

Praxishandbuch Datenschutz für KMU

Schritt für Schritt zur sinnvollen
DSGVO-Compliance

HERAUSGEGEBEN VON

Dr. Karsten Kinast, LL.M.

Dr. Daniel Stanonik, LL.M.

Inhaltsverzeichnis

Vorwort	V
Autorenverzeichnis	XVII
Kapitel 1: Die Benennung des Datenschutzbeauftragten	1
A. Wer benötigt einen Datenschutzbeauftragten?	1
I. Allgemeines	1
II. Der DSB im Konzern	2
III. Der separate DSB im Betriebsrat	2
B. Wie wird man DSB?	3
I. Wonach sucht das Unternehmen den Datenschutzbeauftragten aus?	3
1. Interner DSB	4
2. Externer DSB	4
II. Persönliche und fachliche Voraussetzungen	5
1. Informations- und Kommunikationstechnologie	5
2. Datenschutzrechtliches Wissen	5
3. Erweitertes Fachwissen	5
4. Aktualität	5
5. Betriebswirtschaftliche und organisatorische Kompetenz	6
6. Persönliche Integrität	6
7. Beratungskompetenz	6
8. Unabhängigkeit und Weisungsungebundenheit	6
C. Wie erfolgt die Benennung?	7
I. Schriftliche Benennung	7
II. Meldepflicht des Verantwortlichen bezüglich der Benennung	7
D. Welche Voraussetzungen muss das Unternehmen nach der Benennung des DSB schaffen?	7
I. Datenschutzkoordination	7
II. Zusammenarbeit mit den Abteilungen	7
III. Erreichbarkeit des DSB	8
E. Was sind die Aufgaben des DSB?	8
I. Management	8
II. Überwachung	8
III. Beratung	8
IV. Schulung	8
V. Berichts- und Informationspflicht	8
VI. Verschwiegenheitspflicht	9

F. Wie endet die Benennung als DSB?	9
I. Interner DSB	9
II. Externer DSB	9
G. Zusammenfassung	10

Kapitel 2: Die datenschutzrechtlichen Verantwortlichkeiten und die Organisation innerhalb des Unternehmens

A. Verantwortlichkeiten innerhalb des Unternehmens	11
B. Die Organisation der Tätigkeit des DSB	12
I. Unterrichtung aller Mitarbeiter über die Benennung	12
II. Prozesse für Kommunikation mit DSB	12
III. Wem berichtet der DSB?	12
IV. Zuständigkeiten	13
V. Ansprechpartner im Unternehmen für den DSB	13
VI. Je nach Bedarf Einrichtung eines „DSB-Teams“	14
VII. Ressourcen	14
VIII. Wer ist haftbar: Verantwortlicher, Auftragsverarbeiter, DSB?	14
IX. Das Verhältnis zwischen Betriebsrat, DSB und Verantwortlichem?	15
X. Kommunikation mit Aufsichtsbehörden und Betroffenen	15
C. Zusammenfassung	15

Kapitel 3: Schwachstellenanalyse

A. Erste Phase: Durchführung Schwachstellenanalyse	17
I. Schwachstellenanalyse-Plan	18
II. Erläuterungen zum Schwachstellenanalyse-Plan	29
B. Zweite Phase: Bericht und Maßnahmenumsetzung	32
C. Zusammenfassung	36

Kapitel 4: Umsetzung einzelner Maßnahmen

Kapitel 4.1: Zulässigkeit der Datenverarbeitung

A. Die Verarbeitung personenbezogener Daten	37
B. Prüfung einer Datenverarbeitung	39
I. Rechtmäßigkeit der Datenverarbeitung	40
1. Datenverarbeitungen nach Maßgabe des Art 6 DSGVO	40
a. Einwilligung, Art 6 Abs 1 lit a DSGVO	40
b. Vertragserfüllung, Art 6 Abs 1 lit b DSGVO	41
c. Erfüllung einer rechtlichen Verpflichtung, Art 6 Abs 1 lit c DSGVO	41
d. Lebenswichtige Interessen, Art 6 Abs 1 lit d DSGVO	42

