
6. Übermittlung in Drittländer, Art. 14 Abs. 1 lit. f) DSGVO	241
IV. Informationspflichten nach Art. 14 Abs. 2 DSGVO	241
1. Dauer der Speicherung, Art. 14 Abs. 2 lit. a) DSGVO	241
2. Berechtigte Interessen, Art. 14 Abs. 2 lit. b) DSGVO	242
3. Betroffenenrechte	242
a) Auskunft	242
b) Recht auf Berichtigung	242
c) Recht auf Löschung	242
d) Einschränkung der Verarbeitung	242
e) Widerspruchsrecht	243
f) Recht auf Datenübertragbarkeit	243
g) Einwilligungswiderruf	243
h) Beschwerderecht	243
4. Herkunft der Daten – Datenquelle, Art. 14 Abs. 2 lit. f) DSGVO	243
5. Automatisierte Entscheidungsfindung und Profiling, Art. 14 Abs. 2 lit. g) DSGVO	244
V. Informationspflicht bei Weiterverarbeitung, Art. 14 Abs. 4 DSGVO	244
VI. Generelle Nichtanwendbarkeit der Informationspflicht	244
1. Kenntnis des Betroffenen, Art. 14 Abs. 5 lit. a) DSGVO	244
2. Unmöglichkeit oder unverhältnismäßiger Aufwand, Art. 14 Abs. 5 lit. b) DSGVO	245
a) Erteilung von Informationen ist unmöglich	245
b) Erteilung der Informationen erfordert einen unverhältnismäßigen Aufwand	246
c) Schutzmaßnahmen des Verantwortlichen	247
3. Erlangung oder Offenlegung aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, Art. 14 Abs. 5 lit. c) DSGVO	248
4. Berufsgeheimnisse, Art. 14 Abs. 5 lit. d) DSGVO	249
5. Berechtigte Geheimhaltungsinteressen eines Dritten, § 29 Abs. 1 S. 1 BDSG-Neu	249
VII. Ausnahmen gem. § 33 BDSG-Neu	250
1. Entfall von Informationspflichten bei Weiterverarbeitung öffentlicher Stellen, § 33 Abs. 1 Nr. 1 BDSG-Neu	250
a) Gefährdung der Aufgabenwahrnehmung, § 33 Abs. 1 Nr. 1a) BDSG-Neu ..	250

b) Gefährdung der öffentlichen Sicherheit oder Ordnung oder des Wohls des Bundes oder eines Landes, § 33 Abs. 1 Nr. 1b) BDSG-Neu	250
2. Entfall von Informationspflichten bei Weiterverarbeitung nicht-öffentlicher Stellen, § 33 Abs. 1 Nr. 2 BDSG-Neu	251
a) Beeinträchtigung der Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche, § 33 Abs. 1 Nr. 2a) BDSG-Neu	251
b) Gefährdung der vertraulichen Übermittlung an eine öffentliche Stelle, § 33 Abs. 1 Nr. 2b) BDSG-Neu	251
3. Besondere Schutzvorkehrungen, § 33 Abs. 2 und 3 BDSG-Neu	252
E. Besondere Unterrichtungspflichten im Zusammenhang der Verarbeitung gem. Art. 6 Abs. 1 lit. e) oder f) DSGVO sowie der Direktwerbung, Art. 21 Abs. 4 DSGVO	252
F. Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Art. 34 DSGVO	253
I. Voraussetzung – Voraussichtlich hohes Risiko	253
II. Folgen, Form und Inhalt	255
III. Ausnahmen von der Benachrichtigungspflicht	256
1. Schutz der betroffenen Daten durch geeignete technische und organisatorische Maßnahmen, Art. 34 Abs. 3 lit. a) DSGVO	256
2. Nachfolgende Maßnahmen des Verantwortlichen, Art. 34 Abs. 3 lit. b) DSGVO	257
3. Unverhältnismäßiger Aufwand, Art. 34 Abs. 3 lit. c) DSGVO	257
4. Geheimhaltungsinteressen, § 29 Abs. 1 S. 3 BDSG-Neu	258
IV. Verwertungsverbot im Strafverfahren, § 42 Abs. 4 BDSG-Neu	258
G. Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Art. 33 DSGVO	258
I. Voraussetzung – Voraussichtliches Risiko	258
II. Inhalt der zu übermittelnden Informationen	259
1. Art der Verletzung	259
2. Kategorien und ungefähre Zahl von betroffenen Personen	259
3. Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen	259
4. Beschreibung der wahrscheinlichen Folgen der Verletzung	259
5. Beschreibung der vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung	259
III. Form und Frist der Mitteilung	260
IV. Verwertungsverbot im Strafverfahren, § 42 Abs. 4 BDSG-Neu	260
§ 6 Rechte des Betroffenen	261
A. Vorbemerkung	261
B. Auskunftsrecht der betroffenen Person, Art. 15 DSGVO	261
I. Nachforschungsanspruch – Werden überhaupt Daten über mich verarbeitet?	262
II. Auskunftsanspruch – Welche Daten werden von wem, für wen verarbeitet und was kann ich dagegen tun?	262
1. Allgemeiner Teil des Auskunftsanspruches	263
a) Verarbeitungszwecke	263
b) Kategorien personenbezogener Daten die Verarbeitet werden	263
c) Empfänger oder Kategorien von Empfängern	263
d) Dauer der Datenspeicherung oder die Kriterien ihrer Festlegung	265

