

Inhaltsverzeichnis

Die Autoren	5
1 Einführung und Grundlagen im Überblick	15
1.1 Datenschutz in der EU	19
1.1.1 Regelung mit Durchgriffswirkung	20
1.1.2 Bedeutung der englischen Fassung für die Auslegung	20
1.1.3 Grundsätzliches zur DSGVO	21
1.2 Öffnungsklauseln für nationale Umsetzung	24
1.3 Aufsichtsbehörden	27
1.3.1 Allgemeines zu den Aufsichtsbehörden	27
1.3.2 Datenschutzkonferenz (DSK)	28
1.3.3 Europäischer Datenschutzausschuss (EDSA)	29
1.4 Aufbau der DSGVO	32
1.4.1 Überblick	32
1.4.2 Anwendungsbereich	32
1.4.3 Struktur	35
1.5 Begrifflichkeiten	41
1.6 Verbotsgesetz mit Erlaubnisvorbehalt	43
1.7 Grundsätze des Datenschutzes	47
1.8 Die DSGVO im Überblick	50
1.8.1 Betroffenenrechte	50
1.8.2 Recht auf Datenübertragbarkeit (Datenportabilität)	56
1.8.3 Recht auf Löschung	57
1.8.4 Direkterhebung	59
1.8.5 Marktortprinzip	60
1.8.6 „Privacy by Design“ und „Privacy by Default“	61
1.8.7 Datenschutz-Folgenabschätzung (DSFA)	63
1.8.8 Sanktionen	65
1.9 Drittländer	69
1.9.1 Drittländer mit angemessenem Datenschutzniveau	70

1.9.2	Was ist bei einer internationalen Datenübermittlung zu beachten?	72
1.9.3	Welche Grundsätze gelten für eine Datenübermittlung in Drittländer?	73
1.9.4	Was müssen Anbieter mit Sitz außerhalb der EU beachten?	74
1.9.5	EU-Standardvertragsklauseln	76
2	Beschäftigtendatenschutz	79
2.1	Einleitung ins Thema	79
2.2	Grundlagen	84
2.2.1	Persönlicher Anwendungsbereich	84
2.2.2	Arbeitgeber als Verantwortlicher	85
2.2.3	Sensible Daten	86
2.2.4	Erlaubnissnormen und Einwilligungen	87
2.2.5	Informations-, Auskunfts- und Meldepflichten	89
2.3	Datenschutz im Arbeitsrecht	95
2.3.1	Anbahnung von Arbeitsverhältnissen	95
2.3.2	Durchführung und Beendigung von Arbeitsverhältnissen	98
2.3.3	Industrie 4.0 und Big Data	104
2.3.4	Verschiedene Praxisfragen	111
2.3.5	Tarifverträge und Betriebsvereinbarungen	121
2.3.6	Datenschutz und Betriebsrat	122
2.4	Prozessuales	128
2.4.1	Rechtswidrigkeit von Überwachungs- und Kontrollmaßnahmen	128
2.4.2	Verwertungsverbote	128
2.4.3	Rechtsprechung des BAG und der Landesarbeitsgerichte	129
2.5	Whistleblower-Hinweissystem	133
3	Der Datenschutzbeauftragte	137
3.1	Aufgaben, Rechte und Pflichten des Datenschutzbeauftragten	139

3.2	Einordnung in die Organisation	144
3.2.1	Direktes Vortragsrecht	144
3.2.2	Weisungsungebundenheit	144
3.2.3	Vermeidung von Interessenkonflikten	145
3.2.4	Abberufungsschutz bzw. Sonderkündigungs- schutz	146
3.3	Benennung des Datenschutzbeauftragten	150
3.3.1	Begrifflichkeiten und Formvorschriften	150
3.3.2	Voraussetzungen zur Ausübung der Tätigkeit	151
3.3.3	Wann ist ein Datenschutzbeauftragter zu benen- nen?	153
3.3.4	Interne und externe Datenschutzbeauftragte	158
3.4	Bekanntmachung des Datenschutzbeauftragten	160
3.5	Pflichten der Organisation	163
3.5.1	Ordnungsgemäße und frühzeitige Einbindung in datenschutzrelevante Themen	163
3.5.2	Unterstützung des Datenschutzbeauftragten	164
3.6	Haftung des Datenschutzbeauftragten	166
3.6.1	Generelle Haftung des DSB	166
3.6.2	Haftung des internen Datenschutzbeauftragten .	168
3.6.3	Haftung des externen Datenschutzbeauftragten	170
3.7	Umsetzungsmöglichkeiten im Konzern und für öffentli- che Stellen	173
3.8	Besonderheiten des kirchlichen Datenschutzbeauftrag- ten	175
3.9	Datenschutzbeauftragter und Betriebsrat	177
3.10	Arbeitshilfen	179
3.10.1	Muster: Benennung zum betrieblichen Daten- schutzbeauftragten	179
4	IT-Sicherheit und Datenschutz	183
4.1	Einleitung	183
4.2	Anforderungen an die IT-Sicherheit	186
4.2.1	Gesetzliche Anforderungen an die IT-Sicherheit	186
4.2.2	Untergesetzliche Normen zur IT-Sicherheit	195
4.2.3	Schutzziele der IT-Sicherheit	197

