

# Inhalt

<b>1</b>	<b>ERSTER ÜBERBLICK: WORUM GEHT ES? . . . . .</b>	<b>11</b>
1.1	Weshalb der Datenschutz für Sie wichtig ist . . . . .	11
1.2	Ziel und Zielgruppe des Ratgebers . . . . .	12
1.3	Die Datenschutzgrundverordnung gilt für alle . . . . .	13
1.4	Weshalb die Relevanz des Datenschutzes steigt . . . . .	15
<b>2</b>	<b>DIESE GRUNDLAGEN DES DATENSCHUTZES MÜSSEN SIE KENNEN . . . . .</b>	<b>17</b>
2.1	Anwendbarkeit des Datenschutzrechts . . . . .	17
2.1.1	Welche Daten werden von der DSGVO geschützt? . . . . .	17
2.1.2	Wo gilt die DSGVO überall? . . . . .	19
2.2	Die zentralen Begriffe müssen Sie kennen . . . . .	19
2.2.1	Von zentraler Bedeutung: »personenbezogene Daten« und »betroffene Person« . . . . .	19
2.2.2	Die »verantwortliche Stelle« sind Sie! . . . . .	23
2.2.3	Die »Verarbeitung« von Daten steht im Mittelpunkt . . . . .	23
2.3	Diese Regeln müssen Sie einhalten . . . . .	24
2.3.1	Der Rechtmäßigkeitsgrundsatz: ein Verbot unter Vorbehalt . . . . .	24
2.3.2	Der Zweckbindungsgrundsatz: Verwendung für einen eindeutigen Zweck . . . . .	25
2.3.3	Das Prinzip der Speicherbegrenzung: Nur so lange erforderlich! . . . . .	26
2.3.4	Unbedingt beachten: Das Prinzip der Integrität und Vertraulichkeit . . . . .	28
2.4	Diese Rechte stehen Betroffenen zu . . . . .	28
2.5	Diese Pflichten haben Sie als Verantwortlicher . . . . .	30
<b>3</b>	<b>RECHTSGRUNDLAGEN – WANN IST IHRE DATENVERARBEITUNG LEGAL? . . . . .</b>	<b>33</b>
3.1	Erfüllung eines Vertrages/Durchführung vorvertraglicher Maßnahmen . . . . .	33
3.2	Erfüllung rechtlicher Verpflichtungen . . . . .	35

3.3	Schutz lebenswichtiger Interessen. . . . .	36
3.4	Für Behörden und andere öffentliche Stellen: Ausübung öffentlicher Gewalt . . . . .	36
3.5	Überwiegende berechtigte Interessen. . . . .	37
3.6	Einwilligung . . . . .	39
3.6.1	Wie eine Einwilligung zur Datenverarbeitung abgegeben werden muss. . . . .	39
3.6.2	Musterformulierungen für eine Einwilligungs- erklärung . . . . .	41
3.7	Sehr sensibel: besondere Kategorien personenbezogener Daten. . . . .	42
3.8	Verarbeitung von Beschäftigtendaten. . . . .	44
<b>4</b>	<b>DER DATENSCHUTZBEAUFTRAGTE (DSB) – DAS UNBEKANNTES WESEN? . . . . .</b>	<b>47</b>
4.1	Prüfung der DSB-Pflicht . . . . .	47
4.1.1	Es kommt auf die Kerntätigkeit an. . . . .	47
4.1.2	Die Zahl der Mitarbeiter ist ausschlaggebend . . . . .	48
4.2	Wer ist zum DSB geeignet? . . . . .	49
4.3	Wie wird der DSB richtig ernannt? . . . . .	52
4.3.1	Veröffentlichung der Kontaktdaten des DSB . . . . .	53
4.3.2	Die Meldung des DSB an die Aufsichtsbehörde ist Pflicht . . . . .	53
4.4	Aufgaben und Stellung des DSB . . . . .	54
4.5	Geringes Risiko: die Haftung des DSB . . . . .	57
<b>5</b>	<b>DIESE INFORMATIONSPFLICHTEN MÜSSEN SIE ERFÜLLEN . . . . .</b>	<b>59</b>
5.1	Allgemeine Datenschutzhinweise für Ihre Offline-Tätigkeit . . . . .	60
5.1.1	Pflichtinformationen . . . . .	60
5.1.2	Umsetzung in die Praxis . . . . .	62
5.1.3	So können Datenschutzhinweise aussehen. . . . .	62
5.2	Die Datenschutzerklärung für Ihre Web-Präsenzen . . . . .	67
5.2.1	Weitere Pflichtinformationen müssen enthalten sein . . . . .	67
5.2.2	Die praktische Umsetzung auf Ihrer Website . . . . .	68
5.2.3	Umsetzung in Ihren Social-Media-Profilen . . . . .	73

