

Inhaltsverzeichnis

Vorwort	3
Die Autoren	5

1 Einführung und Grundlagen im Überblick	15
1.1 Datenschutz in der EU	18
1.1.1 Regelung mit Durchgriffswirkung	19
1.1.2 Bedeutung der englischen Fassung für die Auslegung	19
1.1.3 Grundsätzliches zur DSGVO	20
1.2 Öffnungsklauseln für nationale Umsetzung	23
1.3 Aufsichtsbehörden	26
1.3.1 Allgemeines zu den Aufsichtsbehörden	26
1.3.2 Datenschutzkonferenz (DSK)	27
1.3.3 Europäischer Datenschutzausschuss (EDSA)	28
1.4 Aufbau der DSGVO	31
1.4.1 Überblick	31
1.4.2 Anwendungsbereich	31
1.4.3 Struktur	34
1.5 Verbotsgesetz mit Erlaubnisvorbehalt	39
1.6 Grundsätze des Datenschutzes	43
1.7 Die DSGVO im Überblick	46
1.7.1 Betroffenenrechte	46
1.7.2 Recht auf Datenübertragbarkeit (Datenportabilität)	52
1.7.3 Recht auf Löschung	53
1.7.4 Direkterhebung	55
1.7.5 Marktorprinzip	56
1.7.6 „Privacy by Design“ und „Privacy by Default“	57
1.7.7 Datenschutz-Folgenabschätzung (DSFA)	59
1.7.8 Sanktionen	61
1.8 Drittländer	65
1.8.1 Drittländer mit angemessenem Datenschutzniveau	66

1.8.2	Allgemeine Grundsätze der Datenübermittlung	67
1.8.3	Was müssen Anbieter mit Sitz außerhalb der EU beachten?	72
1.8.4	EU-Standardvertragsklauseln	74
2	Beschäftigtendatenschutz	79
2.1	Einleitung ins Thema	79
2.2	Grundlagen	84
2.2.1	Persönlicher Anwendungsbereich – Betroffene	84
2.2.2	Arbeitgeber als Verantwortlicher	85
2.2.3	Sondervorschriften für besondere Kategorien von Daten	86
2.2.4	Erlaubnistatbestände nach § 26 BDSG	88
2.2.5	Betroffenenrechte im Arbeitsverhältnis	93
2.3	Datenschutz im Arbeitsrecht	101
2.3.1	Anbahnung von Arbeitsverhältnissen	101
2.3.2	Durchführung und Beendigung von Arbeitsverhältnissen	111
2.3.3	Industrie 4.0 und Big Data	118
2.3.4	Verschiedene Praxisfragen	120
2.3.5	Datenschutz im Konzern	137
2.3.6	Datenschutz und Betriebsrat	138
2.4	Folgen rechtswidriger Datenverarbeitung im Beschäftigungskontext	144
2.4.1	Verwertungsverbote	144
2.4.2	Rechtsprechung des BAG und der Landesgerichte	146
2.4.3	Bußgeldvorschriften und Strafbarkeit	149
3	Der Datenschutzbeauftragte	151
3.1	Aufgaben, Rechte und Pflichten des Datenschutzbeauftragten	153
3.2	Einordnung in die Organisation	159
3.2.1	Direktes Vortragsrecht	159

3.2.2	Weisungsungebundenheit	159
3.2.3	Vermeidung von Interessenkonflikten	160
3.2.4	Abberufungsschutz bzw. Sonder- kündigungsschutz	161
3.2.5	Zeitanteile für die Ausübung der Tätigkeit als DSB	164
3.3	Benennung des Datenschutzbeauftragten	167
3.3.1	Begrifflichkeiten und Formvorschriften	167
3.3.2	Voraussetzungen zur Ausübung der Tätigkeit	168
3.3.3	Wann ist ein Datenschutzbeauftragter zu be- nennen?	170
3.3.4	Interne und externe Datenschutzbeauftragte	174
3.4	Bekanntmachung des Datenschutzbeauftragten	177
3.5	Pflichten der Organisation	180
3.5.1	Ordnungsgemäße und frühzeitige Einbindung in datenschutzrelevante Themen	180
3.5.2	Unterstützung des Datenschutzbeauftragten	181
3.6	Haftung des Datenschutzbeauftragten	183
3.6.1	Generelle Haftung des DSB	183
3.6.2	Haftung des internen Datenschutzbeauftragten .	185
3.6.3	Haftung des externen Datenschutzbeauftragten	187
3.7	Umsetzungsmöglichkeiten im Konzern und für öffentliche Stellen	190
3.8	Besonderheiten des kirchlichen Datenschutzbeauf- tragten	192
3.9	Datenschutzbeauftragter und Betriebsrat	194
3.10	Arbeitshilfen	196
3.10.1	Muster: Benennung zum betrieblichen Daten- schutzbeauftragten	196
4	Auftragsverarbeitung und gemeinsame Verantwortlichkeit	199
4.1	Auftragsverarbeitung	199
4.1.1	Vertragsparteien einer Vereinbarung zur Auf- tragsverarbeitung	199
4.1.2	Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DSGVO	202

