

Inhaltsverzeichnis

Vorwort	V
1. Einleitung – Warum ist dieses Buch so, wie es ist	1
2. Drei Buchstaben: DSB	4
Was muss ich als DSB wissen?	5
3. Begriffsklärungen	10
3.1 Verantwortlicher	10
3.2 Gemeinsam Verantwortliche	12
3.3 Auftragsverarbeiter	13
3.4 Personenbezogene Daten	14
3.5 Besondere Kategorien personenbezogener Daten („Magendaten“)	16
3.6 Gebräuchliche Abkürzungen	17
4. Wer bin ich als DSB?	18
4.1 Stellung des DSB	19
4.2 Aufgaben des DSB	23
4.3 Was ist nicht Aufgabe des DSB?	25
4.4 Haftung des DSB	26
4.5 Wann muss ein DSB benannt werden?	28
4.6 Muster einer Benennung	29
5. Rechtliche Grundlagen	32
5.1 Rechtsquellen	32
5.2 Sachlicher und räumlicher Anwendungsbereich	34
5.3 Struktur der DSGVO	37
6. Grundsätze für die Verarbeitung personenbezogener Daten	43
6.1 Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	43
6.2 Zweckbindung	44
6.3 Datenminimierung	45
6.4 Richtigkeit	46
6.5 Speicherbegrenzung	46
6.6 Integrität und Vertraulichkeit	47
6.7 Rechenschaftspflicht	47
7. Grundüberlegungen zur „Gemüsenorm“	48
7.1 Art. 6 Abs. 1 lit. a) DSGVO – Einwilligung → „ALTer- native“	50
7.2 Art. 6 Abs. 1 lit. b) DSGVO – Datenverarbeitung zur Vertragserfüllung → „Dickes B“	50

7.3	Art. 6 Abs. 1 lit. c) DSGVO – Datenverarbeitung zur Erfüllung rechtlicher Pflichten → „Caesar“	51
7.4	Art. 6 Abs. 1 lit. d) DSGVO – Datenverarbeitung für lebenswichtige Interessen → „Dead“	51
7.5	Art. 6 Abs. 1 lit. e) DSGVO – Datenverarbeitung für öffentliche Aufgaben → „Echt jetzt“	52
7.6	Art. 6 Abs. 1 lit. f) DSGVO – Datenverarbeitung auf Basis einer Interessenabwägung → „FETT“	53
8.	Die Einwilligung – „ALternative“	54
9.	Datenverarbeitung für Vertragszwecke – „Dickes B“	57
10.	Datenverarbeitung zur Erfüllung rechtlicher Pflichten – „Caesar“	60
11.	Datenverarbeitung für lebenswichtige Interessen – „Dead“	61
12.	Datenverarbeitung für öffentliche Aufgaben – „Echt jetzt“	62
13.	Datenverarbeitung auf Basis einer Interessenabwägung – „FETT“	63
13.1	Erste Stufe – Berechtigtes Interesse des Verantwortlichen oder Dritten	63
13.2	Zweite Stufe – Zur Wahrung des berechtigten Interesses erforderlich.	64
13.3	Dritte Stufe – Abwägung mit entgegenstehenden Interessen der betroffenen Personen	64
13.4	Widerspruchsrecht	65
13.5	Kein „FETT“ für öffentliche Stellen	65
14.	Verarbeitung von „Magendaten“	67
15.	Standard-Datenschutzmodell (SDM) – auf ein Wort	68
16.	Die Informationspflichten der DSGVO	70
16.1	Gut gedacht – schlecht gemacht.	70
16.2	Grundsatz der Transparenz.	70
16.3	Zeitvorgaben für die Beantwortung von Anfragen Betroffener.	71
16.4	Daten zum Betroffenen nicht verfügbar.	72
16.5	Zweifel an der Identität des Betroffenen	72
16.6	Bildsymbole	72
17.	Informationspflichten bei der Erhebung beim Betroffenen	73
17.1	Praktische Begrenzung der Informationsfülle	75
17.2	Die „Link-Lösung“	75
17.3	Ausnahmen von der Informationspflicht	75

17.4	Weiterverarbeitung.....	76
18.	Informationspflichten bei Daten, die nicht beim Betroffenen erhoben wurden.....	77
18.1	Weiterverarbeitung.....	78
18.2	Ausnahmen.....	78
19.	Beispiel einer Information – Datenschutzhinweise für Beschäftigte.....	82
20.	Auskunftsrecht und Recht auf Kopie.....	86
20.1	Erste Stufe – „Ob“ einer Verarbeitung.....	86
20.2	Zweite Stufe – Auskunft zu gespeicherten Daten.....	86
20.3	Dritte Stufe – Weitere Informationen.....	87
20.4	Vierte Stufe – Recht auf Kopie.....	87
21.	Löschansprüche von Betroffenen.....	89
21.1	Recht auf Vergessenwerden.....	89
21.2	Ausnahmen von Löschpflichten.....	90
22.	Weitere Betroffenenrechte.....	91
23.	Datenschutz-Compliance und risikobasierter Ansatz.....	94
24.	Privacy by Design & by Default.....	95
25.	Auftragsverarbeitung.....	98
25.1	Was ist Auftragsverarbeitung?.....	98
25.2	Wann liegt eine Auftragsverarbeitung vor?.....	100
25.3	Wann liegt keine Auftragsverarbeitung vor?.....	101
25.4	Der Auftragsverarbeitungsvertrag.....	102
25.5	Unterauftragnehmer.....	103
25.6	Technische und organisatorische Maßnahmen.....	104
25.7	Mustervertrag.....	105
26.	Gemeinsame Verantwortlichkeit.....	123
26.1	Wann liegt eine gemeinsame Verantwortlichkeit vor?.....	123
26.2	Wie muss ich die gemeinsame Verantwortlichkeit „regeln“?.....	124
26.3	Muster einer Vereinbarung zur gemeinsamen Verantwortlichkeit.....	125
27.	Meldepflichten bei „Datenpannen“.....	131
27.1	Was ist eine Datenschutzverletzung („Datenpanne“)?.....	131
27.2	Wann ist diese bei der Aufsichtsbehörde zu melden?.....	132
27.3	Wie schnell muss die Meldung erfolgen?.....	134
27.4	Wie muss die Meldung erfolgen?.....	134