e) Betroffenenrechte	265
aa) Recht auf Berichtigung	265
bb) Recht auf Löschung	265
cc) Einschränkung der Verarbeitung	265
dd) Widerspruchsrecht	265
ee) Beschwerderecht	265
f) Alle verfügbaren Informationen über die Herkunft der Daten	266
g) Automatisierte Entscheidungsfindung und Profiling	266
h) Übermittlung in Drittländer	266
2. Besonderer Teil des Auskunftsanspruches	266
a) Sämtliche verarbeiteten personenbezogenen Daten	266
b) Recht auf kostenlose Datenkopie	267
aa) Umfang – Was heißt „Kopie der personenbezogenen Daten“?	267
bb) Grundsätzlich kostenfrei	268
cc) Sonderproblem Auskunft über Inhalte der Patientenakte	270
3. Formale Anforderungen an die Auskunftserteilung	271
a) Präzise, transparent, verständlich und leicht zugänglich	271
b) Unverzüglich	271
c) In Papierform, auf Verlangen auch elektronisch	271
d) Gegenüber der richtigen betroffenen Person	272
III. Beschränkungen des Auskunftsanspruches	272
1. Beschränkung bei Verarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken, § 27 Abs. 2 BDSG-Neu	273
2. Beschränkung zugunsten von im öffentlichen Interesse liegender Archive, § 28 Abs. 2 BDSG-Neu	273
3. Geheimhaltungsinteressen, § 29 Abs. 1 S. 2 BDSG-Neu	273
4. Einschränkungen nach § 34 BDSG-Neu	273
a) Keine Informationspflicht nach § 33 BDSG-Neu, § 34 Abs. 1 Nr. 1 BDSG-Neu	273
b) Daten nur noch aufgrund von Aufbewahrungspflichten vorhanden, § 34 Abs. 1 Nr. 2a) BDSG-Neu	274
c) Daten dienen ausschließlich der Datensicherung und Datenschutzkontrolle, § 34 Abs. 1 Nr. 2b) BDSG-Neu	275
d) Besondere Dokumentationspflichten und Zweckbindung, § 34 Abs. 2 BDSG-Neu	275
e) Besonderheiten bei Auskunftsverweigerung durch öffentliche Stellen, § 34 Abs. 3 und 4 BDSG-Neu	276
IV. Auskunftsrecht gegenüber Auskunftsteilen im Zusammenhang mit Verbaucherkreditvergaben, § 30 BDSG-Neu	276
C. Recht auf Berichtigung	276
I. Art. 16 DSGVO	276
II. Einschränkung bei Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, § 28 Abs. 3 BDSG-Neu	277
III. Mitteilungspflicht des Verantwortlichen gegenüber Empfängern, Art. 19 DSGVO	278
D. Recht auf Löschung/„Recht auf Vergessenwerden“, Art. 17 DSGVO	278
I. Lösungsgründe	279
1. Zweckfortfall, Art. 17 Abs. 1 lit. a) DSGVO	279
2. Einwilligungswiderruf, Art. 17 Abs. 1 lit. b) DSGVO	281
3. Widerspruch gegen die Verarbeitung, Art. 17 Abs. 1 lit. c) DSGVO	282

