

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	6
II. Wie Ihnen dieses Buch hilft	8
1. Aufbau	8
2. Checklisten/Muster und Beispiele	8
3. Datenschutzrechtliche Musterdokumentation	9
2. Kapitel	
Datenschutzrechtliche Grundlagen	11
I. Was ist Datenschutz?	11
1. Datensubjekt und Informationelle Selbstbestimmung	11
2. Personenbezogene Daten – was zählt dazu?	12
3. Verarbeitungstatbestände	13
4. Gesetzliche Grundlagen	14
5. Datenschutzrechtliche Grundsätze	15
a) Verbot mit Erlaubnisvorbehalt	15
b) Auskunfts- und Korrekturrechte des Betroffenen	16
c) Datensicherheit	17
d) Rechtliche Risiken und Sanktionen	18
e) Datenvermeidung und Datensparsamkeit / Privacy by Default und Privacy by Design	20
f) Kontrolle/Der Datenschutzbeauftragte	21
II. Gesetzgeberische Aktivitäten	21
1. Datenschutzreform 2009/Inkrafttreten der DS-GVO 2018 ..	21

IX

a) Informationspflichten gemäß Art. 33 DS-GVO	22
b) Datensparsamkeit und Anonymisierung	25
c) Datenschutzbeauftragter	27
d) Auftragsdatenverarbeitung	27
e) Direktmarketing ohne Einwilligung	28
f) Direktmarketing mit Einwilligung	30
g) Stärkung der Position der Aufsichtsbehörden	30
2. Arbeitnehmerdatenschutz	31

3. Kapitel

Datenschutz in der Personalabteilung/Arbeitnehmerdatenschutz

33

I. Bewerberdaten und Bewerbungsprozess

33

1. Welche Daten dürfen erhoben werden?	33
a) Immer zulässig: Stammdaten	33
b) Schutzwürdige Daten	36
c) Vorstrafen	37
d) Schwerbehinderung und Krankheiten	38
e) Gewerkschaftszugehörigkeit	41
f) Religiöse Überzeugung	41
g) Soziale Netzwerke	42
2. Medizinische Untersuchungen und Eignungstests	44
a) Medizinische Untersuchungen	44
b) Eignungstests	45
3. Speicherdauer/Regelfristen	46
4. Weitergabe im Konzern	50
5. Online-Bewerbungen	51
6. Personalberater	53

II. Arbeitsvertrag/Erforderliche Unterlagen

55

1. Zwingend: Verpflichtung auf das Datengeheimnis	55
2. Konzernprivileg	60
3. Merkblatt Datenschutz	62

III. Datenspeicherung im Arbeitsverhältnis

62

1. Umfang der Verarbeitung	62
a) Grundsätze	62

b) Einzelfälle	64
2. Übermittlung an Dritte	65
3. Übermittlung ins Ausland	67
4. Löschung und Sperrung	69
5. Löschung nach Beendigung des Arbeitsverhältnisses	70
IV. Personalakte	71
1. Gesetzliche Rahmenbedingungen	71
2. Datenschutzrechtlich zu beachten	72
a) Zugriff auf die Personalakte	73
b) Inhalte	75
c) Rechte des Arbeitnehmers	76
V. Nutzung von Internet und E-Mail	78
1. Rechtslage bei Gestattung privater Internet- und E-Mail- Nutzung	78
a) Telekommunikationsgesetz	78
b) Zusätzlich: Arbeitnehmerdatenschutz nach der DS-GVO	81
2. Rechtslage bei Verbot privater Internet- und E-Mail- Nutzung	82
3. Ansprüche des Arbeitnehmers	82
4. Wichtig: Regeln der Internet- und E-Mail-Nutzung	83
a) Regelung in Internet- und E-Mail-Policy	84
b) Regelung in einer Betriebsvereinbarung	89
c) Checkliste: Internet- und E-Mail-Policy	93
VI. Nutzung von Telefondaten	96
1. Allgemeine Grundsätze sowie Gespräche mit einer Interessenvertretung	96
2. Call-Center und telefonische Kundenbetreuung	96
VII. Datenschutz und Betriebsrat	98
1. Geltung der DS-GVO für den Betriebsrat	98
2. Datenschutz im Betriebsrat	98
VIII. Videoüberwachung	99
1. Videoüberwachung im öffentlichen Betriebsgelände	99
2. Videoüberwachung im nicht-öffentlichen Betriebsgelände ..	103
3. Videoüberwachung in Rückzugsflächen	104

