

Inhaltsverzeichnis

Vorwort zur 2. Auflage	V
Abkürzungsverzeichnis	XVII
Literatur und Muster	XIX
I. Grundlagen des Datenschutzrechts	1
1. Was ist die Datenschutzgrundverordnung?	1
2. Wieso ist die DSGVO für das Marketing relevant?	1
3. Für wen gilt die DSGVO?	2
4. Für wen gilt die DSGVO nicht?	3
5. Welche Daten werden geschützt?	5
6. Gilt das Datenschutzrecht auch, wenn ich Daten von juristischen Personen verarbeite?	5
7. Wann werden Daten „verarbeitet“?	6
8. Sind nur automatisierte Datenverarbeitungen geschützt?	7
9. Was sind besondere Kategorien personenbezogener Daten?	7
10. Ist die DSGVO nur in Europa beachtlich?	8
11. Wieso gibt es zurzeit so viele Unklarheiten und unterschiedliche Meinungen zur DSGVO?	8
II. Rechtmäßigkeit von Datenverarbeitungen	10
12. Was muss ich beachten, wenn ich Daten verarbeite?	10
13. Darf ich personenbezogene Daten „auf Vorrat“ speichern?	11
14. Darf ich Kundendaten, die ich in den letzten Jahren gesammelt habe, weiterhin verarbeiten?	12
15. Darf ich den Verarbeitungszweck, für den Kundendaten erhoben wurden, ohne Weiteres ändern?	12
16. Rechtsgrundlagen für Datenverarbeitungen, oder: Muss ich immer Einwilligungen einholen, wenn ich Daten verarbeiten will?	13
17. Wie muss ich mit Daten umgehen, die ich für die Erfüllung von Verträgen mit meinen Kunden benötige?	13
18. Was ist zu tun, wenn ich gesetzliche Pflichten wie die steuer- rechtlichen Aufbewahrungspflichten habe?	14
19. Wann habe ich ein „berechtigtes Interesse“ daran, Daten ohne Einwilligung zu verarbeiten?	14
20. Auf welche anderen Rechtsgrundlagen kann ich Datenverarbeitungen stützen?	15
21. Soll ich vorsichtshalber immer Einwilligungen einholen?	16
22. Wie muss eine Einwilligung aussehen?	17
23. Wie konkret müssen die einzelnen Bestandteile der Einwilligungserklärung genannt werden?	17
24. Wie kann eine Einwilligung widerrufen werden?	19

25.	Was muss ich beachten, wenn eine Einwilligung mehrere Datenverarbeitungen umfassen soll?	19
26.	Wann gilt eine Einwilligung als rechtswirksam abgegeben?	21
27.	Kann eine Einwilligung auch mündlich eingeholt werden?	21
28.	Dürfen Kunden, die eine Einwilligung nicht erteilen, Nachteile haben?	22
29.	Darf ich Kunden dazu zwingen, in Datenverarbeitungen einzuwilligen, die mit der Erfüllung eines mit mir abgeschlossenen Vertrags oder der Erbringung einer von mir angebotenen Dienstleistung nichts zu tun haben?	22
30.	Darf ich alte Einwilligungserklärungen weiterverwenden?	23
31.	Was mache ich, wenn ich zwar alte Einwilligungs-erklärungen habe, diese jedoch nicht rechtsgültig sind?	23
32.	Wie darf ich meine Kunden zum Zweck der Einholung der Einwilligung kontaktieren?	24
33.	Unter welchen Voraussetzungen darf ich sensible Daten verarbeiten?	25
34.	Darf ich Daten von Kindern verarbeiten?	26
35.	Welche Anstrengungen muss ich beim Angebot von Online-Services, die sich direkt an Kinder richten, zur Überprüfung der Einwilligung unternehmen?	27
36.	Was muss ich beachten, wenn ich Online-Services für Kinder in mehreren Ländern anbiete?	28
37.	Welche Regeln gelten für Direktmarketing?	28
38.	Was versteht man unter Direktmarketing?	28
39.	Darf ich ohne Einwilligung Direktwerbung versenden?	29
40.	Können mir einzelne meiner Kunden mitteilen, dass sie keine Direktwerbung mehr von mir erhalten wollen?	29
41.	Unter welchen Voraussetzungen darf ich Werbeanrufe tätigen?	30
42.	Was muss ich beachten, wenn ich Direktwerbung per E-Mail versende?	30
43.	Welche Sonderregeln gelten für Adressverlage und Direktmarketingunternehmen?	31
44.	Darf ich Kundendaten an Direktmarketingunternehmen verkaufen?	35
III.	Datenschutz im Internet: Cookies, Social Media, ChatGPT etc	36
45.	Gilt das Datenschutzrecht auch im Internet?	36
46.	Sind IP-Adressen und sonstige Online-Kennungen personenbezogene Daten?	36
47.	Ist die Protokollierung von Daten am Webserver zulässig?	36
48.	Was ist zu beachten, wenn ich auf meiner Website Cookies setze?	37
49.	Wie muss der Nutzer über die Setzung von Cookies informiert werden?	38