e. Aufgabe im öffentlichen Interesse, Art 6 Abs 1 lit e DSGVO	42
f. (Überwiegendes) Berechtigtes Interesse, Art 6 Abs 1 lit f DSGVO	43
2. Verarbeitung von sensiblen Daten (Art 9 DSGVO)	44
a. Einwilligung, Art 9 Abs 2 lit a DSGVO	44
b. Schutz lebenswichtiger Interessen, Art 9 Abs 2 lit c DSGVO	44
c. Öffentlich gemachte sensible Daten, Art 9 Abs 2 lit e DSGVO	44
d. Geltendmachung von Rechtsansprüchen, Art 9 Abs 2 lit f DSGVO	45
e. Verarbeitung im Kontext nationaler oder unionsrechtlicher Vorschriften	45
II. Grundsätze der Datenverarbeitung auf Grundlage des Art 5 DSGVO	46
C. Umsetzung	49
I. Handlungsempfehlung	49
II. Folgen von Rechtsverstößen	49
D. Häufige Fragen und Antworten	50
E. Zusammenfassung	50
Kapitel 4.2: Die technischen und organisatorischen Maßnahmen	50
A. Ausführungen zu einzelnen (Zwecken von) TOM	51
I. Pseudonymisierung	53
II. Verschlüsselung	55
III. Vertraulichkeit	55
IV. Integrität	56
V. Verfügbarkeit	57
VI. Belastbarkeit	57
VII. Wiederherstellbarkeit	57
VIII. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit	57
IX. Beurteilung des angemessenen Schutzniveaus	58
X. Sonderfall bei der Beurteilung des angemessenen Schutzniveaus für Auftragsverarbeitungen: Gewährleistung einer Verarbeitung nur nach Anweisungen des Verantwortlichen	59
XI. Sonderfall Forschungsorganisationsgesetz in Österreich	60

B. Umsetzung	60
I. Handlungsempfehlung	60
II. Folgen von Rechtsverstößen	60
C. Häufige Fragen und Antworten	61
D. Zusammenfassung	62
Kapitel 4.3: Datenschutz durch Technikgestaltung („Privacy by Design“) und durch datenschutzfreundliche Voreinstellung („Privacy by Default“)	62
A. „Privacy by Design“	63
B. „Privacy by Default“	68
C. Zertifizierung	69
D. Adressat	69
E. Welche technischen und organisatorischen Maßnahmen sind zu ergreifen?	69
F. Umsetzung	70
I. Handlungsanweisung	70
II. Folgen von Rechtsverstößen	70
G. Häufige Fragen und Antworten	71
H. Zusammenfassung	72
Kapitel 4.4: Auftragsverarbeitung	73
A. Muster: Auftragsverarbeitungsvertrag	75
B. Erläuterungen zum Muster	88
C. Beispiele für Auftragsverarbeitungen	92
D. Umsetzung	93
I. Handlungsempfehlung	93
II. Folgen von Rechtsverstößen	94
E. Häufige Fragen und Antworten	95
F. Zusammenfassung	95
Kapitel 4.5: Datenübermittlung in Drittstaaten	96
A. Datenübermittlung aufgrund eines Angemessenheitsbeschlusses (Art 45 DSGVO)	96
B. Datenübermittlung vorbehaltlich geeigneter Garantien (Art 46 DSGVO)	98
C. Verbindliche Datenschutzvorschriften (Art 47 DSGVO)	100
D. Vollstreckung und Anerkennung von Entscheidungen aus Drittländern betreffend die Offenlegung von Daten (Art 48 DSGVO)	101
E. Ausnahmen für bestimmte Fälle (Art 49 DSGVO)	101

F. Umsetzung	104
I. Handlungsempfehlung	104
II. Folgen bei Rechtsverstößen	104
G. Häufige Fragen und Antworten	105
H. Zusammenfassung	106
Kapitel 4.6: Gemeinsam Verantwortliche	106
A. Muster – Vertrag zwischen gemeinsamen Verantwortlichen	107
B. Der Weg zu einer Vereinbarung zwischen den gemeinsam Verantwortlichen	114
C. Beispiele für eine gemeinsame Verantwortlichkeit	116
D. Umsetzung	117
I. Handlungsempfehlung	117
II. Folgen von Rechtsverstößen	119
E. Häufige Fragen und Antworten	119
F. Zusammenfassung	120
Kapitel 4.7: Cloud-Computing	120
A. Was ist Cloud-Computing?	120
B. Wozu dient Cloud-Computing?	121
C. Was ist aus datenschutzrechtlicher Sicht bei Cloud-Computing zu beachten?	122
D. Umsetzung	122
I. Handlungsempfehlung	122
1. Auswahl des Cloud-Dienstleisters	122
2. Vertragliche Grundlage	123
3. Die Nutzung von Cloud-Computing-Diensten	124
II. Folgen bei Rechtsverstößen	126
E. Häufige Fragen und Antworten	126
F. Zusammenfassung	127
Kapitel 4.8: Betriebsrat und Betriebsvereinbarungen	127
A. Die Verarbeitung personenbezogener Daten durch den Betriebsrat	128
I. Aufgaben des Betriebsrats	128
II. Der Betriebsrat als eigener Verantwortlicher	128
III. Datenschutzrechtliche Befugnisse	129
B. Betriebsvereinbarungen	129
I. Geltung der DSGVO für Betriebsvereinbarungen	131
II. Reichweite der datenschutzbezogenen Betriebsvereinbarungen	131

