

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	Grundsätzliches zur DSGVO	20
1.2	Aufsichtsbehörden	27
1.2.1	Allgemeines	27
1.2.2	Datenschutzkonferenz (DSK)	28
1.2.3	Europäischer Datenschutzausschuss (EDSA)	29
1.3	Verbotsgesetz mit Erlaubnisvorbehalt	32
1.4	Die DSGVO im Überblick	36
1.4.1	Betroffenenrechte	36
1.4.2	Recht auf Datenübertragbarkeit (Datenportabilität)	42
1.4.3	Recht auf Löschung	43
1.4.4	Direkterhebung	45
1.4.5	Marktortprinzip	46
1.4.6	„Privacy by Design“ und „Privacy by Default“	47
1.4.7	Datenschutz-Folgenabschätzung (DSFA)	49
1.4.8	Sanktionen	51
1.5	Drittländer	55
1.5.1	Drittländer mit angemessenem Datenschutzniveau	56
1.5.2	Allgemeine Grundsätze der Datenübermittlung ...	59
1.5.3	Was müssen Anbieter mit Sitz außerhalb der EU beachten?	64
1.5.4	EU-Standardvertragsklauseln	65

2	Beschäftigtendatenschutz	67
2.1	Einleitung ins Thema	67
2.1.1	Öffnungsklausel für die Datenverarbeitung im Beschäftigungskontext	68
2.1.2	Exkurs: Kirchl. Datenschutzrecht	72
2.2	Grundlagen	73
2.2.1	Persönlicher Anwendungsbereich – Betroffene	74
2.2.2	Arbeitgeber als Verantwortlicher	75
2.2.3	Sondervorschriften für besondere Kategorien personenbezogener Daten	76
2.2.4	Erlaubnistatbestände nach Art. 6 DSGVO und § 26 BDSG	78
2.2.5	Betroffenenrechte im Arbeitsverhältnis	85
2.3	Datenschutz im Arbeitsrecht	93
2.3.1	Anbahnung von Arbeitsverhältnissen	93
2.3.2	Durchführung und Beendigung von Arbeitsverhältnissen	103
2.3.3	Datenverarbeitung durch künstliche Intelligenz	110
2.3.4	Weitere Praxisfragen	113
2.3.5	Datenschutz im Konzern	127
2.3.6	Datenschutz und Betriebsrat	128
2.4	Folgen rechtswidriger Datenverarbeitung im Beschäftigungskontext	133
2.4.1	Verwertungsverbote	133
2.4.2	Rechtsprechung des BAG und der Landesarbeitsgerichte	135
2.4.3	Bußgeldvorschriften und Strafbarkeit	138
3	Der Datenschutzbeauftragte	141
3.1	Aufgaben, Rechte und Pflichten des Datenschutzbeauftragten	143
3.2	Einordnung in die Organisation	151
3.2.1	Direktes Vortragsrecht	151
3.2.2	Weisungsungebundenheit	151
3.2.3	Vermeidung von Interessenkonflikten	152

3.2.4	Abberufungsschutz bzw. Sonderkündigungsschutz	154
3.2.5	Zeitanteile für die Ausübung der Tätigkeit als DSB	157
3.2.6	DSB als Informationssicherheitsbeauftragter oder interne Meldestelle Hinweisgeberschutz	159
3.3	Benennung des Datenschutzbeauftragten	163
3.3.1	Begrifflichkeiten und Formvorschriften	163
3.3.2	Voraussetzungen zur Ausübung der Tätigkeit	164
3.3.3	Wann ist ein Datenschutzbeauftragter zu benennen?	165
3.3.4	Interne und externe Datenschutzbeauftragte	170
3.4	Bekanntmachung des Datenschutzbeauftragten	173
3.5	Pflichten der Organisation	176
3.5.1	Ordnungsgemäße und frühzeitige Einbindung in datenschutzrelevante Themen	176
3.5.2	Unterstützung des Datenschutzbeauftragten	177
3.6	Haftung des Datenschutzbeauftragten	179
3.6.1	Generelle Haftung des DSB	179
3.6.2	Haftung des internen Datenschutzbeauftragten .	181
3.6.3	Haftung des externen Datenschutzbeauftragten	183
3.7	Umsetzungsmöglichkeiten im Konzern und für öffentliche Stellen	186
3.8	Datenschutzbeauftragter und Betriebsrat	188
4	Auftragsverarbeitung und gemeinsame Verantwortlichkeit	191
4.1	Auftragsverarbeitung	191
4.1.1	Vertragsparteien einer Vereinbarung zur Auftragsverarbeitung	191
4.1.2	Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DSGVO	194
4.1.3	Vereinbarungen zwischen den Vertragsparteien	196
4.1.4	Rechte und Pflichten des Auftraggebers	200
4.1.5	Auftragsverarbeitung im Konzern	210
4.2	Gemeinsame Verantwortlichkeit	213
4.2.1	Grundlegendes	213