a) Widerspruch gegen Verarbeitungen im Rahmen der Wahrnehmung einer Aufgabe im öffentlichen Interesse bzw. berechtigter Interessen des Verantwortlichen	282
b) Widerspruch gegen Verarbeitungen zu Zwecken der Direktwerbung	283
4. Unrechtmäßige Verarbeitung	284
5. Löschung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich	284
6. Daten, die in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Art. 8 Abs. 1 DSGVO erhoben wurden, Art. 17 Abs. 1 lit. f) DSGVO	284
II. Entfall der Löschungsberechtigung/-pflicht	285
1. Ausübung des Rechts auf freie Meinungsäußerung und Information, Art. 17 Abs. 3 lit. a) DSGVO	285
2. Erfüllung einer rechtlichen Verpflichtung, Art. 17 Abs. 3 lit. b) Alt. 1 DSGVO ..	287
3. Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, Art. 17 Abs. 3 lit. b) Alt. 2 DSGVO	288
4. Verarbeitung in Ausübung öffentlicher Gewalt, Art. 17 Abs. 3 lit. b) Alt. 3 DSGVO	288
5. Gründe des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, Art. 17 Abs. 3 lit. c) DSGVO	289
6. Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke, Art. 17 Abs. 3 lit. d) DSGVO	289
7. Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen, Art. 17 Abs. 3 lit. e) DSGVO	289
8. Einschränkungen nach § 35 BDSG-Neu	289
a) Regelungsbefugnis?	289
b) Unverhältnismäßiger hoher Aufwand bei nicht-automatisierter Verarbeitung, § 35 Abs. 1 BDSG-Neu	290
c) Pflicht zur Einschränkung der Verarbeitung und Mitteilungspflicht gegenüber dem Betroffenen, § 35 Abs. 2 BDSG-Neu	291
d) Entgegenstehen satzungsgemäßer oder vertraglicher Aufbewahrungsfristen, § 35 Abs. 3 BDSG-Neu	292
III. Besondere Verpflichtungen bei öffentlicher Zugänglichmachung, Art. 17 Abs. 2 DSGVO	293
IV. Mitteilungspflicht des Verantwortlichen gegenüber Empfängern, Art. 19 DSGVO ..	294
E. Recht auf Einschränkung der Verarbeitung, Art. 18 DSGVO	294
I. Bestreiten der Richtigkeit, Art. 18 Abs. 1 lit. a) DSGVO	294
II. Unrechtmäßige Verarbeitung, Art. 18 Abs. 1 lit. b) DSGVO	295
III. Zweckfortfall beim Verantwortlichen	295
IV. Widerspruch gegen die Verarbeitung gemäß Artikel 21 Absatz 1 DSGVO	296
V. Rechtsfolgen der Einschränkung, Art. 18 Abs. 2 DSGVO	296
VI. Beschränkung der Rechte nach § 28 Abs. 4 BDSG-Neu	297
F. Recht auf Datenübertragbarkeit, Art. 20 DSGVO	297
I. Betroffene Daten	298
1. Bereitgestellt	298
2. Personenbezogene Daten, die die betroffene Person betreffen	299
3. Verarbeitung aufgrund von Einwilligung oder Vertrag	299
4. Automatisierte Verarbeitung	300
II. Reichweite des Rechts auf Datenübertragbarkeit	300
1. Strukturiert, gängig und maschinenlesbar	300
2. Übermittlung an die betroffene Person	301

