

SCHLÄGER • THODE (Hrsg.)

Handbuch Datenschutz und IT-Sicherheit

Leseprobe, mehr zum Werk unter www.ESV.info/17727

ESV ERICH
SCHMIDT
VERLAG

datenschutz nord
GRUPPE

Handbuch Datenschutz und IT-Sicherheit

Herausgegeben von

Dr. Uwe Schläger und Jan-Christoph Thode

Unter Mitarbeit von

Dr. Christian Borchers, Conrad S. Conrad, Michael Cyl,
Dr. Sebastian Ertel, Annika Freund, Clemens Grünwald,
Jennifer Jähn, Dr. Irene Karper, Jan-Roman Kitzinger,
Dr. Martin Klein-Hennig, Martin Kolodziej, Dr. Bettina
Kraft, Dr. Sönke Maseberg, Dr. Britta Mester, Lars Meyer,
Dr. Sanela Hodžić, Lea Paschke, Jan Peplow, Olaf Rossow,
Jan Schirmacher, Dr. Uwe Schläger, Felix Schmidt, Markus
Schönmann, Stefan R. Seiter, Daniel Stolper, Oliver Stutz,
Jan-Christoph Thode, Sven Venzke-Caprarese,
Ralf von Rahden

Leseprobe, mehr zum Werk unter www.ESV.info/17727

ERICH SCHMIDT VERLAG

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Weitere Informationen zu diesem Titel finden Sie unter

ESV.info/978 3 503 17727 1

Gedrucktes Werk: ISBN 978 3 503 17727 1

eBook: ISBN 978 3 503 17728 8

Alle Rechte vorbehalten.

© Erich Schmidt Verlag GmbH & Co. KG, Berlin 2018

www.ESV.info

Dieses Papier erfüllt die Frankfurter Forderungen der Deutschen Nationalbibliothek und der Gesellschaft für das Buch bezüglich der Alterungsbeständigkeit und entspricht sowohl den strengen Bestimmungen der US Norm Ansi/Niso Z 39.48-1992 als auch der ISO-Norm 9706.

Satz: schwarz auf weiß, Herrig & Schimschok, Berlin

Druck und Bindung: Hubert & Co., Göttingen

Aus: Dr. Uwe Schläger und Jan-Christoph Thode,
Handbuch Datenschutz und IT-Sicherheit
© Erich Schmidt Verlag GmbH & Co.KG, Berlin 2018

Vorwort

Am 25. Mai 2018 ersetzt die EU-Datenschutz-Grundverordnung das bisherige Bundesdatenschutzgesetz. Nach jahrelanger Diskussion wird damit europäisches Datenschutzrecht endlich harmonisiert, sehr zum Vorteil international tätiger Unternehmen, aber auch zum Vorteil kleinerer Online-Shops, die sich bislang innerhalb der EU nach den jeweils geltenden nationalen Datenschutzvorschriften richten mussten.

Trotz der Harmonisierung kommen auf Unternehmen neue Herausforderungen zu: Neben erweiterten Informations-, Rechenschafts- und Meldepflichten gilt es, für Verfahren mit hohen Risiken für die Persönlichkeitsrechte der Betroffenen eine Datenschutz-Folgenabschätzung durchzuführen. Auftragsverarbeiter müssen künftig ebenso wie Verantwortliche ein Verzeichnis von Verarbeitungstätigkeiten führen. Auch die Eignung technischer und organisatorischer Sicherheitsmaßnahmen muss künftig regelmäßig überprüft und dokumentiert werden. Ganz zu schweigen von den deutlich erweiterten und erhöhten Bußgeldern, die künftig von Datenschutz-Aufsichtsbehörden verhängt werden können.

Die mit der Datenschutz-Grundverordnung verbundenen Neuerungen sollten für Unternehmen, die sich bislang konform zum Bundesdatenschutzgesetz aufgestellt haben, kein besonderes Problem darstellen. Wer bislang seine datenschutzrechtlichen Hausaufgaben erledigt hat, kann auf bestehenden Datenschutzstrukturen aufbauen, muss diese allerdings an einigen Stellen anpassen und gegebenenfalls erweitern. Unternehmen mit gravierenden Datenschutzdefiziten, die in der Vergangenheit eher darauf vertraut haben, nicht negativ aufzufallen, drohen allerdings nunmehr drastische Bußgelder.