50.	Wie wird eine Einwilligung zur Setzung von Cookies wirksam eingeholt?	39
51.	Was ist bei der Ausgestaltung von Cookie-Bannern zu beachten?	39
52.	Was ist zu beachten, wenn ich Google Analytics verwende?	40
53.	Was ist bei der Verwendung von Social-Media-Plugins und Pixels zu bedenken?	42
54.	Was ist bei der Verwendung von Social-Media-Plattformen zu beachten?	44
55.	Welche Vorkehrungen muss ich treffen, wenn ich eine Facebook-Fanpage oder vergleichbare Online-Auftritte anderer Social-Media-Dienstanbieter betreibe?	
56.	Was muss ich beachten, wenn ich auf meiner Website Platz für „Online Behavioral Advertising“ zur Verfügung stelle?	46
57.	Wie kann ich künstliche Intelligenz (zB ChatGPT) datenschutzrechtskonform einsetzen?	47
IV.	Datenschutzrechtliche Aspekte der Aufnahme von	
	Fotos und Videos	49
58.	Sind Fotos und Videos personenbezogene Daten?	49
59.	Unter welchen Voraussetzungen dürfen Fotos und Videos aufgenommen werden?	49
60.	Wann liegen überwiegende berechtigte Interessen an einer Bildaufnahme vor?	50
61.	Wann ist eine Bildaufnahme verboten?	52
62.	Wie kann eine Einwilligung für die Aufnahme eingeholt werden?	53
63.	Was ist bei der Veröffentlichung von Fotos und Videos zu beachten?	53
64.	Ist die Verwendung von GIFs und Memes zulässig?	55
65.	Wie lange dürfen Aufnahmen gespeichert werden?	55
66.	Was gilt für Verarbeitungen von Lichtbildern im Rahmen journalistischer Tätigkeit?	56
V.	Betroffenenrechte	57
67.	Welche Rechte stehen dem Betroffenen zu und wie reagiert man auf Anfragen?	57
68.	Wie muss ich mit Anfragen Dritter, die für eine betroffene Person gestellt werden, umgehen?	58
69.	In welcher Form kann mich der Betroffene kontaktieren und wie muss ich antworten?	59
70.	Binnen welcher Frist muss ich auf die Ausübung eines Betroffenenrechts reagieren?	60
71.	Darf ich Entgelt dafür verlangen, dass ich auf die Ausübung von Betroffenenrechten reagiere?	60

