

Neues Datenschutzrecht

in der Reihe:

Bearbeitungs- und Prüfungsleitfaden

Prozesse prüfen * Risiken vermeiden * Fehler aufdecken

→ Handlungsempfehlungen ableiten

Bearbeitungs- und Prüfungsleitfaden

Neues Datenschutzrecht

Mike Bona-Stecki

Manager/Auditor Informationssicherheit
DekaBank
Frankfurt am Main

Dr. Martin Andreas Duncker (Hrsg.)

Dr. Martin Andreas Duncker Rechtsanwalt und Fachanwalt
für Bank- und Kapitalmarktrecht Zertifizierter Compliance-
Beauftragter (IHK & TÜV) Schlatter Rechtsanwälte
Steuerberater PartGmbH

Thomas Göhrig

Berater für Informationssicherheit und Datenschutz
FCH Compliance GmbH

Dr. Ulrich Hallermann (Hrsg.)

Dr. Ulrich Hallermann Rechtsanwalt und Fachanwalt für
Arbeitsrecht Datenschutzbeauftragter Investitions- und
Strukturbank Rheinland-Pfalz (ISB)

Dr. Markus Lang

Dr. Markus Lang Rechtsanwalt Externer
Datenschutzbeauftragter

Christian Maull (Hrsg.)

Spezialist Compliance
FCH Compliance GmbH
Heidelberg



Dr. Stephanie Müller
Referentin beim Bundesbeauftragten
für den Datenschutz und die Informationsfreiheit

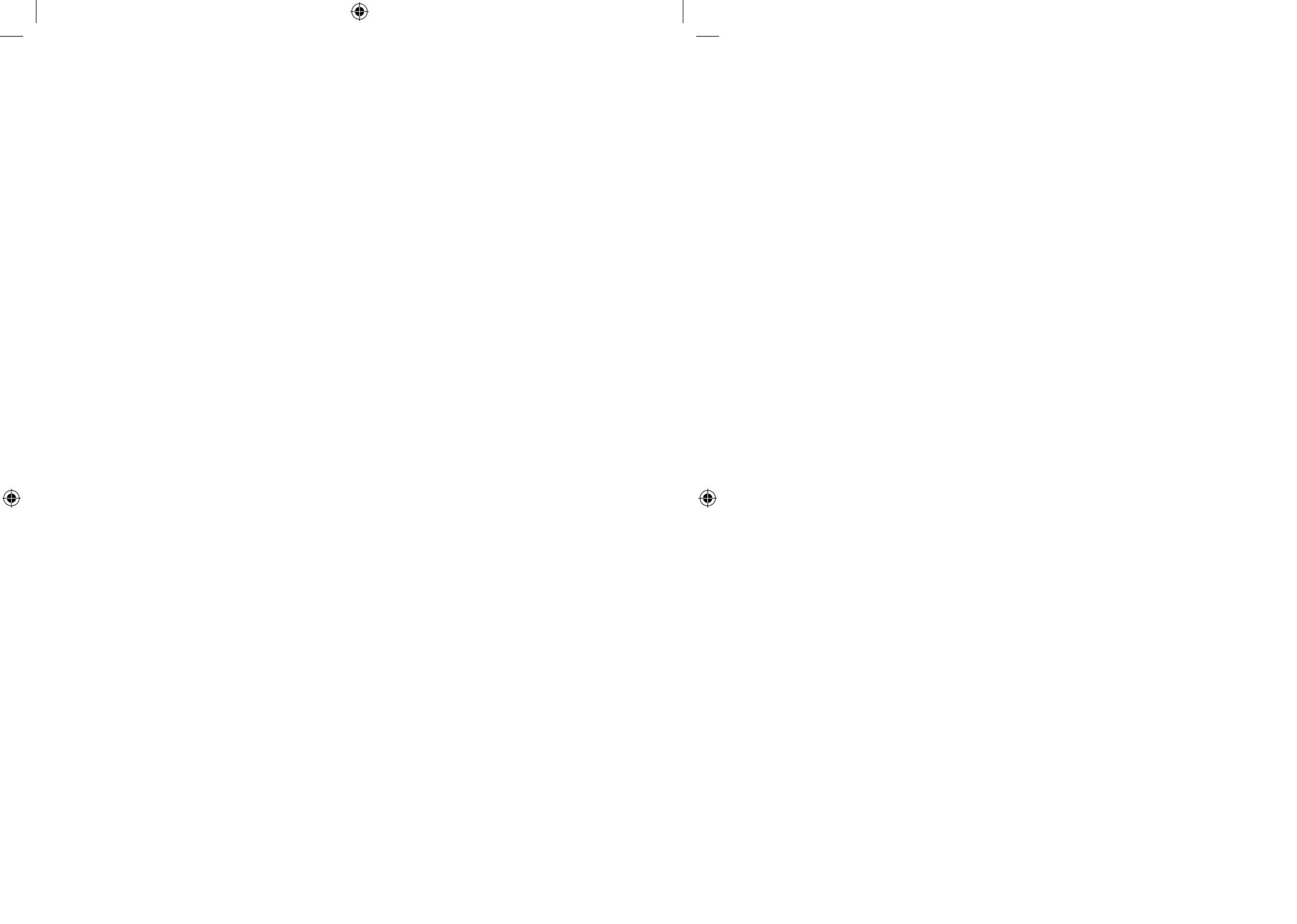
Denise Primus
Rechtsanwältin
Schlatter Rechtsanwälte Steuerberater PartG mbB
Heidelberg