Und hier setzt unser neues Datenschutz-Handbuch an: Wir, dies sind erfahrene Beraterinnen und Berater der datenschutz nord Gruppe, die seit Jahren in den Bereichen Datenschutz und Informationssicherheit als Consultant tätig sind, haben für Sie ein Datenschutz-Handbuch erstellt, das zum einen auf die neuen gesetzlichen Regelungen der Datenschutz-Grundverordnung im Detail eingeht. Zum anderen stellen wir Ihnen Best-Practice-Ansätze vor, wie den neuen gesetzlichen Vorgaben am besten entsprochen werden kann.

Das vorliegende Datenschutz-Handbuch richtet sich an betriebliche Datenschutzbeauftragte, IT-Administratoren, Unternehmensleitungen, Betriebs- oder Personalräte, aber auch an datenschutzinteressierte Beschäftigte und Kunden, die sich entweder einen Überblick über die neuen gesetzlichen Regelungen verschaffen wollen oder praxisgerechte Vorschläge zur Umsetzung der Datenschutz-Grundverordnung nachlesen möchten.

Das Datenschutz-Handbuch gliedert sich im Wesentlichen in zwei Hauptteile: Die Kapitel A bis F sind datenschutzrechtlich geprägte Kapitel, während die Kapitel G

bis J sicherheitstechnische Aspekte in den Vordergrund stellen. Nachdem wir in Kapitel A zunächst auf die neuen datenschutzrechtlichen Grundlagen eingehen, stellen wir in Kapitel B vor, wie ein betriebliches Datenschutz-Management umgesetzt werden sollte. In Kapitel C steht die gesetzeskonforme Verarbeitung von Beschäftigtendaten im Vordergrund, in Kapitel D die gesetzeskonforme Verarbeitung von Kundendaten. Kapitel E beschäftigt sich mit der Verarbeitung personenbezogener Daten im Internet, in sozialen Netzwerken und in unternehmens-eigenen Intranets. Kapitel F stellt dar, in welchem Umfang Videosysteme nach der neuen Datenschutz-Grundverordnung betrieben werden können.

Der zweite Hauptteil des Handbuches beginnt in Kapitel G mit einer Darstellung der rechtlichen Grundlagen der IT-Sicherheit. In Kapitel H werden die Eckpfeiler eines Informationssicherheits-Managements beschrieben. Kapitel I stellt geeignete technisch-organisatorische Maßnahmen vor, und zwar übergreifende Maßnahmen, Infrastrukturmaßnahmen, Maßnahmen seitens der IT-Systeme, Netzwerkmaßnahmen und Maßnahmen auf Anwendungsebene. Und schließlich wird in Kapitel J beschrieben, in welcher Form Penetrationstest zur Evaluierung einer angemessenen IT-Sicherheit durchgeführt werden können.

Trotz der zahlreichen Verweise auf andere Kapitel dieses Buches sind sämtliche Hauptkapitel in sich abgeschlossen und können separat ohne Kenntnis der anderen Kapitel als Erkenntnisquelle dienen.

In diesem Sinne wünschen wir Ihnen als Herausgeber dieses Datenschutz-Handbuchs viel Spaß beim Lesen und Nachschlagen.

Bremen und Berlin, im Januar 2018

Uwe Schläger und
Jan-Christoph Thode

Inhaltsverzeichnis

Vorwort	V
Inhaltsverzeichnis	VII
Bearbeiterverzeichnis	XXVII
Abkürzungsverzeichnis	XXIX
Literaturverzeichnis	XXXIII