72.	Was ist von meiner Informationspflicht gegenüber Betroffenen umfasst?	61
73.	Welchen Unterschied macht es, ob ich die Daten unmittelbar beim Betroffenen erhebe oder von dritter Seite erhalte?	62
74.	Wann genau muss ich meine Informationspflicht erfüllen und reicht es, wenn Informationen lediglich auf Anfrage des Betroffenen erteilt werden?	62
75.	Welche Möglichkeiten der Ausgestaltung für einen Mehrebenenansatz bei der Erfüllung der Informationspflichten gibt es?	64
76.	Muss ich etwas unternehmen, wenn sich die von mir erteilten Informationen nach Art 13 und 14 DSGVO ändern?	64
77.	Was muss ich tun, wenn ich personenbezogene Daten zu anderen Zwecken als ihren ursprünglichen Erhebungszwecken verarbeiten will?	65
78.	Wann trifft mich gegenüber Betroffenen keine Informationspflicht?	65
79.	Was ist vom Recht des Betroffenen auf Auskunft umfasst?	66
80.	Gilt die Auskunftspflicht ohne Einschränkung?	67
81.	Müssen personenbezogene Daten gespeichert werden, um Anfragen von Betroffenen beantworten zu können?	67
82.	Was ist vom Recht auf Berichtigung umfasst?	68
83.	Muss ich Empfänger, denen ich personenbezogene Daten übermittelt habe, über durchgeführte Berichtigungen verständigen?	69
84.	Wann muss ich personenbezogene Daten löschen?	69
85.	Was bedeutet „löschen“ überhaupt?	70
86.	Muss ich ein Löschkonzept erstellen?	70
87.	Muss ich personenbezogene Daten aus Back-ups löschen?	71
88.	Was bedeutet das Recht auf Vergessenwerden?	71
89.	Gibt es Ausnahmen von der Löschungsverpflichtung?	72
90.	Wann steht dem Betroffenen ein Recht auf Einschränkung der Verarbeitung seiner personenbezogenen Daten zu?	72
91.	Wann steht dem Verantwortlichen ein Recht auf Einschränkung der Verarbeitung zu?	73
92.	Was ist unter dem Recht auf Einschränkung der Verarbeitung zu verstehen und wie wird diesem Recht entsprochen?	73
93.	Was darf ich noch mit den eingeschränkt verarbeiteten personenbezogenen Daten tun?	74
94.	Was muss ich tun, wenn doch kein Recht auf Einschränkung mehr besteht?	74
95.	Wann muss der Verantwortliche seiner Mitteilungspflicht nach Art 19 DSGVO in Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten bzw der Einschränkung einer Verarbeitung nachkommen?	75

96.	Was bedeutet das Recht auf Datenübertragbarkeit („Datenportabilität“)?	75
97.	Was bedeutet das Widerspruchsrecht nach Art 21 DSGVO?	76
98.	Wann kommt dem Betroffenen ein Widerspruchsrecht zu?	77
99.	Besteht beim Widerspruchsrecht eine besondere Hinweispflicht?	78
100.	Was muss geschehen, wenn der Betroffene berechtigterweise Widerspruch erhebt?	78
101.	Was muss ich bei automationsunterstützter Entscheidungsfindung im Einzelfall und Profiling beachten?	79
102.	Was ist unter „Profiling“ zu verstehen und wie verhält es sich zu automatisierten Entscheidungen?	80
103.	Wann sind automatisierte Entscheidungen und Profiling zulässig?	82
104.	Welche Anforderungen sind an eine Einwilligung zum Profiling zu stellen?	84
105.	Sind automatisierte Entscheidungen und Profiling auch auf Grundlage sensibler Daten zulässig?	85
106.	Was ist bei automatisierten Entscheidungen und Profiling im Zusammenhang mit Minderjährigen zu beachten?	85
107.	Bestehen besondere Informationspflichten hinsichtlich automatisierter Entscheidungen und Profiling?	86
108.	Welche angemessenen Maßnahmen sind zu empfehlen, wenn automatisierte Entscheidungen und Profiling zu meinen Verarbeitungsvorgängen zählen?	87
109.	Welche Rechte stehen dem Betroffenen zu?	88
VI.	Technische und organisatorische Maßnahmen (TOMs)	89
110.	Welchen Stellenwert haben „technische und organisatorische Maßnahmen“ (kurz: TOMs) nach der DSGVO?	89
111.	Muss nur der Verantwortliche TOMs treffen?	89
112.	Gibt es unterschiedliche Arten von technischen und organisatorischen Maßnahmen?	89
113.	Nach welchen Kriterien müssen TOMs getroffen werden?	90
114.	Wie wird Datenschutz durch Technikgestaltung („Privacy by Design“) umgesetzt?	92
115.	Wie wird Datenschutz durch datenschutzfreundliche Voreinstellungen („Privacy by Default“) umgesetzt?	94
116.	Welche Maßnahmen muss ich treffen, um die von der DSGVO geforderte Datensicherheit am besten einzuhalten?	94
VII.	Outsourcing – Der Auftragsverarbeiter	97
117.	Was ist ein Auftragsverarbeiter?	97
118.	Brauche ich eine Rechtsgrundlage, um einen Auftragsverarbeiter heranzuziehen?	99
119.	Welche Auftragsverarbeiter darf ich auswählen?	100

