

Inhaltsübersicht

Vorwort	V
Inhaltsverzeichnis	IX
1. Kapitel	
Einleitung	1
2. Kapitel	
Datenschutzrechtliche Grundlagen	13
3. Kapitel	
Datenschutz in der Personalabteilung/Arbeitnehmerdatenschutz	37
4. Kapitel	
Marketing und Werbung	153
5. Kapitel	
Datenverarbeitung im Auftrag	213
6. Kapitel	
Technische Organisatorische Maßnahmen/Datensicherheit	237
7. Kapitel	
Die Datenschutz-Grundverordnung (DS-GVO)	253
8. Kapitel	
Die datenschutzkonforme Unternehmensdokumentation nach der DS-GVO	265
Sachverzeichnis	287

Inhaltsverzeichnis

Vorwort	V
Inhaltsübersicht.....	VII
1. Kapitel	
Einleitung	1
I. Datenschutz – Historie und Ausblick	1
1. Geburtsstunde des Datenschutzes: Das Volkszählungsurteil	1
2. Datenschutzskandale	4
3. Ausblick	9
II. Wie Ihnen dieses Buch hilft	11
1. Aufbau	11
2. Checklisten/Muster und Beispiele	11
3. Datenschutzrechtliche Musterdokumentation	12
2. Kapitel	
Datenschutzrechtliche Grundlagen	13
I. Was ist Datenschutz?	13
1. Datensubjekt und Informationelle Selbstbestimmung	13
2. Personenbezogene Daten – was zählt dazu?	14
3. Verarbeitungstatbestände	16
4. Gesetzliche Grundlagen	16
5. Datenschutzrechtliche Grundsätze	17
a) Verbot mit Erlaubnisvorbehalt	17
b) Auskunfts- und Korrekturrechte des Betroffenen	19
c) Datensicherheit	19
d) Rechtliche Risiken und Sanktionen	21
e) Datenvermeidung und Datensparsamkeit / Privacy by Default und Privacy by Design	23
f) Kontrolle/Der Datenschutzbeauftragte	24

II. Gesetzgeberische Aktivitäten	25
1. Datenschutzreform 2009 / Inkrafttreten der DS-GVO 2018	26
a) Informationspflichten gemäß Art. 33 DS-GVO	26
b) Datensparsamkeit und Anonymisierung	30
c) Datenschutzbeauftragter	31
d) Auftragsdatenverarbeitung	32
e) Direktmarketing ohne Einwilligung	32
f) Direktmarketing mit Einwilligung	34
g) Stärkung der Position der Aufsichtsbehörden	35
2. Arbeitnehmerdatenschutz	35

3. Kapitel

Datenschutz in der Personalabteilung/ Arbeitnehmerdatenschutz

37

I. Bewerberdaten und Bewerbungsprozess

37

1. Welche Daten dürfen erhoben werden?	37
a) Immer zulässig: Stammdaten	37
b) Verarbeitung besonderer Kategorien personenbezogener Daten	40
c) Vorstrafen	42
d) Schwerbehinderung und Krankheiten	42
e) Gewerkschaftszugehörigkeit	45
f) Religiöse Überzeugung	45
g) Soziale Netzwerke	46
h) COVID-Impfstatus	48
2. Medizinische Untersuchungen und Eignungstests	49
a) Medizinische Untersuchungen	49
b) Eignungstests	50
3. Speicherdauer/Regelfristen	51
4. Weitergabe personenbezogener Daten im Konzern	55
5. Online-Bewerbungen / Software für Bewerbermanagement	57
6. Personalberater	59