	Seite	Rn.
Teil A		
Datenschutzrechtliche Grundlagen	1	
1. Geschichte des Datenschutzrechts	3	1
1.1. Erste Entwicklungen	3	2
1.2. Das Volkszählungsurteil des Bundesverfassungsgerichts ..	4	7
1.2.1. Recht auf informationelle Selbstbestimmung	4	8
1.2.2. Schutzbereich	6	12
1.2.3. Schranken	6	13
1.2.4. Weiterentwicklung des Rechts auf informatio- nelle Selbstbestimmung	7	15
1.2.5. Langfristige Bedeutung	8	19
1.3. Entwicklung der Datenschutzgesetze in Deutschland ...	9	22
1.3.1. Bedarf an Datenschutzgesetzen	9	23
1.3.2. Landesdatenschutzgesetze	10	26
1.3.3. Bundesdatenschutzgesetz	11	28
1.3.4. Gesetzgebungskompetenz	12	33
1.3.5. Verhältnis Bundesdatenschutzgesetz – Daten- schutzgesetze der Länder	13	35
1.3.6. Europarechtliche Regelungen	13	36
EU-Grundrechte	14	37
Primär- und Sekundärrecht	15	44
Datenschutz-Richtlinie 95/46/EG	16	46
Weitere europarechtliche Vorschriften	17	52
DSGVO	21	61
2. Datenschutzrecht in Deutschland und in der EU	23	64
2.1. Maßgebliche Rechtsquellen	23	64
2.1.1. Datenschutz-Grundverordnung	23	66
2.1.2. Bundesdatenschutzgesetz-neu	24	71
2.1.3. ePrivacy-Verordnung	25	73
2.2. Grundlagen der Datenverarbeitung	26	76
2.2.1. Verbot mit Erlaubnisvorbehalt	26	76
Einwilligung	26	78
Gesetzliche Erlaubnistatbestände	30	98

2.2.2.	Personenbezogene Daten	31	103
2.2.3.	Besondere personenbezogene Daten.	33	111
2.2.4.	Besondere Verarbeitungssituationen.	34	114
2.3.	Datenschutzrechtliche Grundsätze	34	117
2.3.1.	Rechtmäßigkeit	34	120
2.3.2.	Treu und Glauben	35	121
2.3.3.	Transparenz	35	124
2.3.4.	Zweckbindung.	36	126
2.3.5.	Datenminimierung	37	131
2.3.6.	Richtigkeit	38	135
2.3.7.	Speicherbegrenzung	39	137
2.3.8.	Integrität und Vertraulichkeit	39	139
2.3.9.	Rechenschaftspflicht	40	143
2.4.	Betroffenenrechte	41	149
2.4.1.	Auskunft	42	151
2.4.2.	Berichtigung.	43	156
2.4.3.	Löschung	44	160
2.4.4.	Einschränkung der Verarbeitung	45	169
2.4.5.	Datenübertragbarkeit	46	172
2.4.6.	Widerspruch.	47	180
2.4.7.	Wahrnehmung der Rechte	48	184
	Identifizierung der betroffenen Person.	48	186
	Form und Frist	49	189
	Kosten	51	194
2.5.	Sanktionen	51	195
2.5.1.	Datenschutz-Grundverordnung	51	195
2.5.2.	Bundesdatenschutzgesetz-neu.	52	200
3.	Anwendungsbereich der DSGVO.	53	201
3.1.	Niederlassungsprinzip	55	210
3.1.1.	Tätigkeit einer Niederlassung	55	212
3.1.2.	Datenverarbeitung im Rahmen einer Niederlassung	57	218
3.2.	Marktortprinzip.	57	220
3.2.1.	Anbieten von Waren oder Dienstleistungen.	58	224
3.2.2.	Beobachtung des Verhaltens.	60	233
3.2.3.	Pflicht zur Benennung eines Vertreters.	61	238
3.3.	Sonderfall Völkerrecht	62	246
3.4.	Öffnungsklauseln	63	248
3.4.1.	Kollisionsnorm	63	249
3.4.2.	Situation in Deutschland	64	255
4.	Datenschutzrecht außerhalb von Europa.	66	263
4.1.	USA	66	263
4.1.1.	Allgemeine Übersicht.	66	263
4.1.2.	Maßgebliche Rechtsquellen	67	267
4.1.3.	Datenschutzrechtliche Grundsätze.	70	274