Jürgen Ranger
Projektleiter Strategische Projektportfoliosteuerung
Creditplus Bank AG
Stuttgart



Inhaltsübersicht

A. Vorwort (<i>Mauß</i>)	1
B. Aufsichtliche Würdigung (<i>Müller</i>)	5
C. Aufbau und Funktion der Datenschutzorganisation (<i>Ranger</i>)	15
D. Löschpflicht und Löschkonzepte (<i>Duncker/Primus</i>)	57
E. Kundendatenschutz (<i>Lang</i>)	107
F. Beschäftigtendatenschutz und Fraud Maßnahmen (<i>Hallermann</i>)	165
G. Technische und organisatorische Maßnahmen (<i>Bona-Stecki</i>)	213
H. Aktuelle Sonderthemen des Datenschutzes (<i>Mauß</i>)	271
I. Datenschutz bei Datenauswertungen & Big Data (<i>Göbrig</i>)	299



Inhaltsverzeichnis

A. Vorwort	1
B. Aufsichtliche Würdigung	5
I. Inhalte und Bedeutung des Datenschutzmanagements	7
II. Zuständigkeiten und Zusammenspiel der Behörden	8
1. Bundesrepublik Deutschland	8
2. EU	9
3. Zusammenarbeit mit anderen Staaten	12
4. Aufgaben und Befugnisse der Aufsichtsbehörden	13
III. Datenschutzkontrollen und Zertifizierungen	14
C. Aufbau und Funktion der Datenschutzorganisation	15
I. Verhältnis von Compliance-Funktion, Risikomanagement und Datenschutz	17
II. Grundsätze des Datenschutzes	21
1. Zulässigkeit der Verarbeitung und Grundsatz der Zweckbindung	23
2. Grundsatz der Datensparsamkeit und -Vermeidung/ Verhältnismäßigkeitsgrundsatz	24
III. Datenschutzbeauftragter	28
1. Benennung und Stellung des Datenschutzbeauftragten	28
2. Aufgaben des Datenschutzbeauftragten	29
3. Eignung durch Fachkunde und Zuverlässigkeit	32
IV. Bestandteile des Datenschutzmanagements	33
1. Verarbeitungsverzeichnis	33
2. Datenschutz-Richtlinie	40
3. Risikoanalysen und Datenschutzfolgenabschätzungen	43
4. Technische und organisatorische Maßnahmen	48
5. Vertragswesen der verantwortlichen Stelle mit Dritten	51

a)	Auftragsverarbeitungsverträge	51
b)	Verträge bei gemeinsamer Datenverantwortlichkeit	53
c)	Datenübermittlungen in Drittstaaten	53
D.	Löschpflicht und Löschkonzepte	57
I.	Datenschutzrechtliche Einordnung	59
1.	Zum Begriff »Löschen«	62
2.	Verarbeitungsverbot mit Erlaubnisvorbehalt	63
3.	Recht auf Löschung und Pflicht zur Löschung	63
a)	Löschgründe	64
b)	Einschränkung der Löschpflicht: Rückausnahmen	69
c)	Zusätzliche Maßnahmen bei erfolgter Veröffentlichung: Informationspflicht	76
4.	Löschpflicht nach Zweckerreichung?	79
5.	Rechtsfolge: »Unverzügliches« Löschen der personenbezogenen Daten	81
II.	Technische und organisatorische Umsetzung der Löschpflichten	82
1.	Löschkonzepte in ERP-Systemen	88
a)	Mögliche Vorgehensweisen	89
b)	Häufige Probleme/Risiken	90
c)	Praxishinweise	91
2.	Löschkonzepte in Laufwerkstrukturen/ Verzeichnisstrukturen	92
a)	Mögliche Vorgehensweisen	93
b)	Häufige Probleme/Risiken	94
c)	Praxishinweise	95
3.	Papierhafte Aufbewahrungsformen wie Ordnersysteme oder Archive	97
a)	Mögliche Vorgehensweisen	97
b)	Häufige Probleme/Risiken	98
c)	Praxishinweise	98
III.	Sperrung von Datensätzen als Alternative zur Löschung	99
1.	Rechtliche Einordnung	100