II. Arbeitsvertrag/Erforderliche Unterlagen

61

1. Zwingend: Verpflichtung auf das Datengeheimnis	62
2. Konzernprivileg	64
3. Merkblatt Datenschutz	68

III. Datenspeicherung im Arbeitsverhältnis	69
1. Umfang der Verarbeitung	69
a) Grundsätze	69
b) Einzelfälle	70
2. Übermittlung an Dritte	72
3. Übermittlung ins Ausland	74
4. Löschung und Sperrung	76
5. Löschung nach Beendigung des Arbeitsverhältnisses	77
IV. Personalakte	79
1. Gesetzliche Rahmenbedingungen	79
2. Datenschutzrechtlich zu beachten	80
a) Zugriff auf die Personalakte	80
b) Inhalte	82
c) Rechte des Arbeitnehmers	83
d) Datensicherheit	84
V. Nutzung von Internet und E-Mail	86
1. Rechtslage bei Gestattung privater Internet- und E-Mail-Nutzung	87
a) TTDSG	87
b) Zusätzlich: Arbeitnehmerdatenschutz nach der DS-GVO	90
2. Rechtslage bei Verbot privater Internet- und E-Mail- Nutzung	92
3. Ansprüche des Arbeitnehmers	92
4. Wichtig: Regeln der Internet- und E-Mail-Nutzung	93
a) Regelung in Internet- und E-Mail-Policy	94
b) Muster einer Internet-Policy	94
c) Regelung in einer Betriebsvereinbarung	99
d) Muster einer Betriebsvereinbarung Internet- und E-Mail-Nutzung	99
e) Checkliste: Internet- und E-Mail-Policy	102
VI. Nutzung von Telefondaten	105
1. Allgemeine Grundsätze sowie Gespräche mit einer Interessenvertretung	105
2. Call-Center und telefonische Kundenbetreuung	106

VII. Datenschutz und Betriebsrat	107
1. Geltung der DS-GVO für den Betriebsrat	107
2. Datenschutz im Betriebsrat	107
VIII. Videoüberwachung	109
1. Videoüberwachung im öffentlichen Betriebsgelände	109
2. Videoüberwachung im nicht-öffentlichen Betriebsgelände	113
3. Videoüberwachung in Rückzugsflächen	115
4. Aufbewahrungsfristen	115
IX. Ortungssysteme	117
X. Biometrische Verfahren	119
XI. Datenerhebung bei Straftaten und Pflichtverletzungen ..	120
1. Grundsatz: Erhebung von Daten nur mit Kenntnis	120
2. Voraussetzungen der Datenerhebung	121
3. Zweckgebundenheit/Verhältnismäßigkeit	122
4. Zeitliche und technische Einschränkungen	124
XII. Datenschutzrechtliche Haftung und Strafbarkeit	125
XIII. Anonymisierter Abgleich von Daten	127
1. Straftaten und Pflichtverletzungen	128
2. Anonymisierte oder pseudonymisierte Nutzung	129
XIV. Unterrichtungspflicht bei Datenpannen sowie Beschwerderecht	130
XV. Mitarbeiterschulungen	134
XVI. Der Datenschutzbeauftragte	135
1. Pflicht zur Bestellung	135
2. Fachkunde und Zuverlässigkeit	137
3. Datenschutzbeauftragter und Betriebsrat	138
4. Datenschutzbeauftragter und Führungspositionen	139
5. Bestellung des Datenschutzbeauftragten	140
6. Aufgaben des Datenschutzbeauftragten	141
7. Abberufung	144
8. Haftung	145
9. Interner und externer Datenschutzbeauftragter	147

XVII. Datenschutz bei Unternehmensverkäufen	148
XVIII. Praxisecheckliste	149
4. Kapitel	
Marketing und Werbung	153
I. Kunden- und Interessentendaten	153
1. Grundsätze	153
2. Informationspflichten	154
3. Möglichkeiten und Grenzen des CRM	158
a) Nutzungsprofile	158
b) CRM in der Praxis	159
II. Online-Marketing	160
1. Internetauftritt	160
a) Impressum	160
b) Cookie Hinweis/Consent Management zu Cookies	162
c) Consent Management/Cookie Einwilligung	164
d) Konkrete Umsetzung	167
e) Datenschutzerklärung	170
2. Leadgenerierung	177
a) Datenschutzrechtliche Einwilligung immer erforderlich	177
b) Inhalt	178
c) Koppelungsverbot	179
d) Wettbewerbsrechtliche Einwilligung	180
e) Confirmed Opt-In	181
3. Analyse des Nutzerverhaltens im Internet	183
a) Online Nutzungsprofile/Düsseldorfer Kreis	183
b) Google Analytics	185
III. Adressbroking	189
1. Grundsätze	189
2. Widerspruchsrecht/Hinweispflicht	191
3. Verträge mit Adressbrokern	192
IV. Dienstleister und Agenturen	194
1. Verpflichtung auf das Datengeheimnis	194
2. Datenauftragsverarbeitung	197