4.2.2	Gegenstand der Vereinbarung	214
4.2.3	Rechte und Pflichten gemeinsam Verantwortlicher	217
4.2.4	Rechtsprechung	219
5	IT-Sicherheit und Datenschutz	221
5.1	Einleitung	221
5.2	Anforderungen an die IT-Sicherheit	225
5.2.1	Gesetzliche Anforderungen an die IT-Sicherheit	225
5.2.2	Untergesetzliche Normen zur IT-Sicherheit	237
5.2.3	Schutzziele der IT-Sicherheit	239
5.2.4	Managementsystem zur Umsetzung der IT-Sicherheit	241
5.3	Anforderungen an die Sicherheit bei der Verarbeitung personenbezogener Daten nach Art. 32 DSGVO	245
5.3.1	Schutzziele des Datenschutzes	245
5.3.2	Anforderungen an den Schutz personen- bezogener Daten	247
5.3.3	Vorgehen zur Umsetzung der Anforderungen	249
5.4	Gemeinsame Sicherheitsstrategie von IT-Sicherheit und Datenschutz	255
5.4.1	Konfliktpotenziale bei den Schutzzielen	256
5.4.2	Auseinanderfallender Schutzbedarf	257
5.4.3	Fazit	258
5.5	Verzeichnis von Verarbeitungstätigkeiten	259
5.5.1	Inhaltliche Anforderungen beim Verantwortlichen	262
5.5.2	Inhaltliche Anforderungen bei Auftrags- verarbeitern	267
5.6	Datenschutz-Folgenabschätzung (DSFA)	269
5.6.1	Verpflichtung	269
5.6.2	Inhaltliche Anforderungen	274
5.6.3	Konsultationspflicht mit der Datenschutzauf- sichtsbehörde	275
5.7	Besondere Anforderungen bei Cloud-Lösungen und WLAN	276

5.7.1	Auswahl geeigneter Daten und Datenverarbeitungen	277
5.7.2	Auswahl des Anbieters	278
5.7.3	Vertragliche Sicherstellung von Kontrollmöglichkeiten	278
5.7.4	Transfer der Daten in ein Drittland	279
5.7.5	Bereitstellung von WLAN	280
6	Umgang mit personenbezogenen Daten in der Praxis	283
6.1	Zentrale abteilungsübergreifende Datenverarbeitungsaspekte	283
6.1.1	Datenschutz und IT-Prozesse – ein Interessenkonflikt?	283
6.1.2	Personenbezogene Daten und Kriterien zu deren Ermittlung	286
6.1.3	„Erleichternde“ Datenverarbeitungsumstände	289
6.1.4	Datensicherheitsaspekte	292
6.1.5	Datenschutzmanagement	298
6.1.6	Tracking und Datenschutz	300
6.2	Personalabteilung	309
6.2.1	Bewerbungsverfahren	309
6.2.2	Durchführung des Beschäftigungsverhältnisses	315
6.2.3	Offboarding	323
6.3	Marketing und Kommunikation	324
6.3.1	Anforderungen an die Verarbeitung personenbezogener Daten zu Werbe- und Marketingzwecken	326
6.3.2	Werbeansprachen unter Beachtung wettbewerbsrechtlicher Anforderungen	345
6.3.3	Social-Media-Marketing	349
6.3.4	Einsatz von Trackingmechanismen zu Marketingzwecken	352
6.4	Data Acts der EU	358
6.4.1	Digital Markets Act (DMA)	358
6.4.2	Digital Services Act (DSA)	362
6.4.3	Data Governance Act (DGA)	367

6.4.4	Data Act	371
6.5	Datenschutz und künstliche Intelligenz	375
6.5.1	Datenschutzrechtliche Bewertung	376
6.5.2	Positionierung der Aufsichtsbehörden zu KI	381
6.5.3	KI-Verordnung (AI Act) im Überblick	384
6.5.4	KI-Kompetenz	387
7	Rechte der betroffenen Person	389
7.1	Recht auf transparente Information, Kommunikation und Modalitäten der Ausübung von Betroffenenrechten (Art. 12 DSGVO)	390
7.2	Recht auf Information (Artt. 13, 14 DSGVO)	398
7.3	Recht auf Auskunft (Art. 15 DSGVO)	407
7.4	Recht auf Berichtigung (Art. 16 DSGVO)	419
7.5	Recht auf Löschung und Recht auf Vergessenwerden (Art. 17 DSGVO)	425
7.6	Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)	437
7.7	„Recht auf Datenübertragbarkeit“ (Art. 20 DSGVO)	441
7.8	Recht auf Widerspruch (Art. 21 DSGVO)	446
7.9	Recht auf nicht ausschließlich automatisierte Entschei- dungen im Einzelfall inkl. Profiling (Art. 22 DSGVO)	453
8	Rechts-, Haftungs- und Zahlungsfolgen bei Verstößen	461
8.1	Potenzielle (Rechts-)Folgen	461
8.2	Rechte von Betroffenen	462
8.3	Rechte von Aufsichtsbehörden	470
8.4	Erfahrungen mit Bußgeldern	474
8.5	Sonstige (Rechts-)Folgen	479
8.6	Datenschutzsanktionenrecht	481

9	Gesetzesgrundlagen und Arbeitshilfen	485
	Abkürzungsverzeichnis	487
	Stichwortverzeichnis	489