4.1.4.	Betroffenenrechte	72	282
4.1.5.	Sanktionen	73	290
4.2.	Japan	74	294
4.2.1.	Allgemeine Übersicht	74	294
4.2.2.	Maßgebliche Rechtsquellen	75	297
4.2.3.	Datenschutzrechtliche Grundsätze	77	303
4.2.4.	Betroffenenrechte	79	314
4.2.5.	Sanktionen	80	319
4.3.	Russland	81	323
4.3.1.	Allgemeine Übersicht	81	323
4.3.2.	Maßgebliche Rechtsquellen	82	325
4.3.3.	Datenschutzrechtliche Grundsätze	83	330
4.3.4.	Betroffenenrechte	88	355
4.3.5.	Sanktionen	89	358
Teil B			
	Datenschutzmanagement im Unternehmen	91	
1.	Der betriebliche Datenschutzbeauftragte	93	1
1.1.	Bestellpflicht	93	3
1.1.1.	Europarechtliche Regelung mit nationaler Öff- nungsklausel	93	3
1.1.2.	Bestellpflicht nach Art. 37 DSGVO	95	8
	Bestellpflicht für Behörden und öffentliche Stellen	95	10
	Bestellpflicht aufgrund Art, Umfang und Zweck der Verarbeitungsvorgänge	96	14
	Bestellpflicht wegen der Verarbeitung besonders sensibler Daten	98	24
1.1.3.	Gemeinsame Bestellung eines Datenschutzbe- auftragten durch eine Unternehmensgruppe	99	29
	Unternehmensgruppe	100	31
	Sofern von jeder Niederlassung aus leicht er- reicht werden kann.	100	32
	Formvorschriften	100	33
1.1.4.	Die Bestellpflicht nach nationalem Recht – § 38 BDSG-neu	101	36
1.2.	Mitteilungspflicht gegenüber der Aufsichtsbehörde	101	38
1.3.	Qualifikation	102	93
1.3.1.	Berufliche Qualifikation / Fachwissen	102	40
1.3.2.	Persönliche Fähigkeiten	103	43
1.4.	Wahrnehmung durch natürliche oder auch juristische Person?	104	47
1.5.	Stellung im Unternehmen	105	50
1.5.1.	Bereitstellung von Ressourcen	105	52
1.5.2.	Umfassende Einsicht und Unterstützung	106	54

1.6.	Aufgaben	107	58
1.6.1.	Beratung und Information	107	58
1.6.2.	Überwachung der Einhaltung der Verordnung – Einrichtung eines Datenschutzmanagements	108	61
1.6.3.	Zusammenarbeit mit der Aufsichtsbehörde	109	66
1.6.4.	Wahrnehmung von Betroffenenrechten	110	69
	Arbeitnehmer-Betroffenenrechte und neue In- formationspflichten	110	70
1.6.5.	Zeitpunkt und Ausnahmen	112	78
	Kunden-Betroffenenrechte	113	81
1.6.6.	Ansprechpartner für die Aufsichtsbehörde	113	83
1.7.	Abberufung	113	84
2.	Verzeichnis von Verarbeitungstätigkeiten	115	86
2.1.	Sinn und Zweck der Dokumentation	115	87
2.2.	Zuständigkeit	115	89
2.3.	Adressaten	116	91
2.4.	Inhalt und Form	116	94
2.5.	Historie und Aktualisierungsintervall	118	102
3.	Datenschutz-Folgenabschätzung	120	104
3.1.	Anwendungsbereich	120	104
3.2.	Durchführung	121	109
3.2.1.	Informationsbeschaffung	123	114
3.2.2.	Checkliste	123	115
3.2.3.	Bewertung	124	116
4.	Verpflichtung auf das Datengeheimnis	126	119
4.1.	Verpflichtung nach § 5 BDSG-alt	126	119
4.2.	Praxisnahe Umsetzung im Unternehmensumfeld	126	122
4.3.	Adressaten	127	125
4.4.	Sanktionen bei Verletzung	128	127
5.	Meldepflicht bei Datenpannen	129	128
5.1.	Meldepflicht gegenüber der Aufsichtsbehörde	129	128
5.2.	Meldender	130	134
5.3.	Inhalt, Art und Weise und Frist der Meldung	130	135
5.4.	Ausnahme – Risikoabwägung	131	140
5.5.	Dokumentation	132	142
5.6.	Meldepflicht gegenüber dem Betroffenen	132	144
5.7.	Inhalt, Art und Weise und Frist der Meldung	132	145
5.8.	Ausschlussgründe	133	146
6.	Outsourcing	135	150
6.1.	Auftragsverarbeitung – Chancen und Risiken	135	150
6.1.1.	Änderungen durch die DSGVO	135	152
6.1.2.	Dienstleister außerhalb der EU	136	154
6.1.3.	Anpassungen von Verträgen zur Auftragsverar- beitung	137	157
6.2.	Abgrenzung zur Funktionsübertragung	138	162