IX. Ortungssysteme	105
X. Biometrische Verfahren	108
XI. Datenerhebung bei Straftaten und Pflichtverletzungen ..	109
1. Grundsatz: Erhebung von Daten nur mit Kenntnis	109
2. Voraussetzungen der Datenerhebung	110
3. Zweckgebundenheit/Verhältnismäßigkeit	111
4. Zeitliche und technische Einschränkungen	113
XII. Datenschutzrechtliche Haftung und Strafbarkeit	114
XIII. Anonymisierter Abgleich von Daten	116
1. Straftaten und Pflichtverletzungen	116
2. Anonymisierte oder pseudonymisierte Nutzung	118
XIV. Unterrichtungspflicht bei Datenpannen sowie Beschwerderecht	119
XV. Mitarbeiterschulungen	121
XVI. Der Datenschutzbeauftragte	122
1. Pflicht zur Bestellung	122
2. Fachkunde und Zuverlässigkeit	124
3. Datenschutzbeauftragter und Betriebsrat	125
4. Bestellung des Datenschutzbeauftragten	126
5. Aufgaben des Datenschutzbeauftragten	128
6. Abberufung	130
7. Haftung	132
8. Interner und externer Datenschutzbeauftragter	133
XVII. Datenschutz bei Unternehmensverkäufen	134
XVIII. Praxischeckliste	135
4. Kapitel	
Marketing und Werbung	137
I. Kunden- und Interessentendaten	137
1. Grundsätze	137
2. Informationspflichten	138
3. Möglichkeiten und Grenzen des CRM	142

a) Nutzungsprofile	142
b) CRM in der Praxis	143
II. Online-Marketing	144
1. Internetauftritt	144
a) Impressum	144
b) Cookie Hinweis	146
c) Datenschutzerklärung	147
2. Leadgenerierung	155
a) Datenschutzrechtliche Einwilligung immer erforderlich	155
b) Inhalt	155
c) Koppelungsverbot	157
d) Wettbewerbsrechtliche Einwilligung	157
e) Confirmed Opt-In	159
3. Analyse des Nutzerverhaltens im Internet	160
a) Online Nutzungsprofile/Düsseldorfer Kreis	160
b) Google Analytics	162
III. Adressbroking	167
1. Grundsätze	167
2. Widerspruchsrecht/Hinweispflicht	169
3. Verträge mit Adressbrokern	170
IV. Dienstleister und Agenturen	172
1. Verpflichtung auf das Datengeheimnis	172
2. Datenauftragsverarbeitung	175
V. Web 2.0 und Social Media	176
1. Datenschutzniveau der jeweiligen Netzwerke	176
2. Datenschutzrechtliche Aspekte im Unternehmen	177
3. Social-Media-Policy	179
4. Facebook Fanpages/EUGH Urteil	181
VI. Praxischeckliste	183

- 5. Kapitel**
- Datenverarbeitung im Auftrag** 185
 - I. Überblick** 185
 - II. Definition/Vorliegen der Datenverarbeitung im Auftrag** .. 186
 - III. Rechtsfolgen** 188
 - 1. Überprüfung der technischen organisatorischen Maßnahmen 188
 - a) Erstauswahl 188
 - b) Erstkontrolle/Vorabkontrolle 189
 - c) Regelmäßige Kontrolle 190
 - 2. Vertragsinhalte 191
 - IV. Auslandsbezug** 192
 - 1. Systematik 192
 - 2. Kein Drittland (Beispiel Frankreich) 193
 - 3. Drittland mit angemessenem Datenschutzniveau (Beispiel Schweiz) 194
 - 4. Sonderfall USA 194
 - a) Vor dem Safe-Harbor-Urteil 194
 - b) Privacy Shield 198
 - 5. Drittland ohne angemessenes Datenschutzniveau (Beispiel Russland) 200
 - 6. EU-Standardvertragsklausel 201
 - 7. Überblick 202
 - V. Cloud-Computing** 202
 - 1. Technische Hintergründe und Begriffsdefinition 202
 - 2. Datenschutzrechtliche Bewertung 203
- 6. Kapitel**
- Technische Organisatorische Maßnahmen/Datensicherheit** 205
 - I. Datenschutz und Datensicherheit** 205
 - 1. Grundsätze 205
 - 2. Gesetzliche Rahmenbedingungen 206

II. Auditierungen	208
1. Alternativen	208
2. Einzelne IT-Sicherheitskonzepte	209
a) IT-Grundschutzkatalog	209
b) CobiT	211
c) ISO 9000	212
d) ISO/IEC 17799 und BS 7799	212
III. Umsetzung in der Praxis	213
1. Dokumentation technisch-organisatorischer Maßnahmen	213
2. IT-Security-Policy	216
7. Kapitel	
Die Datenschutz-Grundverordnung (DS-GVO)	221
I. Überblick	221
1. Sinn und Zweck	221
2. Systematik: Ein einheitlicher Rechtsrahmen	222
3. Öffnungsklauseln	223
II. Wichtigste Änderungen und Neuregelungen	223
1. Ausweitung der Interessenabwägung	223
2. Internationale Datentransfers und EU-Standardvertrags-	
klauseln	224
3. Datenschutzbeauftragter	225
4. Auftragsverarbeitung	226
5. Datenschutz-Folgenabschätzung	226
6. Technisch-organisatorische Maßnahmen nach der	
DS-GVO	227
7. Meldepflichten	228
8. Hohe Geldbußen nach der DS-GVO	229
III. Öffnungsklauseln und nationale Umsetzung	230

8. Kapitel	
Die datenschutzkonforme Unternehmensdokumentation nach der DS-GVO	233
I. Überblick und Problemstellung	233
II. Verzeichnis von Verarbeitungstätigkeiten	234
1. Gesetzliche Voraussetzungen	234
2. Umsetzung in der Praxis	235
III. Datenschutzrichtlinie/Löschkonzept	238
IV. Datenschutz-Folgenabschätzung	247
V. Sonstige Dokumentation	254
Sachverzeichnis	255