

# Inhalt

Geleitwort .....	13
------------------	----

## **1 Einführung** 15

---

<b>1.1</b>	<b>An wen richtet sich dieses Buch?</b> .....	16
<b>1.2</b>	<b>Was ist die europäische Datenschutz-Grundverordnung?</b> .....	18
<b>1.3</b>	<b>Was bringt die europäische Datenschutz-Grundverordnung?</b> .....	20
<b>1.4</b>	<b>Ist eine Anpassung an die neue Rechtslage zwingend?</b> .....	21
<b>1.5</b>	<b>Welche Maßnahmen müssen unbedingt eingeleitet werden?</b> .....	26
<b>1.6</b>	<b>Warum ist rechtliche Hilfe unverzichtbar?</b> .....	28
<b>1.7</b>	<b>Wie kann man sich immer auf dem neusten Stand halten?</b> .....	28
<b>1.8</b>	<b>Dankeschön!</b> .....	29

## **2 Neuordnung durch Grundordnung: Das neue europäische Datenschutzrecht** 31

---

<b>2.1</b>	<b>Überblick: Wesentliche Änderungen durch die DSGVO</b> .....	32
2.1.1	Datenschutz als europäisches Grundrecht der Bürger .....	33
2.1.2	Marktortprinzip – vereinheitlichtes Regelwerk für Unternehmen .....	34
2.1.3	Rechenschaftspflicht .....	35
2.1.4	Reformierung des Beschwerdesystems .....	35
2.1.5	Umsetzungsanreiz aufgrund hoher Geldbußenrahmen .....	37
<b>2.2</b>	<b>Datenschutzprinzipien</b> .....	38
2.2.1	Grundsatz der Rechtmäßigkeit und der Transparenz/ Verarbeitung nach Treu und Glauben .....	38
2.2.2	Grundsatz der Zweckbindung .....	39
2.2.3	Grundsatz der Datenminimierung .....	39
2.2.4	Grundsatz der Datenrichtigkeit .....	40
2.2.5	Grundsatz der Speicherbegrenzung .....	40

2.2.6	Grundsatz der Integrität und Vertraulichkeit .....	41
2.2.7	Rechenschaftspflicht .....	41
<b>2.3</b>	<b>Grundsätze der Verarbeitung personenbezogener Daten .....</b>	<b>42</b>
2.3.1	Was sind personenbezogene Daten? .....	42
2.3.2	Wann erfolgt die Datenverarbeitung auf Grundlage gesetzlicher Erlaubnisnormen? .....	43
2.3.3	Wie erfolgt die Datenverarbeitung auf Grundlage einer Einwilligung des Betroffenen? .....	47
<b>2.4</b>	<b>Technischer und organisatorischer Datenschutz: Privacy by Design und Privacy by Default .....</b>	<b>53</b>
<b>2.5</b>	<b>Datenschutz-Folgenabschätzung .....</b>	<b>56</b>
2.5.1	In welchen Fällen ist eine Datenschutz-Folgenabschätzung durchzuführen? .....	56
2.5.2	Wie ist das Verfahren durchzuführen und was beinhaltet es? .....	60
<b>2.6</b>	<b>Auftragsverarbeitung .....</b>	<b>61</b>
2.6.1	Was ist Auftragsverarbeitung? .....	61
2.6.2	Wo spielt Auftragsverarbeitung eine Rolle? .....	62
2.6.3	Worin besteht die rechtliche Problematik? .....	62
2.6.4	Welche Regelungen gelten bei der Auftragsverarbeitung? .....	63
2.6.5	Welche Konsequenzen hat ein Verstoß des Auftragsverarbeiters? .....	64
<b>2.7</b>	<b>Datentransfer in Drittstaaten .....</b>	<b>64</b>
2.7.1	Unter welchen Bedingungen ist ein Datentransfer in Drittstaaten zulässig? .....	66
2.7.2	In welche Drittstaaten ist ein Datentransfer zulässig? .....	66
2.7.3	Ist ein Datentransfer in unsichere Drittstaaten auch ohne Kommissionsbeschluss zulässig? .....	68
2.7.4	Kann ein Datentransfer in Drittstaaten auch ohne Angemessenheitsbeschluss und ohne Garantien erfolgen? .....	69
<b>2.8</b>	<b>Erstellung eines Verarbeitungsverzeichnisses .....</b>	<b>69</b>
2.8.1	Wer muss ein Verarbeitungsverzeichnis erstellen? .....	70
2.8.2	Was muss das Verarbeitungsverzeichnis beinhalten? .....	71
2.8.3	Wie ist ein Verarbeitungsverzeichnis zu erstellen? .....	73
<b>2.9</b>	<b>Melde- und Informationspflichten bei Datenpannen .....</b>	<b>76</b>
2.9.1	Was müssen Sie im Falle einer Datenpanne veranlassen? .....	76
2.9.2	Welchen Inhalt muss die Meldung haben? .....	77