Inhaltsverzeichnis

120. Muss ich mit einem Auftragsverarbeiter einen Vertrag abschließen?	100
121. Wie muss ein Auftragsverarbeitervertrag aussehen?	101
122. Darf ein Auftragsverarbeiter Sub-Auftragsverarbeiter einsetzen?	102
123. Was ist zu beachten, wenn ich Auftragsverarbeiter außerhalb der EU einsetze?	104
124. Was passiert, wenn ein Auftragsverarbeiter meine Weisungen missachtet?	104
125. Haftet der Auftragsverarbeiter für Datenschutzverstöße?	105
VIII. Das Verarbeitungsverzeichnis	106
126. Was ist ein Verarbeitungsverzeichnis und wozu dient es?	106
127. Muss ich in jedem Fall ein Verarbeitungsverzeichnis führen?	106
128. Was kann mir passieren, wenn ich kein Verarbeitungsverzeichnis führe?	107
129. Welche Inhaltserfordernisse muss mein Verarbeitungsverzeichnis erfüllen?	108
130. Wie detailliert sind die einzelnen Verarbeitungen anzuführen?	110
131. Muss ich ein zusätzliches Verarbeitungsverzeichnis führen, wenn ich im Auftrag eines Dritten Daten verarbeite?	110
IX. Richtiger Umgang mit „Data Breaches“	112
132. Was ist unter „Data Breach“ zu verstehen?	112
133. Wann liegt ein Data Breach vor?	112
134. Welche Verpflichtungen treffen mich, wenn ein Data Breach auftritt?	113
135. Wonach wird beurteilt, ob voraussichtlich kein Risiko für die Rechte und Freiheiten natürlicher Personen vorliegt?	114
136. Wonach wird beurteilt, ob voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen vorliegt? ...	114
137. Muss einem Betroffenen bei voraussichtlich hohem Risiko in jedem Fall Meldung erstattet werden?	116
138. Kann die Aufsichtsbehörde die Meldung an Betroffene erzwingen?	117
139. Muss ich bei der Meldung Fristen einhalten?	117
140. Welche Form- und Inhaltserfordernisse sind bei einer Meldung zu beachten?	118
141. Was ist bei grenzüberschreitenden Datenverarbeitungen zu beachten?	120
142. Was kann mir passieren, wenn ich der Meldeverpflichtung nicht oder nicht rechtzeitig entspreche?	121
143. Welche Aufzeichnungen müssen aufgrund eines Data Breach geführt werden und wie lange müssen diese aufbewahrt werden?	121
X. Datenschutz-Folgenabschätzung	122
144. Was ist eine Datenschutz-Folgenabschätzung (DSFA) und wozu dient sie?	122