5.3	Diese Probleme könnten Ihnen bei Ihrer Website begegnen . . . . .	76
5.3.1	Aus Datenschutzsicht nicht ganz ungefährlich: der Einsatz von Analyse-Tools. . . . .	76
5.3.2	Vorsicht beim Einsatz von Cookies . . . . .	79
5.3.3	Was Sie beim Einsatz von Kontaktformularen beachten müssen . . . . .	85
5.3.4	So sichern Sie Ihre Website mit einem SSL-/TLS-Zertifikat ab . . . . .	88
<b>6</b>	<b>WAS SIE BEI EINZELNEN WERBEMASSNAHMEN BEACHTEN MÜSSEN. . . . .</b>	<b>91</b>
6.1	Diese Spielregeln gelten für Werbeanrufe . . . . .	92
6.2	Werbung per Post: altmodisch, aber sicher . . . . .	95
6.3	Augen auf bei elektronischer Werbung . . . . .	96
6.3.1	Formen der elektronischen Werbung . . . . .	97
6.3.2	Bitte beachten: das Double-Opt-In-Verfahren . . . . .	98
6.3.3	Für die Praxis relevant: Ausnahme bei Bestandskunden . . . . .	102
6.3.4	Checkliste elektronische Werbung . . . . .	103
<b>7</b>	<b>EINE LÄSTIGE PFLICHT: DIE INTERNE DATENSCHUTZDOKUMENTATION . . . . .</b>	<b>105</b>
7.1	So gestalten Sie das Verarbeitungsverzeichnis (VVT) . . . . .	105
7.1.1	Der Aufbau des VVT einer verantwortlichen Stelle. . . . .	105
7.1.2	Auftragsverarbeiter müssen ein zusätzliches VVT führen . . . . .	113
7.1.3	In der Praxis kaum von Bedeutung: Ausnahmefälle . . . . .	115
7.2	Welche technischen und organisatorischen Maßnahmen (TOMs) sind in Ihrem Unternehmen sinnvoll? . . . . .	116
7.2.1	Sie müssen Ihr eigenes Risiko bewerten . . . . .	117
7.2.2	So setzen Sie geeignete TOMs in die Praxis um . . . . .	123
7.2.3	Bitte beachten: das Verfahren zur regelmäßigen Selbstüberprüfung (PDCA-Zyklus) . . . . .	129
7.3	Standards/Zertifizierungen . . . . .	131
7.4	Diese Anlagen passen zum VVT. . . . .	132
7.5	So kann ein VVT aussehen . . . . .	135

<b>8</b>	<b>DATENÜBERMITTLUNGEN – SO GELINGEN SIE RECHTSKONFORM ..</b>	<b>137</b>
8.1	Das ist bei einem Auftragsverarbeitungsverhältnis zu beachten .....	138
8.1.1	Typische Beispiele von AV-Verhältnissen .....	139
8.1.2	In diesen Fällen handelt es sich nicht um AV-Verhältnisse.....	141
8.1.3	Wichtig: der AV-Vertrag .....	143
8.2	Wie »die gemeinsame Verantwortlichkeit« zu regeln ist .....	146
8.2.1	Typische Beispiele gemeinsamer Verantwortlichkeit....	146
8.2.2	Der Joint-Controllership-Vertrag.....	148
8.3	Die getrennte Verantwortlichkeit bei der Datenübermittlung ..	151
8.4	Das ist bei einer Datenübermittlung ins Ausland wichtig.....	152
8.4.1	Die EU-/EWR-Staaten sind unproblematisch .....	153
8.4.2	Nicht-EU-Staaten mit angemessenem Schutzniveau....	154
8.4.3	Bei unsicheren Drittstaaten sind weitere Maßnahmen notwendig .....	154
8.5	Datenübermittlung in der Praxis: Übersicht über die eigenen Datenflüsse .....	163
<b>9</b>	<b>DER RICHTIGE UMGANG MIT BETROFFENENRECHTEN .....</b>	<b>167</b>
9.1	So reagieren Sie richtig .....	167
9.1.1	First things first: Prüfung der Identität .....	168
9.1.2	Erfüllung der Betroffenenrechte: zeitnah, transparent und korrekt .....	170
9.1.3	Unbekannte Person: Negativauskunft oder Ablehnung des Antrags .....	172
9.2	Recht auf Auskunft .....	174
9.2.1	Welche Daten müssen Sie mitteilen? .....	174
9.2.2	Eine korrekte Antwort in der Praxis .....	177
9.3	Recht auf Berichtigung .....	179
9.4	Recht auf Löschung .....	180
9.4.1	Wann müssen Daten gelöscht werden? .....	180
9.4.2	In diesen Fällen müssen personenbezogene Daten nicht gelöscht werden.....	182
9.4.3	Das Recht auf Vergessenwerden .....	184
9.4.4	Auch ein Antrag auf Löschung muss beantwortet werden .....	185