<b>2.10</b>	<b>Rechte der Betroffenen</b> .....	78
2.10.1	Recht auf Auskunft .....	79
2.10.2	Recht auf Datenübertragbarkeit .....	79
2.10.3	Recht auf Vergessenwerden und Recht auf Berichtigung .....	79
2.10.4	Recht auf Widerspruch gegen die Datenverarbeitung .....	80
2.10.5	Recht auf Widerspruch bei automatisierten Einzelfall- entscheidungen .....	81
<b>2.11</b>	<b>Arbeitnehmerdatenschutz</b> .....	83
2.11.1	Was genau ist Arbeitnehmerdatenschutz? .....	83
2.11.2	Wo ist der Arbeitnehmerdatenschutz geregelt? .....	83
2.11.3	Was sagt die Datenschutz-Grundverordnung zum Arbeitneh- merdatenschutz? .....	84
2.11.4	Wann dürfen Daten nach dem neuen Bundesdatenschutzgesetz verarbeitet werden? .....	84
2.11.5	Was ist bei der Einholung einer Einwilligung zu beachten? .....	86
2.11.6	Welche Rolle spielt der Betriebsrat im Arbeitnehmerdatenschutz? .....	86
2.11.7	Welche Rolle spielen die Aufsichtsbehörden und welche Rechte haben sie? .....	87
<b>2.12</b>	<b>Datenschutzbeauftragter</b> .....	87
2.12.1	Welche Bedeutung hat der Datenschutzbeauftragte? .....	87
2.12.2	Welche gesetzlichen Normierungen regeln die Modalitäten rund um die Bestellung des Datenschutzbeauftragten? .....	88
2.12.3	Wer muss einen Datenschutzbeauftragten bestellen? .....	88
2.12.4	Wie wird der Datenschutzbeauftragte bestellt? .....	90
2.12.5	Welche Aufgaben hat der Datenschutzbeauftragte? .....	90
2.12.6	Welche Anforderungen werden an den Datenschutzbeauftragten gestellt? .....	91
2.12.7	Welche Person kommt als Datenschutzbeauftragter in Betracht? .....	92
2.12.8	Welche rechtlichen Besonderheiten bestehen bei der Bestellung eines externen Datenschutzbeauftragten? .....	92
<b>2.13</b>	<b>Datenschutzerklärung</b> .....	94
2.13.1	Wann ist eine Datenschutzerklärung erforderlich? .....	95
2.13.2	Wie ist eine Datenschutzerklärung aufzubauen? .....	96
2.13.3	Welchen Inhalt muss eine Datenschutzerklärung haben? .....	97
2.13.4	Wie muss die Datenschutzerklärung übermittelt werden? .....	105
2.13.5	Wo muss die Datenschutzerklärung platziert werden? .....	107

<b>2.14</b>	<b>Datenschutzaudit</b> .....	108
2.14.1	Was ist ein Datenschutzaudit? .....	109
2.14.2	Warum ist ein Datenschutzaudit sinnvoll? .....	110
2.14.3	Wann sollten Sie ein Datenschutzaudit in die Wege leiten? .....	111
2.14.4	Wer kann ein Datenschutzaudit durchführen? .....	111
2.14.5	Wie wird ein Zertifizierungsverfahren ablaufen? .....	112
2.14.6	Was passiert nach dem Datenschutzaudit? .....	113

### **3 Praxischeck I: Website und Online-Shop DSGVO-konform gestalten** 115

---

<b>3.1</b>	<b>Webanalyse: IP-Adressen, Verträge und Widerspruch</b> .....	116
3.1.1	Wann ist der Einsatz von Webanalyse-Tools zulässig? .....	117
3.1.2	Wie erfolgt der rechtskonforme Umgang mit IP-Adressen? .....	119
3.1.3	Wie muss der Vertrag mit Google Analytics und Co. genau abgeschlossen werden? .....	122
3.1.4	Was ist bezüglich des Widerspruchs gegen die Webanalyse zu beachten? .....	126
<b>3.2</b>	<b>Newsletter-Versand: Double Opt-In und Abbestell-Link</b> .....	129
3.2.1	Wie holt man eine rechtskonforme Einwilligung ein? .....	129
3.2.2	Wie muss die Abbestellmöglichkeit ausgestaltet sein? .....	133
3.2.3	Was ist beim Einsatz von Newsletter-Dienstleistern aus Drittstaaten zu beachten? .....	138
<b>3.3</b>	<b>Online-Targeting, Retargeting und Remarketing: Der Einsatz von Cookies</b> .....	143
3.3.1	Was sind Cookies? .....	144
3.3.2	Wie können Cookies nach der Datenschutz-Grundverordnung eingesetzt werden? .....	145
3.3.3	Welchen Einfluss wird die e-Privacy-Verordnung auf das Setzen von Cookies haben? .....	151
<b>3.4</b>	<b>Social Media: Fanpages, Plug-ins und Custom Audiences</b> .....	154
3.4.1	Wer haftet für Datenschutzverstöße auf Fanpages in sozialen Netzwerken? .....	154
3.4.2	Was ist beim Einsatz von Social Plug-ins zu beachten? .....	157

3.4.3	Wie sieht es mit »Facebook Custom Audiences« über die Website aus? .....	163
3.4.4	Ist der Einsatz von »Facebook Custom Audiences« im Listenverfahren zulässig? .....	170

