

Inhaltsverzeichnis

Vorwort	3
Die Autoren	5

1 Einführung und Grundlagen im Überblick 15

1.1	Datenschutz in der EU	17
1.1.1	Regelung mit Durchgriffswirkung	18
1.1.2	Bedeutung der englischen Fassung für die Auslegung	18
1.1.3	Grundsätzliches zur DSGVO	19
1.2	Öffnungsklauseln für nationale Umsetzung	22
1.3	Aufsichtsbehörden	26
1.3.1	Allgemeines	26
1.3.2	Datenschutzkonferenz (DSK)	27
1.3.3	Europäischer Datenschutzausschuss (EDSA)	28
1.4	Aufbau der DSGVO	32
1.4.1	Überblick	32
1.4.2	Anwendungsbereich	32
1.4.3	Struktur	35
1.5	Verbotsgesetz mit Erlaubnisvorbehalt	41
1.6	Grundsätze des Datenschutzes	45
1.7	Die DSGVO im Überblick	48
1.7.1	Betroffenenrechte	48
1.7.2	Recht auf Datenübertragbarkeit (Datenportabilität)	54
1.7.3	Recht auf Löschung	56
1.7.4	Direkterhebung	57
1.7.5	Marktortprinzip	58
1.7.6	„Privacy by Design“ und „Privacy by Default“	59
1.7.7	Datenschutz-Folgenabschätzung (DSFA)	62
1.7.8	Sanktionen	64
1.8	Drittländer	68
1.8.1	Drittländer mit angemessenem Datenschutzniveau	69

1.8.2	Allgemeine Grundsätze der Datenübermittlung ...	72
1.8.3	Was müssen Anbieter mit Sitz außerhalb der EU beachten?	77
1.8.4	EU-Standardvertragsklauseln	78
2	Beschäftigtendatenschutz	83
2.1	Einleitung ins Thema	83
2.1.1	Öffnungsklausel für die Datenverarbeitung im Beschäftigungskontext	84
2.1.2	Exkurs: Kirchliches Datenschutzrecht	87
2.2	Grundlagen	89
2.2.1	Persönlicher Anwendungsbereich – Betroffene ...	90
2.2.2	Arbeitgeber als Verantwortlicher	91
2.2.3	Sondervorschriften für besondere Kategorien von Daten	92
2.2.4	Erlaubnistatbestände nach Art. 6 DSGVO und § 26 BDSG	94
2.2.5	Betroffenenrechte im Arbeitsverhältnis	100
2.3	Datenschutz im Arbeitsrecht	109
2.3.1	Anbahnung von Arbeitsverhältnissen	109
2.3.2	Durchführung und Beendigung von Arbeitsverhältnissen	119
2.3.3	Datenverarbeitung durch künstliche Intelligenz (KI)	126
2.3.4	Weitere Praxisfragen	129
2.3.5	Datenschutz im Konzern	147
2.3.6	Datenschutz und Betriebsrat	148
2.4	Folgen rechtswidriger Datenverarbeitung im Beschäftigungskontext	154
2.4.1	Verwertungsverbote	154
2.4.2	Rechtsprechung des BAG und der Landesarbeitsgerichte	156
2.4.3	Bußgeldvorschriften und Strafbarkeit	159

3 Der Datenschutzbeauftragte	161
3.1 Aufgaben, Rechte und Pflichten des Datenschutzbeauftragten	163
3.2 Einordnung in die Organisation	170
3.2.1 Direktes Vortragsrecht	170
3.2.2 Weisungsungebundenheit	170
3.2.3 Vermeidung von Interessenkonflikten	171
3.2.4 Abberufungsschutz bzw. Sonderkündigungsschutz	173
3.2.5 Zeitanteile für die Ausübung der Tätigkeit als DSB	176
3.3 Benennung des Datenschutzbeauftragten	179
3.3.1 Begrifflichkeiten und Formvorschriften	179
3.3.2 Voraussetzungen zur Ausübung der Tätigkeit	180
3.3.3 Wann ist ein Datenschutzbeauftragter zu benennen?	182
3.3.4 Interne und externe Datenschutzbeauftragte	186
3.4 Bekanntmachung des Datenschutzbeauftragten	189
3.5 Pflichten der Organisation	192
3.5.1 Ordnungsgemäße und frühzeitige Einbindung in datenschutzrelevante Themen	192
3.5.2 Unterstützung des Datenschutzbeauftragten	193
3.6 Haftung des Datenschutzbeauftragten	195
3.6.1 Generelle Haftung des DSB	195
3.6.2 Haftung des internen Datenschutzbeauftragten	197
3.6.3 Haftung des externen Datenschutzbeauftragten	199
3.7 Umsetzungsmöglichkeiten im Konzern und für öffentliche Stellen	202
3.8 Besonderheiten des kirchlichen Datenschutzbeauftragten	204
3.9 Datenschutzbeauftragter und Betriebsrat	205