3. Direktübermittlung an einen neuen Verantwortlichen	301
III. Einschränkungen	302
IV. Verpflichtungen des „übernehmenden“ Verantwortlichen	302
G. Widerspruchsrecht, Art. 21 DSGVO	303
I. Überblick über den grundsätzlichen Inhalt des Widerspruchsrechts	303
II. Widerspruch gem. Art. 21 Abs. 1 DSGVO	303
1. Gegenstand	303
2. Inhaltliche Anforderungen	304
3. Formale Anforderungen/Frist	305
4. Rechtsfolgen	306
III. Werbewiderspruch, Art. 21 Abs. 2 DSGVO	307
1. Gegenstand, inhaltliche und formale Anforderungen	307
2. Rechtsfolgen	309
IV. Widerspruch gegen die Verwendung zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken, Art. 21 Abs. 5 DSGVO	309
V. Kein Widerspruchsrecht gegenüber öffentlichen Stellen, § 36 BDSG-Neu	309
VI. Einschränkungen für Archiv- und Forschungszwecke, § 27 Abs. 2 BDSG-Neu und § 28 Abs. 4 BDSG-Neu	310
§ 7 Sicherungsmechanismen zur Einhaltung der DSGVO	311
A. Vorbemerkungen	311
B. Grundsätzliches	311
C. Umsetzung technischer und organisatorischer Maßnahmen, Art. 32 DSGVO	315
I. Pseudonymisierung	316
1. Medizinische Forschung und Diagnostik	316
2. Videoüberwachung	317
3. Test-, Demo- oder Trainingssysteme	318
4. Umsetzungsmöglichkeiten für Pseudonymisierung	318
II. Verschlüsselung	318
III. Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste	319
1. Vertraulichkeit	319
2. Integrität	319
3. Verfügbarkeit	320
4. Belastbarkeit	320
IV. Wiederherstellbarkeit	321
V. Organisatorische Maßnahmen	321
VI. Regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen	322
D. Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Art. 25 DSGVO ..	322
I. Zentrale Begriffe und ihre Grundlagen	323
1. Datenschutz durch Technik – Data protection by Design	323
a) Historische Entwicklung	323
b) Schlussfolgerungen für die inhaltliche Bestimmung von pdD	326
2. Datenschutz durch datenschutzfreundliche Voreinstellungen – Data protection by Default	326

II. Umsetzungspflicht des Verantwortlichen	328
E. Dokumentation von Verarbeitungstätigkeiten	328
I. Verzeichnis über Verarbeitungstätigkeiten des Verantwortlichen, Art. 30 DSGVO	329
1. Abweichungen zum bisherigen Recht	329
2. Formale und inhaltliche Anforderungen	330
3. Ausnahmen von der Verpflichtung zur Führung eines Verzeichnisses	330
II. Verzeichnis über Verarbeitungstätigkeiten des Verantwortlichen	331
III. Aus anderen Bestimmungen abzuleitende Dokumentationspflichten	331
F. Datenschutz-Folgenabschätzung	334
I. Regelungsgegenstand und Anwendungsbereich	334
1. Prüfungsgegenstand – Target of Evaluation (ToE)	334
2. Voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen	337
a) Hohes Risiko	337
b) Eintrittswahrscheinlichkeit und Prognosezeitpunkt	342
II. Durchführungsvorgaben	342
1. Konsultation des Datenschutzbeauftragten	342
2. Form und Mindestinhalte	343
a) Systematische Beschreibung der Verarbeitungsvorgänge und der Zwecke der Verarbeitung	344
b) Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck	345
c) Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen	345
d) Darstellung von Abhilfemaßnahmen	345
e) Gruppierte Darstellung	346
f) Rückgriff auf bestehende Zertifizierungsverfahren und Leitlinien	347
3. Einholung des Standpunkts des Betroffenen	348
4. Überprüfungsverfahren	348
5. Gruppen- oder Branchen-Folgenabschätzung?	348
III. Besondere Konsultationspflichten	348
G. Datenschutzbeauftragter	349
I. Verpflichtung zur Bestellung eines Datenschutzbeauftragten	350
1. Regelung innerhalb der DSGVO, Art. 37 Abs. 1	350
a) Verarbeitung durch Behörden und öffentliche Stellen	350
b) Die Kerntätigkeit besteht aus Datenverarbeitungsvorgängen, die eine regelmäßige und systematische Überwachung von betroffenen Personen in großem Umfang erfordern	350
c) Die Kerntätigkeit besteht in der umfangreichen Verarbeitung besonderer Kategorien von Daten gem. Art. 9 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten liegt	351
2. Weitergehende Verpflichtungen in §§ 5–7 und 38 BDSG-Neu	352
II. Anforderungen an die Person des Datenschutzbeauftragten	352
1. Fachliche Eignung	352
2. Unabhängigkeit	353
3. Verschwiegenheitspflicht	355
4. Interner oder externer betrieblicher Datenschutzbeauftragter	355