INHALTSVERZEICHNIS

2.	Technisch-organisatorische Umsetzung	101
3.	Häufige Probleme/Risiken	102
4.	Praxishinweise	102
IV.	Zusammenfassung	103
V.	Literaturverzeichnis	103
E.	Kundendatenschutz	107
I.	Ausgangspunkt	109
1.	Datenschutz und Bankgeheimnis	109
2.	Datenschutzrechtliche Zulässigkeit	110
II.	Analyse von Kundendaten	111
1.	Wesentliche Vorgaben	111
2.	Checkliste	113
3.	Praxishinweise	114
III.	Scoring	114
1.	Wesentliche Vorgaben	115
a)	Erlaubnistatbestände	115
b)	Weitere Vorgaben gem. § 31 BDSG	116
2.	Checkliste	117
3.	Praxishinweise	120
IV.	Automatisierte Entscheidungen im Einzelfall	121
1.	Wesentliche Vorgaben	121
a)	Zulässigkeit	122
b)	Profiling	122
2.	Checkliste	123
3.	Praxishinweise	125
V.	Datenweitergabe an Auskunftfeien	125
1.	Wesentliche Vorgaben	125
2.	Checkliste	128
3.	Praxishinweise	128

VI. Verarbeitung zu werblichen Zwecken und werbliche Ansprache	129
1. Wesentliche Vorgaben	129
a) Verarbeitung zu Zwecken der Werbung auf Basis von Art. 6 Abs. 1 lit. f DSGVO	130
b) Verarbeitung zu Zwecken der Werbung auf Basis einer Einwilligung	132
c) Werbung per Telefon, Fax, SMS und E-Mail	134
2. Checkliste	136
3. Praxishinweise	139
VII. Kundenzufriedenheitsbefragungen	140
1. Wesentliche Vorgaben	140
2. Checkliste	141
3. Praxishinweise	142
VIII. Widerspruchsrecht	143
1. Wesentliche Vorgaben	143
a) Allgemeines Widerspruchsrecht	143
b) Widerspruchsrecht bei Direktwerbung	144
2. Checkliste	145
3. Praxishinweise	146
IX. Recht auf Auskunft	147
1. Wesentlicher Inhalt	147
a) Pflicht zur Auskunft	147
b) Inhalt der Auskunft	147
c) Verfahren und Form der Auskunft	149
d) Ausnahmen von der Auskunftspflicht	150
e) Verstoß gegen die Auskunftspflicht	151
2. Checkliste	151
3. Praxishinweise	153
X. Weitere Rechte der Kunden (Berichtigung, Löschung und Einschränkung)	154
1. Wesentliche Vorgaben	155
a) Recht auf Berichtigung	156

b) Recht auf Löschung	156
c) Recht auf Einschränkung der Verarbeitung	157
d) Recht auf Datenübertragbarkeit	158
2. Checkliste	159
3. Praxishinweise	160
XI. Melde- und Benachrichtigungspflicht bei Verletzung des Datenschutzes nach Art. 33 und 34 DSGVO	160
1. Wesentliche Vorgaben	160
2. Checkliste	162
3. Praxishinweise	163
XII. Literaturverzeichnis	163
F. Beschäftigtendatenschutz und Fraud Maßnahmen	165
I. Grundlagen des Beschäftigtendatenschutzes	167
1. Die rechtliche Ausgangslage unter Berücksichtigung der Datenschutzgrundverordnung	167
a) Definition des Beschäftigten	167
b) Datenschutz des Beschäftigten	167
c) Checklisten	172
2. Datenschutz in der Bewerbungsphase	175
a) Erheben und Speichern in der Bewerbungsphase	175
b) Verarbeiten und Nutzen in der Bewerbungsphase	176
c) Problematik der AGG Klagen auch im Datenschutz?	177
d) Facebook, Fanpages und der Datenschutz	177
3. Datenschutz im Beschäftigtenverhältnis	179
a) Erheben und Speichern nach Einstellung	179
b) Verarbeiten und Nutzen im Beschäftigtenverhältnis	179
c) Auftragsverarbeitungen (Art. 28 DSGVO) und gemeinsame Verantwortung (Art. 26 DSGVO)	180
d) Datenschutzfolgenabschätzung	181
e) Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)	181
f) Verpflichtung auf das Datengeheimnis nach der DSGVO	182

