

# Inhaltsverzeichnis

Vorwort .....	V
Abkürzungsverzeichnis .....	XV
Musterverzeichnis .....	XVII
<b>1. Auf einen Blick .....</b>	<b>1</b>
1.1. Step-by-Step .....	1
1.2. Must-haves .....	2
1.2.1. Verzeichnis der Verarbeitungstätigkeiten .....	3
1.2.2. Datenschutzerklärung .....	3
1.2.3. Speicher-/Löschkonzept .....	3
1.2.4. Strategie für Anfragebeantwortung .....	4
1.2.5. Auftragsverarbeitungsvertrag .....	4
1.2.6. Datenschutz-Audit .....	4
1.3. No-Gos .....	4
1.3.1. Nichtausreichende Einwilligung .....	4
1.3.2. Mangelnde Sicherheitsmaßnahmen .....	5
1.3.3. Verspätete Meldung von Datenschutzverletzungen ....	5
1.3.4. Verhalten gegenüber der Aufsichtsbehörde .....	5
<b>2. Grundlagen .....</b>	<b>7</b>
2.1. Rechtsgrundlagen .....	7
2.2. Grundrecht auf Datenschutz .....	9
2.3. Anwendungsbereich der DSGVO .....	10
2.3.1. Worauf ist die DSGVO anwendbar? .....	10
2.3.2. Auf wen bzw wo ist die DSGVO anwendbar? .....	11
2.4. Kontrolle .....	14
2.4.1. Wer überprüft die Einhaltung der DSGVO? .....	14
2.4.2. Welche Aufgaben hat die Aufsichtsbehörde? .....	15
2.4.3. Wer kontrolliert die Aufsichtsbehörde? .....	16
2.5. Wichtige Begriffe .....	16
2.6. Akteure im Datenschutzrecht .....	21
2.6.1. Wer ist Verantwortlicher? .....	22
2.6.2. Was sind Gemeinsam Verantwortliche? .....	23
2.6.3. Wer ist Auftragsverarbeiter? .....	25
2.6.4. Wer sind Dritte? .....	26
2.6.5. Wer ist Empfänger? .....	27
2.6.6. Wie finde ich meine Rolle? .....	27
<b>3. Grundsätze der Verarbeitung .....</b>	<b>29</b>
3.1. Prinzipien .....	29
3.1.1. Rechtmäßigkeitsgrundsatz .....	30

3.1.2.	Verarbeitung nach Treu und Glauben .....	31
3.1.3.	Transparenzgrundsatz .....	31
3.1.4.	Zweckbindung .....	32
3.1.5.	Datenminimierung .....	34
3.1.6.	Richtigkeit .....	34
3.1.7.	Speicherbegrenzung .....	35
3.1.8.	Integrität und Vertraulichkeit .....	36
3.1.9.	Rechenschaftspflicht .....	36
3.2.	Rechtmäßigkeit .....	37
3.2.1.	Welche Rechtsgrundlagen gibt es? .....	39
3.2.1.1.	Einwilligung .....	39
3.2.1.2.	Vertragserfüllung .....	45
3.2.1.3.	Erfüllung einer rechtlichen Verpflichtung .....	47
3.2.1.4.	Lebenswichtige Interessen .....	48
3.2.1.5.	Wahrnehmung einer Aufgabe im öffentlichen Interesse .....	48
3.2.1.6.	Berechtigte Interessen des Verantwortlichen oder eines Dritten. ....	49
3.2.2.	Wann darf ich besondere Kategorien von Daten verarbeiten? .....	51
3.2.2.1.	Ausdrückliche Einwilligung .....	52
3.2.2.2.	Rechte und Pflichten aus Arbeits- und Sozialrecht ...	53
3.2.2.3.	Lebenswichtige Interessen .....	53
3.2.2.4.	Mitgliederdaten .....	53
3.2.2.5.	Offensichtlich öffentlich machen .....	54
3.2.2.6.	Rechtsansprüche .....	54
3.2.2.7.	Erhebliches öffentliches Interesse .....	54
3.2.2.8.	Gesundheits- und Sozialbereich .....	55
3.2.2.9.	Öffentliches Interesse im Bereich der öffentlichen Gesundheit .....	55
3.2.2.10.	Archiv-, Forschungs- oder statistische Zwecke .....	55
3.2.3.	Wann darf ich strafrechtlich relevante Daten verarbeiten? .....	55
3.3.	Exkurs: Profiling und automatisierte Entscheidungsfindung .....	56
3.3.1.	Wann ist Profiling erlaubt? .....	56
3.3.2.	Wann ist automatisierte Entscheidungsfindung erlaubt? .....	57
<b>4.</b>	<b>Pflichten der Akteure .....</b>	<b>60</b>
4.1.	Verzeichnis der Verarbeitungstätigkeiten .....	60
4.1.1.	Was muss das Verzeichensverzeichnis beinhalten? .....	61
4.1.2.	In welcher Form muss das Verzeichensverzeichnis geführt werden? .....	65