4.1.3	Vereinbarungen zwischen den Vertragsparteien	203
4.1.4	Rechte und Pflichten des Auftraggebers	208
4.2	Gemeinsame Verantwortlichkeit	218
4.2.1	Grundlegendes	218
4.2.2	Gegenstand der Vereinbarung	219
4.2.3	Rechte und Pflichten gemeinsam Verantwortlicher	222
4.2.4	Rechtsprechung	224
4.3	Arbeitshilfen	226
4.3.1	Checkliste: Gemeinsame Verantwortlichkeit	226
5	IT-Sicherheit und Datenschutz	229
5.1	Einleitung	229
5.2	Anforderungen an die IT-Sicherheit	232
5.2.1	Gesetzliche Anforderungen an die IT-Sicherheit	232
5.2.2	Untergesetzliche Normen zur IT-Sicherheit	242
5.2.3	Schutzziele der IT-Sicherheit	244
5.2.4	Managementsystem zur Umsetzung der IT-Sicherheit	245
5.3	Anforderungen an die Sicherheit bei der Verarbeitung personenbezogener Daten nach Art. 32 DSGVO	249
5.3.1	Schutzziele des Datenschutzes	249
5.3.2	Anforderungen an den Schutz personenbezogener Daten	251
5.3.3	Vorgehen zur Umsetzung der Anforderungen	252
5.4	Gemeinsame Sicherheitsstrategie von IT-Sicherheit und Datenschutz	259
5.4.1	Konfliktpotenziale bei den Schutzz Zielen	259
5.4.2	Auseinanderfallender Schutzbedarf	261
5.4.3	Fazit	261
5.5	Dokumentationserfordernis: Verzeichnis von Verarbeitungstätigkeiten	262
5.5.1	Inhaltliche Anforderungen beim Verantwortlichen	265

5.5.2	Inhaltliche Anforderungen bei Auftragsverarbeitern	270
5.6	Datenschutz-Folgenabschätzung (DSFA)	272
5.6.1	Verpflichtung	272
5.6.2	Inhaltliche Anforderungen	276
5.6.3	Konsultationspflicht mit der Datenschutzaufsichtsbehörde	277
5.7	Besondere Anforderungen bei Cloud-Lösungen	279
5.7.1	Auswahl geeigneter Daten und Datenverarbeitungen	280
5.7.2	Auswahl des Anbieters	281
5.7.3	Vertragliche Sicherstellung von Kontrollmöglichkeiten	282
5.7.4	Transfer der Daten in ein Drittland	282
5.8	Besondere Anforderungen bei der Bereitstellung von WLAN	285
5.8.1	Zugang nur für Betriebsangehörige	285
5.8.2	Zugang auch für Externe	286

6 Umgang mit personenbezogenen Daten in der Praxis 291

6.1	Zentrale abteilungsübergreifende Datenverarbeitungsaspekte	291
6.1.1	Datenschutz und IT-Prozesse – ein Interessenkonflikt?	291
6.1.2	Personenbezogene Daten und Kriterien zu deren Ermittlung	294
6.1.3	„Erleichternde“ Datenverarbeitungsumstände	296
6.1.4	Datensicherheitsaspekte	299
6.1.5	Bedeutung des Standard-Datenschutzmodells ..	303
6.1.6	Datenschutzmanagement	308
6.1.7	Datenschutz und Künstliche Intelligenz	310
6.1.8	Tracking und Datenschutz	316
6.2	Personalabteilung	327
6.2.1	Bewerbungsverfahren	327
6.2.2	Durchführung des Beschäftigungsverhältnisses ..	333
6.2.3	Offboarding	340

6.3	Marketing und Kommunikation	341
6.3.1	Anforderungen an die Verarbeitung personen- bezogener Daten zu Werbe- und Marketingzwe- cken	343
6.3.2	Werbeansprachen unter Beachtung wettbe- werbsrechtlicher Anforderungen	360
6.3.3	Social-Media-Marketing	364
6.3.4	Einsatz von Trackingmechanismen zu Marke- tingzwecken	369
6.4	Data Acts: Gesetze über die digitalen Dienste, digitalen Märkte und Daten-Governance der EU	375
6.4.1	Digital Markets Act (DMA)	375
6.4.2	Digital Services Act (DSA)	379
6.4.3	Data Governance Act (DGA)	384
6.5	Arbeitshilfen	389
6.5.1	Checkliste: Einwilligungserklärung und Widerruf im Marketing	389
6.5.2	Checkliste: Cookies und Webanalyse	391
6.5.3	Checkliste: Umgang mit personenbezogenen Daten im Beschäftigungsverhältnis	393
6.5.4	Checkliste: Umgang mit personenbezogenen Daten im Bewerbungsverfahren	395
7	Rechte der betroffenen Person	399
7.1	Recht auf transparente Information, Kommunikation und Modalitäten der Ausübung von Betroffenenrechten (Art. 12 DSGVO)	400
7.2	Recht auf Information (Artt. 13, 14 DSGVO)	408
7.3	Recht auf Auskunft (Art. 15 DSGVO)	417
7.4	Recht auf Berichtigung (Art. 16 DSGVO)	428
7.5	Recht auf Löschung und Recht auf Vergessenwerden (Art. 17 DSGVO)	434
7.6	Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)	445
7.7	„Recht auf Datenübertragbarkeit“ (Art. 20 DSGVO)	449
7.8	Recht auf Widerspruch (Art. 21 DSGVO)	454

7.9	Recht auf nicht ausschließlich automatisierte Entscheidungen im Einzelfall inkl. Profiling (Art. 22 DSGVO)	461
7.10	Sonderfall: Recht am eigenen Bild (DSGVO vs. KUG) ...	468
8	Rechts-, Haftungs- und Zahlungsfolgen bei Verstößen	479
8.1	Potenzielle (Rechts-)Folgen	479
8.2	Rechte von Betroffenen	480
8.3	Rechte von Aufsichtsbehörden	486
8.4	Erfahrungen mit Bußgeldern	490
8.5	Sonstige (Rechts-)Folgen	496
	Gesetzesgrundlagen und Adressen	499
	Abkürzungsverzeichnis	500
	Stichwortverzeichnis	503