4.2.4	Managementsystem zur Umsetzung der IT-Sicherheit	198
4.3	Anforderungen an die Sicherheit bei der Verarbeitung personenbezogener Daten nach Art. 32 DSGVO	202
4.3.1	Schutzziele des Datenschutzes	202
4.3.2	Anforderungen an den Schutz personenbezogener Daten	204
4.3.3	Vorgehen zur Umsetzung der Anforderungen	205
4.4	Gemeinsame Sicherheitsstrategie von IT-Sicherheit und Datenschutz	212
4.4.1	Konfliktpotenziale bei den Schutzzielen	212
4.4.2	Auseinanderfallender Schutzbedarf	214
4.4.3	Fazit	214
4.5	Dokumentationserfordernis: Verzeichnis von Verarbeitungstätigkeiten	215
4.5.1	Inhaltliche Anforderungen beim Verantwortlichen	218
4.5.2	Inhaltliche Anforderungen bei Auftragsverarbeitern	223
4.6	Datenschutz-Folgenabschätzung (DSFA)	224
4.6.1	Verpflichtung	224
4.6.2	Inhaltliche Anforderungen	228
4.6.3	Konsultationspflicht mit der Datenschutzaufsichtsbehörde	229
4.7	Besondere Anforderungen bei Cloud-Lösungen	231
4.7.1	Auswahl geeigneter Daten und Datenverarbeitungen	232
4.7.2	Auswahl des Anbieters	233
4.7.3	Vertragliche Sicherstellung von Kontrollmöglichkeiten	234
4.7.4	Transfer der Daten in ein Drittland	234
4.8	Besondere Anforderungen bei der Bereitstellung von WLAN	237
4.8.1	Zugang nur für Betriebsangehörige	237
4.8.2	Zugang auch für Externe	238

5	Umgang mit personenbezogenen Daten in der Praxis	243
5.1	Zentrale abteilungsübergreifende Datenverarbeitungsaspekte	243
5.1.1	Datenschutz und IT-Prozesse – ein Interessenkonflikt?	243
5.1.2	Personenbezogene Daten und Kriterien zu deren Ermittlung	246
5.1.3	„Erleichternde“ Datenverarbeitungsumstände	249
5.1.4	Datensicherheitsaspekte	251
5.1.5	Bedeutung des Standard-Datenschutzmodells ..	256
5.1.6	Datenschutzmanagement	260
5.1.7	Datenschutz und Künstliche Intelligenz	262
5.1.8	Tracking und Datenschutz	269
5.2	Personalabteilung	280
5.2.1	Bewerbungsverfahren	280
5.2.2	Durchführung des Beschäftigungsverhältnisses	286
5.2.3	Offboarding	293
5.3	Marketing und Kommunikation	294
5.3.1	Anforderungen an die Verarbeitung personenbezogener Daten zu Werbe- und Marketingzwecken nach DSGVO	296
5.3.2	Werbeansprachen unter Beachtung wettbewerbsrechtlicher Anforderungen	312
5.3.3	Social-Media-Marketing	315
5.3.4	Einsatz von Trackingmechanismen zu Marketingzwecken	319
5.4	Arbeitshilfen	325
5.4.1	Checkliste: Einwilligungserklärung und Widerruf im Marketing	325
5.4.2	Checkliste: Cookies und Webanalyse	327
5.4.3	Checkliste: Umgang mit personenbezogenen Daten im Beschäftigungsverhältnis	329
5.4.4	Checkliste: Umgang mit personenbezogenen Daten im Bewerbungsverfahren	332

6	Rechte der betroffenen Person	335
6.1	Recht auf transparente Information, Kommunikation und Modalitäten der Ausübung von Betroffenenrechten (Art. 12 DSGVO)	336
6.2	Recht auf Information (Artt. 13, 14 DSGVO)	343
6.3	Recht auf Auskunft (Art. 15 DSGVO)	352
6.4	Recht auf Berichtigung (Art. 16 DSGVO)	361
6.5	Recht auf Löschung und Recht auf Vergessenwerden (Art. 17 DSGVO)	367
6.6	Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)	378
6.7	„Recht auf Datenübertragbarkeit“ (Art. 20 DSGVO)	382
6.8	Recht auf Widerspruch (Art. 21 DSGVO)	386
6.9	Recht auf nicht ausschließlich automatisierte Entscheidungen im Einzelfall inkl. Profiling (Art. 22 DSGVO)	392
6.10	Sonderfall: Recht am eigenen Bild (DSGVO vs. KUG)	398
7	Rechts-, Haftungs- und Zahlungsfolgen bei Verstößen	409
7.1	Potenzielle (Rechts-)Folgen	409
7.2	Rechte von Betroffenen	410
7.3	Rechte von Aufsichtsbehörden	415
7.4	Erfahrungen mit Bußgeldern	419
7.5	Sonstige (Rechts-)Folgen	426
	Adressen der Aufsichtsbehörden	429
	Gesetzesgrundlagen	435
	Abkürzungsverzeichnis	436
	Stichwortverzeichnis	439