4.2.	Datenschutzerklärung .....	66
4.2.1.	Wie erteile ich transparente Informationen? .....	67
4.2.2.	Inhalt einer Datenschutzerklärung .....	72
4.2.2.1.	Erhebung personenbezogener Daten bei der betroffenen Person .....	73
4.2.2.2.	Erhebung von personenbezogenen Daten nicht bei der betroffenen Person .....	81
4.2.2.3.	Ausnahmen von der Informationspflicht .....	81
4.2.3.	Änderung der Datenschutzerklärung .....	82
4.3.	Bestellung eines Datenschutzbeauftragten .....	83
4.3.1.	Wann muss ein Datenschutzbeauftragter bestellt werden? .....	83
4.3.2.	Wer kann als Datenschutzbeauftragter bestellt werden? .....	85
4.3.3.	Welche Stellung hat der Datenschutzbeauftragte? .....	85
4.4.	DSFA .....	86
4.4.1.	Wann ist eine DSFA notwendig .....	89
4.4.2.	Wie mache ich eine DSFA? .....	94
4.4.2.1.	Gegenstand der DSFA .....	94
4.4.2.2.	Form .....	94
4.4.2.3.	Inhalt .....	94
4.4.3.	Konsultation mit der Datenschutzbehörde .....	98
4.5.	Speicher-/Löschkonzept .....	98
4.6.	Datensicherheit .....	102
4.6.1.	Was ist Privacy by Design? .....	102
4.6.2.	Was ist Privacy by Default? .....	103
4.6.3.	Welche TOM sind zu treffen? .....	104
4.6.4.	Müssen Maßnahmen laufend evaluiert werden? .....	105
4.7.	Meldung von Datenschutzverletzungen (Data Breach Notification) .....	107
4.7.1.	Was ist ein Data Breach? .....	107
4.7.2.	Wann und wie melde ich an die Datenschutzbehörde? .....	108
4.7.3.	Wann und wie melde ich an Betroffene? .....	112
4.7.4.	Was muss dokumentiert werden? .....	113
4.8.	Datenschutz-Audit .....	114
4.8.1.	Wie oft sollte ein Audit durchgeführt werden? .....	115
4.8.2.	Was sollte ein Audit beinhalten? .....	115
<b>5.</b>	<b>Bildverarbeitung</b> .....	<b>118</b>
5.1.	Was ist Bildverarbeitung? .....	118
5.2.	Unter welchen Voraussetzungen ist Bildverarbeitung zulässig? ...	119
5.3.	Exkurs: Medienprivileg .....	120

