

# Inhaltsverzeichnis

<b>A. Einleitung</b>	1
<b>B. Grundlagen des Datenschutzes</b>	3
I.    Gesetze	3
1. Allgemeines	3
2. Datenschutz-Grundverordnung	4
3. DSAnpUG-EU – BDSG nF	6
4. Ausgewählte spezialgesetzliche Vorschriften	7
a) Telegesetze	7
b) Sozialdatenschutz	7
5. Landesdatenschutzgesetze	8
6. Kirchen	9
II.   Grundlegende Begriffe des Datenschutzes	10
1. Datenschutz	10
2. Daten-/Informationssicherheit	10
3. Personenbezogene Daten	11
4. Verarbeitung	14
5. Verantwortlicher	15
<b>C. Benennung des Datenschutzbeauftragten</b>	17
I.    Pflicht zur Benennung	17
II.   Ausübungsformen	20
III.  Form und Zeitpunkt der Benennung	24
IV.  Folgen der Nichtbenennung trotz Verpflichtung	25
<b>D. Anforderungen an den Datenschutzbeauftragten</b>	27
I.    Allgemeines	27
II.   Fachwissen	28
1. Juristische Kenntnisse	28
2. Betriebswirtschaftliche Kenntnisse	29
3. IT-Kenntnisse	30
4. Unternehmenskenntnisse	30
III.  Fähigkeit zur Aufgabenerfüllung	32
IV.  Unvereinbarkeit mit anderen Tätigkeiten	33
<b>E. Stellung des Datenschutzbeauftragten</b>	37
I.    Unabhängigkeit	37
1. Organisatorische Eingliederung	38
2. Benachteiligungs-/Abberufungsverbot	38

3.	Weisungsfreiheit .....	41
4.	Unterstützungsverpflichtung des Verantwortlichen/Auftragsverarbeiters .....	42
II.	Verschwiegenheit .....	43
III.	Haftung .....	45
<b>F.</b>	<b>Aufgaben des Datenschutzbeauftragten .....</b>	<b>49</b>
I.	Allgemeines .....	49
II.	Aufgaben im Einzelnen .....	57
1.	Überwachung der Rechtmäßigkeit der Datenverarbeitung ..	57
a)	Einwilligung .....	58
b)	Gesetzliche Erlaubnistatbestände .....	63
c)	Zweckänderung .....	65
d)	Besondere Kategorien personenbezogener Daten .....	66
e)	Grundsätze des Art. 5 DS-GVO .....	70
2.	Beratung und Überwachung im Zusammenhang mit der Datenschutz-Folgenabschätzung .....	72
a)	Zuständigkeit .....	73
b)	Voraussetzungen .....	74
c)	Durchführung .....	77
d)	Konsultation der Aufsichtsbehörde .....	81
3.	Führen des Verzeichnisses von Verarbeitungstätigkeiten .....	82
4.	Beratung und Überwachung hinsichtlich der Wahrung der Rechte der betroffenen Personen .....	85
a)	Allgemeines .....	85
b)	Modalitäten und Verfahren .....	86
c)	Übersicht über die einzelnen Rechte der betroffenen Person .....	88
d)	Informationspflichten .....	89
e)	Auskunftsrecht nach Art. 15 DS-GVO .....	94
f)	Recht auf Berichtigung nach Art. 16 DS-GVO .....	99
g)	Recht auf Löschung („Recht auf Vergessenwerden“) nach Art. 17 DS-GVO .....	101
h)	Recht auf Einschränkung der Verarbeitung nach Art. 18 DS-GVO .....	106
i)	Widerspruchsrecht nach Art. 21 DS-GVO .....	109
j)	Recht auf Datenübertragbarkeit nach Art. 20 DS-GVO ..	110
5.	Auswahl und Kontrolle von Dienstleistern .....	114
a)	Allgemeines .....	114
b)	Auftragsverarbeitung .....	114
c)	Gemeinsam Verantwortliche .....	120
6.	Prüfung internationaler Datentransfers .....	123
a)	Allgemeines .....	123
b)	Angemessenheitsbeschluss .....	124
c)	Geeignete Garantien .....	126
7.	Erfüllung der Meldepflichten bei Datenpannen .....	131
a)	Meldung an die Aufsichtsbehörde .....	131

b) Benachrichtigungspflicht gegenüber den betroffenen Personen . . . . .	136
8. Zusammenarbeit mit der Aufsichtsbehörde einschließlich der vorherigen Konsultation . . . . .	138
9. Sensibilisierung und Schulung . . . . .	139
10. Mitwirkung in Mitbestimmungsprozessen . . . . .	140
11. Erstellen eines Tätigkeitsberichts . . . . .	141
12. Erarbeitung und Pflege eines Datenschutz-Handbuchs . . . . .	141
III. Aufbau und Umsetzung eines Datenschutz-Managementsystems (DSMS) . . . . .	142