4	Auftragsverarbeitung und gemeinsame Verantwortlichkeit	209
4.1	Auftragsverarbeitung	209
4.1.1	Vertragsparteien einer Vereinbarung zur Auftragsverarbeitung	209
4.1.2	Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DSGVO	212
4.1.3	Vereinbarungen zwischen den Vertragsparteien	214
4.1.4	Rechte und Pflichten des Auftraggebers	218
4.2	Gemeinsame Verantwortlichkeit	228
4.2.1	Grundlegendes	228
4.2.2	Gegenstand der Vereinbarung	229
4.2.3	Rechte und Pflichten gemeinsam Verantwortlicher	232
4.2.4	Rechtsprechung	234
5	IT-Sicherheit und Datenschutz	237
5.1	Einleitung	237
5.2	Anforderungen an die IT-Sicherheit	241
5.2.1	Gesetzliche Anforderungen an die IT-Sicherheit	241
5.2.2	Untergesetzliche Normen zur IT-Sicherheit	252
5.2.3	Schutzziele der IT-Sicherheit	254
5.2.4	Managementsystem zur Umsetzung der IT-Sicherheit	255
5.3	Anforderungen an die Sicherheit bei der Verarbeitung personenbezogener Daten nach Art. 32 DSGVO	259
5.3.1	Schutzziele des Datenschutzes	259
5.3.2	Anforderungen an den Schutz personenbezogener Daten	261
5.3.3	Vorgehen zur Umsetzung der Anforderungen	263
5.4	Gemeinsame Sicherheitsstrategie von IT-Sicherheit und Datenschutz	270
5.4.1	Konfliktpotenziale bei den Schutzzielen	271
5.4.2	Auseinanderfallender Schutzbedarf	272
5.4.3	Fazit	273

5.5	Verzeichnis von Verarbeitungstätigkeiten	274
5.5.1	Inhaltliche Anforderungen beim Verantwortlichen	277
5.5.2	Inhaltliche Anforderungen bei Auftragsverarbeitern	283
5.6	Datenschutz-Folgenabschätzung (DSFA)	285
5.6.1	Verpflichtung	285
5.6.2	Inhaltliche Anforderungen	290
5.6.3	Konsultationspflicht mit der Datenschutz-aufsichtsbehörde	291
5.7	Besondere Anforderungen bei Cloud-Lösungen	293
5.7.1	Auswahl geeigneter Daten und Datenverarbeitungen	294
5.7.2	Auswahl des Anbieters	295
5.7.3	Vertragliche Sicherstellung von Kontrollmöglichkeiten	296
5.7.4	Transfer der Daten in ein Drittland	296
5.8	Besondere Anforderungen bei der Bereitstellung von WLAN	299
5.8.1	Zugang nur für Betriebsangehörige	299
5.8.2	Zugang auch für Externe	300

6 **Umgang mit personenbezogenen Daten in der Praxis** 303

6.1	Zentrale abteilungsübergreifende Datenverarbeitungsaspekte	303
6.1.1	Datenschutz und IT-Prozesse – ein Interessenkonflikt?	303
6.1.2	Personenbezogene Daten und Kriterien zu deren Ermittlung	306
6.1.3	„Erleichternde“ Datenverarbeitungsumstände	309
6.1.4	Datensicherheitsaspekte	311
6.1.5	Bedeutung des Standard-Datenschutzmodells ..	316
6.1.6	Datenschutzmanagement	320
6.1.7	Datenschutz und künstliche Intelligenz	322
6.1.8	Tracking und Datenschutz	330

6.2	Personalabteilung	341
6.2.1	Bewerbungsverfahren	341
6.2.2	Durchführung des Beschäftigungsverhältnisses	347
6.2.3	Offboarding	355
6.3	Marketing und Kommunikation	356
6.3.1	Anforderungen an die Verarbeitung personen- bezogener Daten zu Werbe- und Marketing- zwecken	358
6.3.2	Werbeansprachen unter Beachtung wettbewerbsrechtlicher Anforderungen	375
6.3.3	Social-Media-Marketing	379
6.3.4	Einsatz von Trackingmechanismen zu Marketingzwecken	384
6.4	Data Acts der EU	389
6.4.1	Digital Markets Act (DMA)	389
6.4.2	Digital Services Act (DSA)	392
6.4.3	Data Governance Act (DGA)	397
6.4.4	Data Act	402
6.5	Arbeitshilfen	406
7	Rechte der betroffenen Person	407
7.1	Recht auf transparente Information, Kommunikation und Modalitäten der Ausübung von Betroffenenrechten (Art. 12 DSGVO)	408
7.2	Recht auf Information (Artt. 13, 14 DSGVO)	415
7.3	Recht auf Auskunft (Art. 15 DSGVO)	424
7.4	Recht auf Berichtigung (Art. 16 DSGVO)	435
7.5	Recht auf Löschung und Recht auf Vergessenwerden (Art. 17 DSGVO)	441
7.6	Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)	452
7.7	„Recht auf Datenübertragbarkeit“ (Art. 20 DSGVO)	456
7.8	Recht auf Widerspruch (Art. 21 DSGVO)	461
7.9	Recht auf nicht ausschließlich automatisierte Entschei- dungen im Einzelfall inkl. Profiling (Art. 22 DSGVO)	468
7.10	Sonderfall: Recht am eigenen Bild (DSGVO vs. KUG) ...	476

8	Rechts-, Haftungs- und Zahlungsfolgen bei Verstößen	487
8.1	Potenzielle (Rechts-)Folgen	487
8.2	Rechte von Betroffenen	488
8.3	Rechte von Aufsichtsbehörden	495
8.4	Erfahrungen mit Bußgeldern	498
8.5	Sonstige (Rechts-)Folgen	504
8.6	Datenschutzsanktionenrecht	506
	Gesetzesgrundlagen und Adressen	510
	Abkürzungsverzeichnis	511
	Stichwortverzeichnis	513