5.4.	Welche besonderen Sicherheitsmaßnahmen müssen getroffen werden? .....	121
5.5.	Wie ist Bildverarbeitung zu kennzeichnen? .....	121
<b>6.</b>	<b>Arbeit mit Dritten</b> .....	<b>123</b>
6.1.	Auftragsverarbeiter .....	123
6.1.1.	Was ist bei der Auswahl von Auftragsverarbeitern zu beachten? .....	123
6.1.2.	Was ist beim Einsatz von Sub-Auftragsverarbeitern zu beachten? .....	124
6.1.3.	Wer haftet für Verstöße? .....	125
6.1.4.	Wie ist ein Auftragsverarbeitungsvertrag zu gestalten? .....	126
6.2.	Gemeinsame Verantwortliche .....	133
6.2.1.	Wer haftet bei Verstößen? .....	133
6.2.2.	Wie ist eine Joint-Controller-Vereinbarung zu gestalten? .....	134
6.2.3.	Welche Informationen müssen offengelegt werden? .....	138
6.3.	Getrennte Verantwortliche .....	139
6.4.	Datenübermittlungen .....	143
6.4.1.	Unter welcher Voraussetzung ist Datenübermittlung zulässig? .....	143
6.4.2.	Was gilt es bei Datenübermittlungen ins Ausland zu beachten? .....	145
6.4.2.1.	Angemessenheitsbeschluss der EU-Kommission .....	145
6.4.2.2.	Spezialfall USA .....	146
6.4.2.3.	Geeignete Garantien .....	149
6.4.2.3.1.	Standarddatenschutzklauseln .....	149
6.4.2.3.2.	BCR .....	150
6.4.2.4.	Ausnahmen für bestimmte Fälle (Art 49 DSGVO) ...	151
6.4.2.5.	Auffangtatbestand zwingende berechnete Interessen ...	153
6.4.2.6.	Genehmigung durch die Datenschutzbehörde .....	155
6.4.3.	Entscheidungshilfe Rechtmäßigkeit der Datenübermittlung .....	156
<b>7.</b>	<b>Datenschutz und Arbeitsrecht</b> .....	<b>157</b>
7.1.	Zulässigkeit der Verarbeitung .....	158
7.1.1.	Unter welchen Voraussetzungen ist die Verarbeitung der Daten von Arbeitnehmer*innen zulässig? .....	158
7.1.2.	Was gilt es bei besonderen Kategorien personenbezogener Daten zu beachten? .....	160

7.1.3.	Was gilt es bei strafrechtlich relevanten Daten zu beachten? .....	161
7.1.4.	Wie lange dürfen Arbeitnehmerdaten gespeichert werden? .....	162
7.2.	Bewerberdaten .....	163
7.2.1.	Unter welche Voraussetzungen ist die Verarbeitung von Bewerberdaten zulässig? .....	163
7.2.2.	Wie können die Informationspflichten erfüllt werden? .....	164
7.2.3.	Wie lange dürfen Bewerbungsdaten gespeichert werden? .....	164
7.3.	Datengeheimnis .....	165
7.3.1.	Müssen Arbeitnehmer*innen zur Einhaltung des Datengeheimnisses verpflichtet werden? .....	165
7.3.2.	In welcher Form muss die Verpflichtung erfolgen? ....	166
7.4.	Betriebsrat .....	166
7.4.1.	Hat der Betriebsrat ein Mitspracherecht bzgl Arbeitnehmerdatenverarbeitung? .....	167
7.4.2.	Welchen Maßnahmen muss der Betriebsrat zustimmen? .....	167
7.5.	Remote Working .....	168
7.5.1.	Welche datenschutzrechtlichen Regelungen gelten für Remote Working? .....	169
7.5.2.	Welche zusätzlichen Maßnahmen sollten iZm Remote Working getroffen werden? .....	169
7.6.	Die Kontrolle von Arbeitnehmer*innen .....	170
7.6.1.	Ist eine Kontrolle der Internetnutzung zulässig? .....	171
7.6.2.	Dürfen Arbeitnehmer*innen videoüberwacht werden? .....	173
7.6.3.	Wie können Hinweisgebersysteme eingesetzt werden? .....	175
<b>8.</b>	<b>Konkrete Anwendungsfälle</b> .....	<b>178</b>
8.1.	Kundendaten .....	178
8.1.1.	Was gilt es bei der Erhebung von Kundendaten zu beachten? .....	178
8.1.2.	Wie kann eine ausreichende Information über die Datenverarbeitung gegeben werden? .....	180
8.2.	Cookies, Werbe-Identifizier & ähnliche Technologien .....	181
8.2.1.	Ist für den Einsatz von Cookies und Werbe-Identifizieren die Einwilligung der Betroffenen notwendig? .....	182
8.2.2.	Wie kann die Einwilligung eingeholt werden? .....	183