145. Nach welchen Kriterien entscheidet sich, ob eine Datenschutz-Folgenabschätzung durchgeführt werden muss?	122
146. Woher weiß ich, wann „wahrscheinlich ein hohes Risiko“ besteht?	124
147. Muss eine Datenschutz-Folgenabschätzung auch für bestehende Datenverarbeitungen durchgeführt werden?	127
148. Muss immer für jede Verarbeitung separat eine Datenschutz-Folgenabschätzung durchgeführt werden?	128
149. Muss ich eine Datenschutz-Folgenabschätzung durchführen, wenn ich die konkrete Verarbeitung (an einen Auftragsverarbeiter) outgesourct habe?	128
150. Zu welchem Zeitpunkt muss eine Datenschutz-Folgenabschätzung durchgeführt werden?	128
151. Wer sollte an der Durchführung einer Datenschutz-Folgenabschätzung mitwirken?	129
152. Wie muss eine Datenschutz-Folgenabschätzung durchgeführt werden?	129
153. Darf ich mich damit begnügen, einmal eine Datenschutz-Folgenabschätzung durchgeführt zu haben?	132
154. Muss man das Ergebnis einer Datenschutz-Folgenabschätzung veröffentlichen?	132
155. Wann muss ein Konsultationsverfahren vor der Aufsichtsbehörde eingeleitet werden?	133
156. Droht eine Strafe, wenn die Bestimmungen über die DSFA nicht eingehalten werden?	133
XI. Der Datenschutzbeauftragte	134
157. Was ist ein Datenschutzbeauftragter?	134
158. Wann muss ein Datenschutzbeauftragter benannt werden?	134
159. Wer kommt als Datenschutzbeauftragter infrage?	136
160. Muss der Datenschutzbeauftragte ein Mitarbeiter des Unternehmens des Verantwortlichen/Auftragsverarbeiters sein?	137
161. Darf der Geschäftsführer eines Unternehmens sich selbst zum Datenschutzbeauftragten benennen?	137
162. Wie wird ein Datenschutzbeauftragter benannt?	138
163. Welche Stellung hat der Datenschutzbeauftragte im Unternehmen?	138
164. Welche Aufgaben hat der Datenschutzbeauftragte?	141
165. Haftet der Datenschutzbeauftragte für Rechtsverstöße?	142
XII. Datenübermittlung an Länder außerhalb der EU	143
166. Was muss ich beachten, wenn ich Daten in andere EU-Länder übermittle?	143
167. Was muss ich beachten, wenn ich Daten an Länder außerhalb der EU übermittle?	143
168. Was gilt als „Übermittlung“?	147

Inhaltsverzeichnis

169. Was gilt als Datenübermittlung „in ein Drittland“?	148
170. Inwiefern gilt die DSGVO für Weiterübermittlungen von Daten?	148
171. Unter welchen Voraussetzungen ist eine Datenübermittlung in Drittländer zulässig?	148
172. Was ist ein „Angemessenheitsbeschluss“ der EU-Kommission und für welche Länder gibt es einen solchen?	149
173. Gibt es einen Angemessenheitsbeschluss für die USA?	149
174. Was sind „geeignete Garantien“?	150
175. Was sind „Binding Corporate Rules“ und wie werden diese erzeugt?	151
176. Wann ist eine Datenübermittlung zulässig, obwohl weder ein Angemessenheitsbeschluss noch geeignete Garantien vorliegen?	152
XIII. Haftung, Sanktionen, Rechtsschutz	154
177. Welche Folgen kann ein Verstoß gegen geltendes Datenschutzrecht nach sich ziehen?	154
178. Welche Behörde ist für die Verhängung von Geldbußen und Geldstrafen zuständig?	155
179. Wie hoch können Geldbußen nach der DSGVO und sonstige Verwaltungsstrafen ausfallen?	155
180. Nach welchen Kriterien bestimmt sich die Höhe der verhängten Geldbuße?	157
181. Welche sonstigen Sanktionen können über mich verhängt werden?	159
182. Wer haftet für Geldbußen und Geldstrafen für datenschutz- rechtliche Verstöße?	160
183. Wie läuft das Verfahren vor der Datenschutzbehörde bei der Verhängung von Sanktionen ab?	161
184. Wie kann ich eine über mich verhängte Geldbuße oder sonstige Sanktion bekämpfen?	162
185. Welche zivilrechtlichen Ansprüche können gegen mich geltend gemacht werden?	162
186. Kann ich für Fehler meines Auftragsverarbeiters in Anspruch genommen werden?	165
Stichwortverzeichnis	167