C. Umsetzung	132
I. Handlungsempfehlung	132
II. Folgen von Rechtsverstößen	133
D. Häufige Fragen und Antworten	134
E. Zusammenfassung	134
Kapitel 4.9: Die Einwilligung der betroffenen Person	134
A. Mustereinwilligungen	135
B. Voraussetzungen einer Einwilligung	137
I. Freiwilligkeit	137
II. Konkreter Fall (Bestimmtheit)	139
III. Unmissverständlichkeit der Erklärung	140
IV. Informationspflichten in Zusammenhang mit dem Erteilen einer Einwilligung	141
C. Widerrufsrecht, Art 7 Abs 3 DSGVO	142
D. Einwilligung eines Kindes, Art 8 DSGVO	143
E. Typische Anwendungsfälle für eine erforderliche Einwilligung	144
F. Umsetzung	144
I. Handlungsempfehlung	144
II. Folgen von Rechtsverstößen	145
G. Häufige Fragen und Antworten	145
H. Zusammenfassung	146
Kapitel 4.10: Informationspflichten	146
A. Muster: Informationspflichten im Rahmen der Verarbeitung von Beschäftigtendaten	146
I. Informationspflichten bei Erhebung von personenbezogenen Daten bei der betroffenen Person	150
1. Verantwortlicher	151
2. Datenschutzbeauftragter	151
3. Datenkategorien	151
4. Zweck und Rechtsgrundlage der Verarbeitung	151
5. Weitergabe und Drittstaatübermittlung	152
6. Angaben zu Betroffenenrechten	152
7. Widerspruch	153
8. Speicherdauer	153
9. Pflicht zur Bereitstellung	153
II. Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden	154
B. Zeitpunkt der Information	154

C. Ausnahmen von der Informationspflicht	154
D. Umsetzung	155
I. Handlungsempfehlung	155
II. Folgen bei Rechtsverstößen	156
E. Häufige Fragen und Antworten	156
F. Zusammenfassung	157
Kapitel 4.11: Betroffenenrechte	157
A. Muster	158
B. Die Betroffenenrechte im Einzelnen	161
I. Auskunftsrecht der betroffenen Person	161
II. Recht auf Berichtigung	165
III. Recht auf Löschung	165
IV. Recht auf Einschränkung der Verarbeitung	166
V. Recht auf Datenportabilität	167
VI. Widerspruchsrecht	168
VII. Beschwerderecht	169
C. Umsetzung	169
I. Handlungsempfehlung	169
II. Folgen bei Rechtsverstößen	170
D. Häufige Fragen und Antworten	170
E. Zusammenfassung	171
Kapitel 4.12: Verpflichtung auf die Vertraulichkeit und das Datengeheimnis	172
A. Mustervorlagen	172
I. Vertraulichkeitserklärung	172
II. Verschwiegenheitsverpflichtung eines Auftragsverarbeiters	176
B. Erläuterung zu den Mustern	178
C. Umsetzung	180
I. Handlungsempfehlung	180
II. Folgen bei Rechtsverstößen	181
D. Häufige Fragen und Antworten	181
E. Zusammenfassung	182
Kapitel 4.13: Das Verzeichnis von Verarbeitungstätigkeiten	183
A. Muster – Verarbeitungsverzeichnis	184
B. Inhalt des Verarbeitungsverzeichnisses	194
C. Beispiel für Verarbeitungstätigkeiten	195