## **4 Praxischeck II: Die 30 am häufigsten gestellten Fragen (FAQ)** 175

---

4.1	Für wen gilt die Datenschutz-Grundverordnung? .....	175
4.2	Welche Daten dürfen nicht erfasst werden? .....	176
4.3	Gilt die Datenschutz-Grundverordnung auch für Alt-Daten? .....	177
4.4	Was passiert bei Verstößen gegen die Datenschutz-Grundverordnung? .....	177
4.5	Was ist die e-Privacy-Verordnung? .....	177
4.6	In welchem Verhältnis steht die Datenschutz-Grundverordnung zur e-Privacy-Verordnung? .....	178
4.7	Wie können Daten im Unternehmen geschützt werden? .....	178
4.8	Benötigen Unternehmen immer ein Sicherheitskonzept? .....	179
4.9	Was wird aus den bisherigen Datenschutzzertifikaten? .....	179
4.10	Muss jede Datenschutzerklärung angepasst werden? .....	179
4.11	Ist der Einsatz eines Datenschutz-Generators sinnvoll? .....	180
4.12	Woher weiß ich, welche Plug-ins ich in meine Datenschutzerklärung aufnehmen muss? .....	180
4.13	Wer benötigt einen Datenschutzbeauftragten? .....	180
4.14	Welche Mitarbeiter sind bei der Berechnung der Zehn-Personen-Grenze für einen Datenschutzbeauftragten einzubeziehen? .....	181
4.15	Wer kann Datenschutzbeauftragter werden? .....	181
4.16	Muss der Datenschutzbeauftragte schriftlich bestellt werden? .....	181
4.17	Was passiert mit vor der Datenschutzreform bestellten Datenschutzbeauftragten? .....	182
4.18	Was ist bei der Einholung einer Einwilligung nach neuem Recht zu beachten? .....	182

<b>4.19</b>	<b>Was ist mit Einwilligungen, die vor Inkrafttreten der Datenschutz-Grundverordnung erteilt wurden?</b> .....	182
<b>4.20</b>	<b>Müssen Einwilligungen protokolliert werden und wie kann dies elektronisch erfolgen?</b> .....	183
<b>4.21</b>	<b>Können alte Kontaktformulare weiter genutzt werden?</b> .....	183
<b>4.22</b>	<b>Was ist beim Einsatz einer ausländischen Cloud zu beachten?</b> .....	183
<b>4.23</b>	<b>Was ist das Privacy-Shield-Abkommen?</b> .....	184
<b>4.24</b>	<b>Was ist Big Data?</b> .....	184
<b>4.25</b>	<b>Muss man Abmahnungen fürchten?</b> .....	185
<b>4.26</b>	<b>Sollte man überhaupt auf eine Abmahnung reagieren?</b> .....	186
<b>4.27</b>	<b>Was passiert, wenn man keine Unterlassungserklärung abgibt?</b> .....	186
<b>4.28</b>	<b>Sollte man die Unterlassungserklärung der Gegenseite unterschreiben?</b> ....	186
<b>4.29</b>	<b>Wie kann man auf eine einstweilige Verfügung reagieren?</b> .....	187
<b>4.30</b>	<b>Was ist zu tun, wenn man eine Klageschrift erhält?</b> .....	187

## **5 Mustertexte** 189

---

<b>5.1</b>	<b>Muster für Datenschutzerklärungen</b> .....	189
5.1.1	Checkliste zur Datenschutzerklärung für Website und Online-Shop .....	191
5.1.2	Datenschutzerklärung für die Website .....	194
5.1.3	Erweiterte Datenschutzerklärung für den Einsatz von »Google Web Fonts« .....	210
5.1.4	Erweiterte Datenschutzerklärung für den Einsatz von »Google Tag Manager« .....	211
5.1.5	Erweiterte Datenschutzerklärung für den Einsatz des Newsletter-Dienstleiters »MailChimp« .....	215
5.1.6	Erweiterte Datenschutzerklärung für den Online-Shop .....	219
5.1.7	Datenschutzerklärung für Beschäftigte .....	224
<b>5.2</b>	<b>Muster für Einwilligungserklärungen</b> .....	237
5.2.1	Einwilligung in den Erhalt eines Newsletters .....	237
5.2.2	Einwilligung in den Erhalt des Newsletters über einen Newsletter-Dienstleister .....	238
5.2.3	Einwilligung in Bonitätsprüfungen .....	239

<b>5.3</b>	<b>Muster eines Verarbeitungsverzeichnisses für Verantwortliche .....</b>	<b>240</b>
<b>5.4</b>	<b>Muster eines Vertrags zur Auftragsverarbeitung .....</b>	<b>250</b>
<b>5.5</b>	<b>Aufbau eines Datenschutzkonzepts .....</b>	<b>256</b>
<b>5.6</b>	<b>Leitfaden zur Erstellung eines Datensicherheitskonzepts .....</b>	<b>262</b>

## **6      Fazit und Ausblick** **267**

---

Index .....	271
-------------	-----