III. Aufgaben des Datenschutzbeauftragten	356
IV. Besondere Verpflichtungen des Verantwortlichen bzw. des Auftragsverarbeiters ..	357
H. Zertifizierung	358
I. Verhaltensregeln – Code of Conduct	358
I. Allgemeines	358
II. Anforderungen an Verhaltensregeln	359
1. Ausarbeitungsberechtigung	359
2. Mögliche Inhalte	359
3. Überwachung	360
III. Genehmigungsverfahren	360
IV. Rechtswirkungen	360

§ 8 Auftragsverarbeitung 363

A. Allgemeines	363
B. Begriff und rechtliche Grundlage der Auftragsverarbeitung	363
I. Stellung des Auftragsverarbeiters – Abgrenzung zum Verantwortlichen	363
II. Abgrenzung zur gemeinsamen Verantwortung gem. Art. 26 DSGVO	366
1. Erforderlichkeit der Abgrenzung/haftungsrechtliche Gesichtspunkte	366
2. Wann liegt eine gemeinsame Verantwortung vor?	367
3. Inhaltliche Anforderungen an die gemeinsame Verantwortung	368
a) Festlegung der jeweiligen tatsächlichen Funktionen und Beziehungen in einer Vereinbarung	368
b) Zur Verfügung Stellung von Informationen an die betroffene Person	371
III. Wesen der Auftragsverarbeitung – Privilegierungsfunktion	371
C. Inhaltliche Anforderungen an die Auftragsverarbeitung	372
I. Begründung durch Vertrag oder anderes Rechtsinstrument	372
II. Inhaltliche Anforderungen an den Vertrag	373
1. Allgemeine Anforderungen	373
2. Besondere Anforderungen	374
a) Handlung auf dokumentierte Weisung	374
b) Vertraulichkeits- oder gesetzliche Verschwiegenheitspflicht	375
c) Ergreifen technisch-organisatorischer Maßnahmen nach Art. 32 DSGVO ..	376
d) Bedingungen der Inanspruchnahme von Unter-Auftragsverarbeitern	377
e) Unterstützung im Zusammenhang mit der Erfüllung von Betroffenenrech- ten	377
f) Unterstützung bei der Einhaltung der dem Verantwortlichen in den Art. 32 bis 36 DSGVO auferlegten Pflichten	377
g) Lösch- und Rückgabepflichten	378
h) Kontroll- und Betretungs- und Auskunftsrechte des Verantwortlichen und Nachweis- und Informationspflichten des Auftragsverarbeiters	378
3. Sinnvolle vertragliche Ergänzungen	379
D. Weitere Pflichten des Auftragsverarbeiters	379
I. Verpflichtung zu Vertreterbestellung, Art. 27 DSGVO	379
II. Führung eines Verzeichnisses über Verarbeitungstätigkeiten, Art. 30 Abs. 2 DSGVO	380
III. Zusammenarbeit mit der Aufsichtsbehörde, Art. 31 DSGVO	381
IV. Verpflichtung zur Bestellung eines Datenschutzbeauftragten, Art. 37 DSGVO ...	381
V. Adressat der Befugnisse der Aufsichtsbehörden, Art. 58 DSGVO	381