9.5	Recht auf Einschränkung .....	186
9.6	Recht auf Datenübertragbarkeit .....	187
9.7	Recht auf Widerspruch .....	189
9.8	Recht auf Widerruf einer erteilten Einwilligung .....	190
9.9	Recht auf Beschwerde .....	191
<b>10</b>	<b>BEI VERSTÖSSEN GEGEN DAS DATENSCHUTZRECHT DROHEN STRAFEN .....</b>	<b>193</b>
10.1	Die Aufgaben der Aufsichtsbehörden .....	193
10.2	Diese Sanktionen können die Aufsichtsbehörden verhängen ..	194
10.2.1	Unterlassungsverfügung heißt »Stopp« .....	194
10.2.2	Geldbußen: Es gibt leichte und schwere Verstöße ..	195
10.2.3	Wie berechnet sich die Höhe von Bußgeldern? .....	196
10.3	Betroffene Personen können Schadensersatz fordern .....	203
10.4	Auch möglich: Abmahnungen von der Konkurrenz .....	206
<b>11</b>	<b>DATENPANNEN – WAS MUSS WANN AN WEN GEMELDET WERDEN? .....</b>	<b>209</b>
11.1	So erkennen Sie Datenpannen .....	209
11.2	Die Meldung an die Aufsichtsbehörde .....	212
11.3	Worst-Case-Szenario: Meldung an Betroffene .....	216
11.3.1	Liegt ein »hohes« Risiko vor? .....	216
11.3.2	Die Datenpanne muss den Betroffenen gemeldet werden .....	218
11.3.3	In Ausnahmen ist eine Benachrichtigung nicht notwendig .....	220
11.4	Für den Notfall gerüstet sein .....	221
<b>12</b>	<b>DIE DATENSCHUTZ-FOLGENABSCHÄTZUNG (DSFA) .....</b>	<b>225</b>
12.1	Werden Sie auf der Positiv-Liste fündig? .....	226
12.2	Die Leitlinien der Artikel-29-Gruppe können weiterhelfen ..	228
12.3	Und was sagt das Gesetz? .....	230
12.4	Durchführung einer DSFA .....	231

<b>13</b>	<b>DATENSCHUTZ IM BESCHÄFTIGENVERHÄLTNIS .....</b>	<b>235</b>
13.1	Verpflichtung auf Vertraulichkeit .....	235
13.2	Privatnutzung von Telefon, Internet & E-Mail .....	237
13.3	Home-Office, Tele-Arbeit & Co. ....	239
13.4	Umgang mit Bewerberdaten .....	243
13.5	Datenschutz bei Videokonferenzen & Messenger-Diensten....	245
13.5.1	Das sollten Sie bei Videokonferenzen beachten.....	246
13.5.2	Nutzung von Messenger-Diensten .....	249
<b>14</b>	<b>»ALL-IN-CHECKLISTE«: DIE UMSETZUNG DES DATENSCHUTZES SCHRITT FÜR SCHRITT .....</b>	<b>251</b>
<b>15</b>	<b>TOOLBOX .....</b>	<b>255</b>
15.1	Überblick Datenschutz-Software .....	255
15.2	Datenschutz-Podcasts – hören Sie doch mal rein.....	256
15.3	Kostenlose Newsletter.....	257
15.4	Nützliche Internetseiten .....	258
	<b>ABKÜRZUNGSVERZEICHNIS .....</b>	<b>261</b>
	<b>INDEX .....</b>	<b>263</b>