D. Umsetzung	196
I. Handlungsempfehlung	196
II. Folgen bei Rechtsverstößen	197
E. Häufige Fragen und Antworten	197
F. Zusammenfassung	198
Kapitel 4.14: Die Datenschutz-Folgenabschätzung	199
A. Verarbeitungsvorgänge, die eine DSFA erfordern	201
I. Deutschland	202
II. Österreich	212
1. Blacklist als Positivliste für durchzuführende DSFA	212
2. Whitelist über nicht durchzuführende DSFA	220
B. Muster zur Datenschutz-Folgenabschätzung	221
C. Vorgehensweise bei einer Datenschutz-Folgenabschätzung	226
I. Ausgangsfrage: Muss eine DSFA überhaupt durchgeführt werden?	226
II. Durchführung einer DSFA	227
D. Umsetzung	232
I. Handlungsempfehlung	232
II. Folgen bei Rechtsverstößen	232
E. Häufige Fragen und Antworten	233
F. Zusammenfassung	233
Kapitel 4.15: Datenpannen	234
A. Muster – Internes Vorgehen bei Datenpannen	234
B. Erläuterungen zum Vorgehen bei Datenpannen	236
I. Meldung seitens des zuständigen Mitarbeiters	236
II. Sachverhaltsermittlung	236
III. Sofortmaßnahmen	239
IV. Entscheidung über Meldepflicht	239
V. Weitere Maßnahmen	239
C. Beispiele für Datenpannen	239
I. Definition	239
II. Typische Beispiele	240
D. Meldepflicht an die zuständige Aufsichtsbehörde	241
E. Benachrichtigung des Betroffenen, Art 34 DSGVO	250
F. Umsetzung	251
I. Handlungsempfehlung	251
1. Zeitpunkt der Meldung	251
2. Dokumentation	251
II. Folgen von Rechtsverstößen	252

G. Häufige Fragen und Antworten	252
H. Zusammenfassung	253
Kapitel 4.16: Datenschutzerklärung auf der Website	254
A. Musterdatenschutzerklärung für Websitebetreiber	254
B. Inhalt einer Datenschutzerklärung	268
C. Umsetzung	272
I. Handlungsempfehlung	272
II. Folgen von Rechtsverstößen	272
D. Häufige Fragen und Antworten	273
E. Zusammenfassung	274
Kapitel 4.17: Die Zertifizierung	275
A. Zertifizierende Stellen	276
B. Inhalt der Zertifizierung	276
C. Umsetzung	277
I. Handlungsempfehlung	277
II. Nutzen einer Zertifizierung	278
III. Folgen von Rechtsverstößen	278
D. Häufige Fragen und Antworten	279
E. Zusammenfassung	280
Kapitel 5: Datenschutz in den einzelnen Abteilungen	
Kapitel 5.1: Datenschutz in der Personalabteilung	281
A. Wer ist Mitarbeiter?	282
B. Bewerbungs- und Einstellungsphase	283
C. Beschäftigungszeit im Unternehmen	284
I. Personalakten	284
II. Erhebung und anschließende Verwendung von Mitarbeiterfotos	285
III. Mitarbeiterbewertungen	286
IV. Lohn- und Gehaltsabrechnungen	286
V. Geburtstagslisten	287
VI. Mitarbeiterportal	287
VII. Weitergabe von Mitarbeiterdaten an Dritte	288
VIII. Private Nutzung von dienstlicher Hard- und Software	288
IX. Vorsicht vor der Überwachung von Mitarbeitern	289
D. Ende des Beschäftigungsverhältnisses	290
E. Umsetzung	290
F. Zusammenfassung	296

Kapitel 5.2: Datenschutz in der IT-Abteilung	297
A. PDCA-Modell	297
B. Angemessene technische und organisatorische Maßnahmen	298
I. Ausgangssituation und Vorüberlegungen	298
II. Gewährleistungsziele	299
III. Risikobewertung	299
IV. Bestimmen von Abhilfemaßnahmen	300
1. Protokollierung	301
2. Dokumentation	301
3. Löschen und Vernichten	302
C. Zusammenfassung	302
Kapitel 5.3: Datenschutz in der Marketing-Abteilung	302
A. Kundenmanagementsystem	302
B. Newsletter	303
C. Werbung	305
D. Website	306
E. Social Media	306
F. Zufriedenheitsumfragen	307
G. Messestand	307
H. Datenkauf (Adresshandel)	308
I. Zusammenfassung	309
Kapitel 6: Bußgelder und andere Sanktionen	311
A. Handlungsmöglichkeiten der Aufsichtsbehörden	311
B. Andere Sanktionen	314
C. Bußgelder und Sanktionen in der Praxis	314
D. Adressat der Bußgelder und Sanktionen	315
E. Zusammenfassung	316
Kapitel 7: Schulungen	317
Kapitel 8: Datenschutz-Maintenance	321
Stichwortverzeichnis	325