27.5	Dokumentation der Datenpanne.	135
27.6	Meldepflicht gegenüber Betroffenen.	136
28.	Verzeichnis von Verarbeitungstätigkeiten	138
28.1	Gibt es Ausnahmen?.	138
28.2	Was ist das Verarbeitungsverzeichnis?.	139
28.3	Wie erstelle ich das Verarbeitungsverzeichnis praktisch? . .	140
28.4	Wie pflege ich das Verarbeitungsverzeichnis?.	141
28.5	Muster für ein Verarbeitungsverzeichnis	141
29.	Datenschutz-Folgenabschätzung (DSFA)	172
29.1	„In dubio pro DSFA“	172
29.2	Wann ist eine DSFA durchzuführen?.	173
29.3	Was muss eine DSFA beinhalten?	173
29.4	Empfehlung für die Praxis als DSB	175
29.5	Besonderheiten für „Caesar“ und „Echt jetzt“.	176
30.	Haftung für Datenschutzverletzungen?	177
	Was muss ein DSB zu Schadensersatzansprüchen der DSGVO wissen?	177
31.	Aufsichtsbehörde.	178
32.	Beschäftigtendatenschutz	179
33.	Datenverarbeitung in Drittländern	181
34.	Datensicherheit nach DSGVO – Einleitung	182
35.	Rechtsgrundlagen zur Datensicherheit	183
35.1	Was ist eigentlich „Datensicherheit“?	183
35.2	Datensicherheit in der DSGVO	184
35.3	Grundsatz der „Integrität und Vertraulichkeit“ (Art. 5 Abs. 1 lit. f) DSGVO).	184
35.4	Sicherheit der Verarbeitung (Art. 32 DSGVO)	186
35.5	Weitere Rechtsgrundlagen zur Datensicherheit.	189
36.	Sanktionen bei Nicht- oder Schlechtumsetzung von Daten- sicherheit	192
37.	Haftungsrisiken bei Nicht- oder Schlechtumsetzung von Daten- sicherheit	193
38.	Umsetzung von Datensicherheit (Theorie)	195
38.1	Datensicherheit für „Beginner“	195
38.2	Wie und wieviel Datensicherheitsmaßnahmen muss ich denn treffen?	197
38.3	Was wollen wir schützen?	198

38.4	Hilfreiche Dokumente	198
38.5	Schritt 1 – Die Analyse	199
38.6	Schritt 2 – Die Schutzbedarfsfeststellung	200
38.7	Schritt 3 – Die Risikoanalyse.....	202
38.8	Schritt 4 – Maßnahmen treffen	204
39.	Überlegung für eine praktikable Umsetzung von Datensicherheit in KMU	205
40.	Wie organisiere ich als DSB meine Arbeit?	206
41.	Wie fange ich an? – Erste Schritte als DSB	209
	Zu Beginn – Organisation und Abläufe kennenlernen	209
42.	Wir bauen uns ein Datenschutzmanagementsystem (DSMS).....	212
42.1	Top-Management ins Boot holen.....	213
42.2	Leitlinie zu Datenschutz und Informationssicherheit	213
42.3	Datensicherheits-/Datenschutz-Team bilden	217
42.4	Verarbeitungsverzeichnis	217
42.5	TOM-Dokument.....	217
42.6	Beispiel: TOM-Dokument	218
42.7	Kritische Prozesse identifizieren & Schutzbedarf feststellen	223
42.8	Risikoanalyse in „dreieckig“.....	224
42.9	Richtlinien erstellen und verbindlich machen	226
42.10	Richtlinie zum Datenschutz (für Beschäftigte)	227
42.11	Richtlinie zur Umsetzung von Datenschutzmaßnahmen...	229
42.12	Richtlinie für die Umsetzung von Betroffenenrechten	234
42.13	IT-Richtlinie für Nutzer	236
42.14	Richtlinie für Speicherorte.....	242
42.15	Richtlinie für die Nutzung mobiler IT-Systeme.....	244
42.16	Richtlinie für die Nutzung mobiler Datenträger	246
42.17	Richtlinie Regelungen für Lieferanten und sonstige Auf- tragnehmer	249
42.18	Richtlinie für Störungen und Ausfälle.....	252
42.19	Richtlinie für Sicherheitsvorfälle.....	253
42.20	Notfallplan	255
42.21	Evaluierung	258
43.	Schlusswort	259
	QR-Code zum Download der Muster	260