E. Pflichten des Auftraggebers	381
--------------------------------------	-----

§ 9 Das Beschäftigungsdatenschutzrecht im BDSG-NEU 383

A. Einführung	383
B. Rechtsgrundlagen	384
I. Aktuelle Regelungen zum Beschäftigtendatenschutz im BDSG	384
II. Aufbau des § 26 BDSG-Neu	385
C. Datenschutz im Bewerbungsverfahren	388
I. Einführung	388
II. Bewerberprofilerstellung anhand öffentlich zugänglicher Quellen	389
III. Datenerhebung im Bewerbungsgespräch	394
1. Begrenzung des Fragerechts	394
2. Verhaltensanalysen, Persönlichkeitstests, ärztliche Untersuchungen	394
IV. Nicht berücksichtigte Bewerber	395
D. Datenschutz im Rahmen bestehender Beschäftigungsverhältnisse	396
I. Einführung	396
II. Internet-, E-Mail und Telefon- und Handynutzung am Arbeitsplatz	396
III. Arbeitnehmerdaten im Internetauftritt des Unternehmens	397
1. Einwilligungserfordernis	397
2. Bilder ausgeschiedener Mitarbeiter im Internet	398
3. Zulässiger Inhalt von Informationen im Internet	399
IV. Einrichtung elektronischer Informationsdatenbanken	399
V. Unterhaltung sogenannter Skill-Datenbanken	399
E. Datenschutz nach Beendigung des Beschäftigungsverhältnisses	400

§ 10 Datenexport in Drittländer 401

A. Vorbemerkung	401
B. Angemessenheitsbeschluss, Art. 45 DSGVO	401
C. Vorliegen geeigneter Garantien, Art. 46 DSGVO	402
I. Verbindliche Unternehmensvorschriften – Binding Corporate Rules	402
1. Bisherige Rechtslage	402
2. Neue Rechtslage	404
II. Standarddatenschutzklauseln	406
III. Genehmigte Verhaltensregeln und Zertifizierungen	407
D. Weitere Ausnahmetatbestände	407

§ 11 Rechtsbehelfe, Haftung, Geldbußen und Sanktionen 409

A. Aufsichtsrechtliche Befugnisse und Maßnahmen	409
I. Aufsichtsbehörden	409
1. Anforderungen an die Unabhängigkeit	409
2. Bestimmung der örtlichen Zuständigkeit	410
II. Aufgaben der Aufsichtsbehörde	411
III. Befugnisse der Aufsichtsbehörden	411
IV. Rechtsbehelfe des Verantwortlichen und des Auftragsverarbeiters	413
B. Rechtsstellung der betroffenen Person	413
I. Beschwerderecht	413
1. Inhalt	413

2. Rechtsbehelfe	413
II. Recht auf Schadenersatz	414
1. Inhalt	414
2. Rechtsbehelfe	414
C. Geldbußen	414
I. Grundlegendes zur Bemessung	414
II. Bußgeldrahmen	415
III. Rechtsbehelfe	416
IV. Adressaten – Organhaftung?	416
D. Strafvorschriften	417
§ 12 Österreich	419
A. Vorbemerkung	419
B. Aufbau des DSG 2018	419
C. Regelungen im Einzelnen	419
I. Berichtigung und Löschung personenbezogener Daten, § 4 Abs. 2 DSG 2018	419
II. Verarbeitung von Daten über gerichtlich oder verwaltungsbehördliche strafbare Handlungen, § 4 Abs. 3 DSG 2018	421
III. Konkretisierung in Bezug auf Art. 8 DSGVO	421
IV. Datenschutzbeauftragter, § 5 DSG 2018	421
V. Datengeheimnis, § 6 DSG 2018	422
VI. Übermittlung von Adressdaten zum Zwecke der Benachrichtigung und Befragung, § 8 DSG 2018	422
VII. Medienprivileg, § 9 DSG 2018	423
VIII. Bildverarbeitung und Videoüberwachung zu privaten Zwecken, §§ 12, 13 DSG 2018	423
IX. Datenschutzaufsicht, §§ 14 – 23 DSG 2018	425
X. Nähere Ausgestaltung zu Rechtsbehelfen, Haftung und Sanktionen, §§ 24 – 30 DSG 2018	425
1. Beschwerderecht, § 24 DSG 2018	425
2. Schadenersatz – Zuständigkeit	426
3. Geldbußen	426
Anhang 1: VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES	427
Anhang 2: BDSG-Neu (Auszug)	537
Stichwortverzeichnis	565