g)	Betriebsvereinbarungen	182
h)	Informationspflichten gegenüber Arbeitnehmern gem. Art. 13 DSGVO	183
4.	Checklisten	184
a)	Checkliste für den Fachbereich	184
b)	Zusammenfassende Checkliste für die Revision/Wirtschaftsprüfung	190
5.	Übermittlung personenbezogener Daten im Konzern	191
a)	Wesentliche Vorgaben	191
b)	Checkliste	192
II.	Datenschutz und Compliance	193
1.	Abgrenzung von Datenschutz und Compliance	193
2.	Ergebnis	194
3.	Checklisten	195
a)	Checkliste für betroffene Abteilungen (insbesondere Personal und Datenschutz)	195
b)	Checkliste für Revision und Wirtschaftsprüfung	196
III.	Zulässigkeit der Verarbeitung von Mitarbeiter- und Kundendaten in Research Systemen	197
1.	Abgrenzung zur datenschutzrechtlichen Zulässigkeit der Aufdeckung von begangenen Straftaten	197
2.	Die Regelung zum Research in § 25 h KWG	198
3.	§ 25 h KWG und der Datenschutz	198
4.	Vorschlag für die Praxis	199
5.	Checklisten	200
a)	Hausintern (Fraud, Geldwäsche und Datenschutz)	200
b)	Checkliste für Revision und Wirtschaftsprüfung	203
IV.	Erhebung von Beschäftigtendaten zur Aufdeckung von Straftaten/behördliche Ermittlungsbefugnisse	204
1.	Aufdeckung von Straftaten und behördliche Ermittlungsbefugnisse	204
a)	Grundlagen zur Aufdeckung von Straftaten	204
b)	Behördliche Ermittlungsbefugnisse	206

c) Aufdeckung von Straftaten durch die Videüberwachung (BAG vom 23.08.2018, 2 AZR 133/18)	207
2. Checklisten	208
a) Checklisten Aufdeckung von Straftaten	208
b) Checklisten Behördliche Ermittlungsbefugnisse	210
V. Zusammenfassende Praxistipps	211
VI. Literaturhinweise	211
G. Technische und organisatorische Maßnahmen	213
I. Einführung	215
1. Grundlagen und Begriffsbestimmung	215
2. Rechtliche Einordnung	216
3. Änderungen durch die DSGVO	217
II. Überblick über die technischen und organisatorischen Maßnahmen	218
1. Vertraulichkeit	219
a) Wesentliche Inhalte	219
b) Risiken	219
c) Maßnahmen	220
d) Checkliste	226
e) Praxishinweise	229
2. Integrität	229
a) Wesentliche Inhalte	229
b) Risiken	229
c) Maßnahmen	230
d) Checkliste	232
e) Praxishinweise	232
3. Verfügbarkeit/Belastbarkeit	232
a) Wesentliche Inhalte	232
b) Risiken	233
c) Maßnahmen	233
d) Checkliste	239
e) Praxishinweise	242