V. Web 2.0 und Social Media	198
1. Datenschutzniveau der jeweiligen Netzwerke	198
2. Datenschutzrechtliche Aspekte im Unternehmen	200
3. Social-Media-Policy	201
4. Facebook Fanpages / EUGH Urteil	203
V. Künstliche Intelligenz und ChatGPT	206
1. Ausgangssituation	206
2. Empfehlung aus Praxissicht	208
a) Umgang mit vertraulichen Informationen / Betriebs- geheimnissen	208
b) Umgang mit personenbezogenen Daten	208
c) Umgang mit diskriminierenden, schädlichen und irre- führenden Antworten	209
d) Urheberrechtsverletzungen	209
e) KI-Scanner	209
f) Persönlichkeitsrechte	209
g) Schulung der Mitarbeiter	210
VI. Praxisecheckliste	212
5. Kapitel	
Datenverarbeitung im Auftrag	213
I. Überblick	213
II. Definition/Vorliegen der Datenverarbeitung im Auftrag ..	214
III. Rechtsfolgen	216
1. Überprüfung der technischen organisatorischen Maß- nahmen	216
a) Erstauswahl	216
b) Erstkontrolle/Vorabkontrolle	217
c) Regelmäßige Kontrolle	218
2. Vertragsinhalte	219
Checkliste Vertrag zur Auftragsverarbeitung nach Art. 28 DS-GVO	219
IV. Auslandsbezug	220
1. Systematik	220

2. Kein Drittland (Beispiel Frankreich)	221
3. Drittland mit angemessenem Datenschutzniveau (Beispiel Schweiz)	222
4. Sonderfall USA	222
a) Vor dem Safe-Harbor-Urteil / Schrems I	222
b) Privacy Shield	226
c) Schrems II Urteil	228
d) Aktuelle Entwicklungen: Bußgeld gegen Meta	229
e) TADAP-Framework	229
5. Drittland ohne angemessenes Datenschutzniveau (Beispiel Russland)	232
6. EU-Standardvertragsklausel	233
7. Überblick	234
V. Cloud-Computing	234
1. Technische Hintergründe und Begriffsdefinition	234
2. Datenschutzrechtliche Bewertung	235
6. Kapitel	
Technische Organisatorische Maßnahmen/Datensicherheit ..	237
I. Datenschutz und Datensicherheit	237
1. Grundsätze	237
2. Zunahme der Cyberkriminalität	238
3. Gesetzliche Rahmenbedingungen	239
II. Auditierungen	241
1. Alternativen	241
2. Einzelne IT-Sicherheitskonzepte	242
a) IT-Grundschutzkatalog	242
b) CobiT	244
c) ISO 9000	245
d) ISO/IEC 17799 und BS 7799	245
III. Umsetzung in der Praxis	246
1. Dokumentation technisch-organisatorischer Maßnahmen	246
2. IT-Security-Policy	249

7. Kapitel	
Die Datenschutz-Grundverordnung (DS-GVO)	253
I. Überblick	253
1. Sinn und Zweck	253
2. Systematik: Ein einheitlicher Rechtsrahmen	254
3. Öffnungsklauseln	255
II. Wichtigste Änderungen und Neuregelungen	255
1. Ausweitung der Interessenabwägung	255
2. Internationale Datentransfers und EU-Standardvertrags-	
klauseln	256
3. Datenschutzbeauftragter	257
4. Auftragsverarbeitung	258
5. Datenschutz-Folgenabschätzung	258
6. Technisch-organisatorische Maßnahmen nach der DS-GVO	259
7. Meldepflichten	260
8. Hohe Geldbußen nach der DS-GVO	261
III. Öffnungsklauseln und nationale Umsetzung	262
8. Kapitel	
Die datenschutzkonforme Unternehmensdokumentation	
nach der DS-GVO	265
I. Überblick und Problemstellung	265
II. Verzeichnis von Verarbeitungstätigkeiten	266
1. Gesetzliche Voraussetzungen	266
2. Umsetzung in der Praxis	267
III. Datenschutzrichtlinie/Löschkonzept	270
IV. Datenschutz-Folgenabschätzung	279
V. Sonstige Dokumentation	281
Sachverzeichnis	287