## **G. Die technischen und organisatorischen Maßnahmen . . . . . 147**

I. Grundlagen . . . . .	147
1. Einleitung und Grundlagen . . . . .	147
2. Datenschutzziele . . . . .	149
a) Vertraulichkeit . . . . .	149
b) Integrität . . . . .	150
c) Verfügbarkeit . . . . .	150
d) Belastbarkeit . . . . .	150
3. Mögliche erweiterte Datenschutzziele gemäß anderer Datenschutzgesetze . . . . .	151
a) Authentizität . . . . .	151
b) Revisionsfähigkeit . . . . .	151
c) Transparenz . . . . .	151
II. Risikobasierter Bewertungsansatz . . . . .	152
1. Juristische Grundlagen . . . . .	153
2. Angemessenheitsprinzip . . . . .	153
3. Technische „Privacy by“-Anforderungen . . . . .	154
a) Privacy by Design . . . . .	155
b) Privacy by Default . . . . .	155
III. Umsetzung der Datenschutzziele . . . . .	156
1. Berechtigungsbasierte Maßnahmen . . . . .	156
a) Zutrittsregelungen . . . . .	157
b) Zugangsrichtlinien . . . . .	159
c) Zugriffrechte . . . . .	161
2. Schutz bei Systemen . . . . .	161
a) Physikalische und umweltbezogene Maßnahmen . . . . .	161
b) Kryptografie . . . . .	163
c) Maßnahmen zum Schutz vor bössartiger Software . . . . .	164
d) Sichere Kommunikation . . . . .	165
e) Verfügbarkeitssicherung . . . . .	165
3. Prozessbetreffende Maßnahmen . . . . .	167
a) Einführung von IT-Systemen . . . . .	167
b) Beschaffung, Abnahme, Freigabe . . . . .	170
c) Wartung . . . . .	170
d) Protokolldatenerfassung und -auswertung . . . . .	172
e) Sichere Vernichtung von Datenträgern/Unterlagen . . . . .	174

IV.	Informationssicherheitsmanagement (ISMS) . . . . .	175
1.	ISMS als bewährter Schutz . . . . .	175
2.	Datenschutz-Management-System als Ableitung eines ISMS . . . . .	176
V.	Normen . . . . .	177
VI.	Vertiefende Informationen . . . . .	179
<b>H.</b>	<b>Checklisten . . . . .</b>	<b>181</b>
I.	Checkliste zu Kapitel C „Benennung des Datenschutzbeauftragten“ . . . . .	181
II.	Checkliste zu Kapitel D „Anforderung an den Datenschutzbeauftragten“ . . . . .	181
III.	Checkliste zu Kapitel E „Stellung des Datenschutz- beauftragten“ . . . . .	182
IV.	Checkliste zu Kapitel F „Aufgaben des Datenschutz- beauftragten“ . . . . .	182
1.	Überwachung der Rechtmäßigkeit der Verarbeitung durch Einwilligung . . . . .	182
2.	Beratung und Überwachung im Zusammenhang mit der Datenschutz-Folgenabschätzung . . . . .	183
a)	Voraussetzung . . . . .	183
b)	Durchführung . . . . .	183
3.	Führen des Verzeichnisses von Verarbeitungstätigkeiten . . . . .	183
4.	Beratung und Überwachung hinsichtlich der Wahrung der Rechte der betroffenen Personen . . . . .	184
a)	Recht auf Information nach Art. 13, 14 DS-GVO . . . . .	184
b)	Identifikation im Rahmen des Auskunftsrechts nach Art. 15 . . . . .	184
c)	Inhalt der Auskunft . . . . .	184
d)	Recht auf Berichtigung nach Art. 16 DS-GVO . . . . .	185
e)	Recht auf Löschung („Recht auf Vergessenwerden“) nach Art. 17 DS GVO . . . . .	185
f)	Recht auf Einschränkung der Verarbeitung nach Art. 18 DS-GVO . . . . .	185
g)	Widerspruchsrecht nach Art. 21 DS-GVO . . . . .	186
h)	Recht auf Datenübertragbarkeit nach Art. 20 DS-GVO . . . . .	186
5.	Auswahl und Kontrolle Dienstleister . . . . .	186
a)	Auftragsdatenverarbeitung . . . . .	186
b)	Gemeinsame Verantwortliche . . . . .	187
6.	Erfüllung der Meldepflicht bei Datenpannen . . . . .	187
7.	Sensibilisierung und Schulung . . . . .	188
8.	Mitwirkung in Mitbestimmungsprozessen . . . . .	188
9.	Erstellen eines Tätigkeitsberichts . . . . .	189
10.	Erarbeitung und Pflege eines Datenschutz-Handbuchs . . . . .	189
11.	Aufbau und Umsetzung eines Datenschutz-Management- systems . . . . .	189

V.	Checkliste zu Kapitel G „Die technischen und organisatorische Maßnahmen“	190
1.	Berechtigungs-basierte Maßnahmen	190
a)	Zutrittsregelungen	190
b)	Zugangsrichtlinien	190
c)	Zugriffsrechte	190
2.	Schutz bei Systemen	190
3.	Prozessbetreffende Maßnahmen	191
4.	Informationssicherheitsmanagement (ISMS)	192
<b>Sachverzeichnis</b>		<b>195</b>