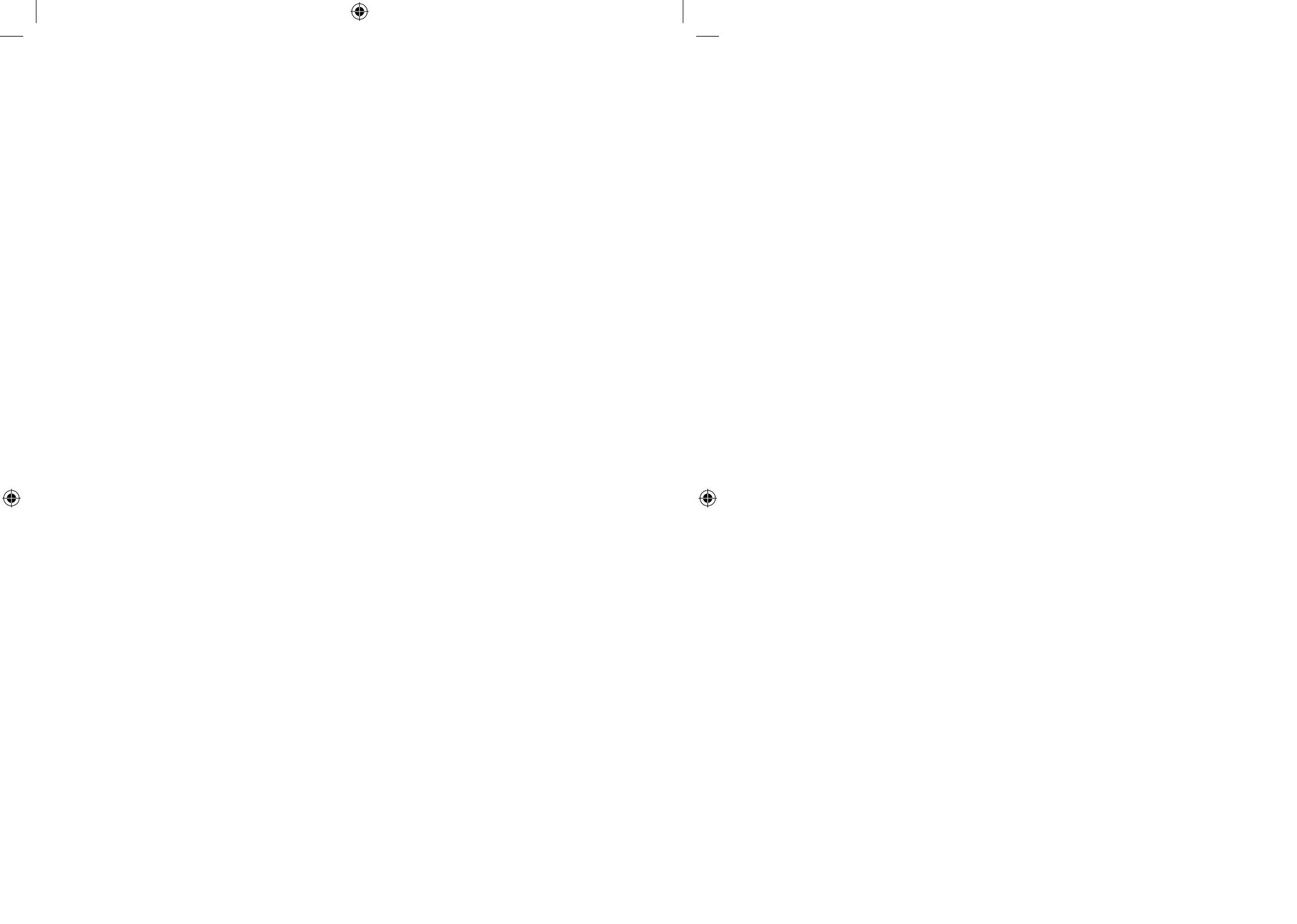
4.	Wiederherstellbarkeit bei physischen oder technischen Zwischenfällen	242
a)	Wesentliche Inhalte	242
b)	Risiken	243
c)	Maßnahmen	243
d)	Checkliste	248
e)	Praxishinweise	249
5.	Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit	249
a)	Wesentliche Inhalte	249
b)	Risiken	250
c)	Maßnahmen	250
d)	Checkliste	252
e)	Praxishinweise	253
6.	Pseudonymisierung und Verschlüsselung personenbezogener Daten	253
a)	Wesentliche Inhalte	253
b)	Risiken	254
c)	Maßnahmen	254
d)	Checkliste	256
e)	Praxishinweise	257
III.	Wahl der geeigneten Maßnahmen	258
1.	Grundsätzliches	258
2.	Nutzung von Standards und Normen	261
3.	Standard-Datenschutzmodell	263
IV.	Sicherheit der Verarbeitung bei Auftragsverarbeitungen und Auftragsverarbeiter	264
1.	Vorgaben an Auftragsverarbeitungen und Auftragsverarbeiter	264
a)	Rechtliche Grundlagen	264
b)	Risiken	264
c)	Maßnahmen	264
d)	Checkliste	266
e)	Praxishinweise	267