8.3.	Social Media .....	184
8.3.1.	Wie können Share/Like Buttons datenschutzkonform eingebunden werden? .....	185
8.3.2.	Wie können Posts und Widgets datenschutzkonform eingebunden werden? .....	187
8.3.3.	Was gilt es bei Social-Media-Profilen zu beachten? ..	188
8.4.	Kommunikationstools .....	192
8.4.1.	Wie können Kommunikationstools datenschutzkonform eingesetzt werden? .....	193
8.4.2.	Ist ein Auftragsverarbeitungsvertrag notwendig? .....	194
8.5.	Newsletter/E-Mail-Marketing .....	195
8.5.1.	Ist für Newsletter und E-Mail-Marketing die Einwilligung der Betroffenen notwendig? .....	195
8.5.2.	Ist ein Auftragsverarbeitungsvertrag notwendig? .....	198
8.6.	M&A-Transaktionen .....	198
8.6.1.	Wer nimmt welche Rolle ein? .....	199
8.6.2.	Unter welchen Voraussetzungen ist eine Datenverarbeitung zulässig? .....	200
8.6.3.	Dürfen sämtliche Arbeitnehmer-/Kundendaten offengelegt werden? .....	201
8.6.4.	Wie müssen Betroffene über die Datenverarbeitung informiert werden? .....	202
<b>9.</b>	<b>Betroffenenrechte</b> .....	<b>204</b>
9.1.	Die Rechte im Detail .....	205
9.1.1.	Auskunftsrecht (Art 15 DSGVO) .....	205
9.1.2.	Recht auf Berichtigung (Art 16 DSGVO) .....	206
9.1.3.	Recht auf Löschung (Art 17 DSGVO) .....	207
9.1.4.	Recht auf Einschränkung (Art 18 DSGVO) .....	209
9.1.5.	Recht auf Datenübertragbarkeit (Art 20 DSGVO) ....	210
9.1.6.	Recht auf Widerspruch (Art 21 DSGVO) .....	211
9.1.7.	Recht auf Widerruf der Einwilligung (Art 7 Abs 3 DSGVO) .....	212
9.1.8.	Beschwerderecht (Art 77 DSGVO) .....	213
9.2.	Beantwortung von Anfragen .....	213
9.2.1.	Was ist immer zu beachten? .....	214
9.2.1.1.	Medium .....	214
9.2.1.2.	Frist für Beantwortung .....	215
9.2.1.3.	Identitätsfeststellung .....	215
9.2.1.4.	Verbesserung .....	217
9.2.1.5.	Kosten .....	217
9.2.2.	Wie beantworte ich ein Auskunftsansuchen? .....	218
9.2.3.	Wie beantworte ich ein Berichtigungsansuchen? .....	223

9.2.4.	Wie beantworte ich ein Löschbegehren? .....	223
9.2.5.	Wie beantworte ich ein Einschränkungsbegehren? ...	225
9.2.6.	Wie beantworte ich ein Begehren auf Datenübertragung? .....	225
9.2.7.	Wie behandle ich einen Widerspruch? .....	226
9.2.8.	Wie behandle ich einen Widerruf der Einwilligung? .....	226
9.2.9.	Wie gehe ich mit einer Beschwerde um? .....	227
<b>10.</b>	<b>Konsequenzen</b> .....	228
10.1.	Geldbußen .....	228
10.1.1.	Wie hoch sind die Geldbußen? .....	228
10.1.2.	Wer haftet für Geldbußen? .....	231
10.2.	Andere Sanktionen .....	233
<b>11.</b>	<b>Prüfschema: Rechtmäßigkeit der Datenverarbeitung</b> .....	235
	Stichwortverzeichnis .....	237