2. Überwachung der Einhaltung	267
a) Vor-Ort-Kontrollen	268
b) Nachweise, Zertifikate oder Testate	268
c) Praxishinweise	269
V. Literaturverzeichnis	269
H. Aktuelle Sonderthemen des Datenschutzes	271
I. Messengerdienste	273
1. Beschreibung des Themas	273
2. Datenschutzrechtliche Einordnung	274
3. Praxishinweise	290
II. ePrivacy-VO	290
1. Ausblick	290
2. Praxistipps	296
III. Literaturverzeichnis	297
I. Datenschutz bei Datenauswertungen & Big Data	299
I. Reichweite des Begriffs »personenbezogene Daten«	301
II. Einführung eines BI-Tools	302
1. Organisatorische Rahmenbedingungen	302
2. Datenschutzrechtliche Beurteilung	302
a) Rechtmäßigkeit und Zweckbindung	303
b) Datenminimierung und Speicherbegrenzung	306
c) Richtigkeit	307
d) Integrität und Vertraulichkeit	307
3. Checkliste	309
III. Datenschutz-Folgenabschätzung	310
1. Vorprüfung	310
2. Durchführung der Folgenabschätzung	311
a) Beschreibung der Verarbeitung	311
b) Notwendigkeit und Verhältnismäßigkeit	312
c) Risikobewertung	312

INHALTSVERZEICHNIS

d) Maßnahmen	312
e) Standpunkt der Betroffenen	313
f) Restrisiko	313
IV. Datenauswertungen	314
1. Organisatorische Rahmenbedingungen	314
2. Datenschutzrechtliche Beurteilung	315
a) Rechtmäßigkeit und Zweckbindung	315
b) Datenminimierung und Speicherbegrenzung	316
c) Richtigkeit	316
d) Integrität und Vertraulichkeit	317
V. Checkliste	318

A.
Vorwort



A. Vorwort

Zum 25. Mai 2018 trat die Europäische Datenschutz-Grundverordnung (EU-DSGVO) in Kraft und ersetzte das bisherige Bundesdatenschutzgesetz (BDSG) als maßgebende Rechtsvorschrift in Sachen Datenschutz. Parallel zur EU-DSGVO trat das neue Bundesdatenschutzgesetz in Kraft und konkretisiert die für die EU-Mitgliedsstaaten in der EU-DSGVO enthaltenen Öffnungsklauseln. 1

Im Jahre 1970 verabschiedete Hessen das erste Datenschutzgesetz der Welt und schuf somit den ersten Meilenstein des deutschen Datenschutzrechts. Seitdem folgten zahlreiche technische und rechtliche Entwicklungen und der Schutz personenbezogener Daten gewann zunehmend an Bedeutung. Aufgrund dieser Historie verwundert es nicht, dass auch in der Neuregelung des Datenschutzrechts altbekannte Themen in mehr oder minder bekanntem Umfang wiederzufinden sind. Trotz alledem ist die EU-DSGVO mehr als alter Wein in neuen Schläuchen, denn ihre Einführung brachte umfangreiche Änderungen und Herausforderungen mit sich, welche Verantwortliche Stellen noch heute beschäftigen. Die Spannweite der Handlungsfelder reicht von Dokumentations- und Nachweispflichten, über die Umsetzung von Betroffenenrechten und technisch-organisatorischen Maßnahmen, bis hin zu Sonderkonstellationen bei Datenübermittlungen innerhalb und außerhalb eines Unternehmens oder einer Unternehmensgruppe, sowohl im europäischen In- als auch im Ausland. 2

Die Summe der einzelnen Themen und deren Verknüpfung untereinander erforderte die Einführung eines Datenschutzmanagements zur rechtskonformen Umsetzung regulatorischer Anforderungen und der gleichzeitig möglichst hohen Effektivität getroffener Maßnahmen. In seiner neuen Ausrichtung unter der EU-DSGVO wurde die Datenschutzfunktion mehr und mehr an bestehende Compliance-Funktionen angepasst und verortet sich nunmehr als Bestandteil der zweiten Verteidigungslinie im Modell der three-lines-of-defense. 3

Dieses Buch dient sowohl als Arbeitsunterlage für Datenschutzbeauftragte, Syndikusrechtsanwälte, Rechtsanwälte, Berater und Wissenschaftler, sowie als Prüfungshilfe für Revisoren und Datenschutzauditoren. Es befasst sich sowohl mit den Grundlagen des Datenschutzes als auch themenspezifischen Herausforderungen, sowie aktuellen rechtlichen Entwicklungen und Erfahrungen der Aufsichtsbehörden und unterstützt durch zahlreiche praxisorientierte Checklisten im Alltag. 4