6.3.	Gemeinsam für die Verarbeitung Verantwortliche.	138	163
6.4.	Übermittlung an Drittländer außerhalb der EU	138	164
6.4.1.	Übermittlung auf Grundlage eines Angemessenheitsbeschlusses	139	165
6.4.2.	Übermittlung auf Grundlage von Binding Corporate Rules	140	168
6.4.3.	Übermittlung auf Grundlage der EU-Standardvertragsklauseln	142	173
7.	Kontrolle des Datenschutzes	143	175
7.1.	Rolle des Datenschutzbeauftragten	143	175
7.2.	Abgleich der Verfahrenspraxis mit Verfahrensverzeichnis ..	143	177
7.3.	Abgleich der Verfahrenspraxis mit Betriebsvereinbarungen oder Richtlinien	143	178
7.4.	Auditierung der Auftragsverarbeiter	144	180
7.5.	Nachweis durch Zertifikate	145	184
7.6.	Dokumentation	145	185
8.	Datenlöschung	146	186
8.1.	Das Praxisproblem – Warum soll ich Daten löschen?	146	186
8.2.	Bestandsaufnahme für Löschfristen	147	190
8.3.	Erstellung eines Löschkonzepts	147	192
8.3.1.	(Automatisierte) Umsetzung von Löschpflichten ..	147	192
8.3.2.	Sicher löschen – Vorgaben des BSI	148	194
9.	Datenweitergabe im Konzern	150	198
9.1.	Konzernprivileg	151	200
9.2.	Auftragsverarbeitung im Konzern	152	204
9.3.	Gemeinsame Verantwortlichkeit	152	207
9.4.	Übermittlung innerhalb Europas	155	216
9.4.1.	Einwilligung	156	218
9.4.2.	Vertragserfüllung	157	222
9.4.3.	Rechtliche Verpflichtung	157	224
9.4.4.	Interessenabwägung	158	226
9.5.	Beschäftigtendaten	159	230
9.6.	Übermittlung außerhalb Europas	160	237

Teil C

	Verarbeitung von Beschäftigtendaten	163	
1.	Regelungen zum Beschäftigtendatenschutz	165	1
1.1.	Öffnungsklausel	165	4
1.2.	Regelungen im BDSG-neu	166	7
1.3.	Betriebsvereinbarungen	167	17
2.	Bewerbermanagement	169	20
2.1.	Zulässigkeit der Verarbeitung im Bewerbungsverfahren ..	169	22
2.1.1.	Fragerecht des Arbeitgebers	169	23
2.1.2.	Recherche des Arbeitgebers in sozialen Netzwerken	172	39

	Freizeitorientierte soziale Netzwerke.....	172	40
	Berufsorientierte soziale Netzwerke.....	173	43
2.1.3.	Ärztliche Untersuchungen und psychologische Tests	173	44
	Einstellungsuntersuchungen	173	44
	Psychologische Tests und Persönlichkeitstests. ...	174	48
2.2.	Dauer der Speicherung von Bewerberdaten	174	50
3.	Personalakten	176	58
3.1.	Inhalte.....	176	61
3.2.	Zugriffsrechte.....	177	67
3.3.	Aufbewahrungsdauer	178	69
3.4.	Rechte des Mitarbeiters.....	179	78
3.5.	Best Practice.....	180	83
4.	Zeiterfassung	182	91
4.1.	Abhängigkeit vom Arbeitszeitmodell	182	95
4.2.	Erfassung der Kommt-, Geht- und Pausenzeiten	182	97
4.3.	Zugriffsrechte.....	183	99
4.4.	Aufbewahrungszeiten	183	102
5.	Personalentwicklung	184	103
5.1.	Schulungssysteme/Learning Management Systems	185	111
5.1.1.	Pflichtschulungen und freiwillig angebotene Schulungen.....	185	112
5.1.2.	Zugriffsrechte	186	118
5.1.3.	Beauftragung von Dienstleistern	187	120
5.2.	Mitarbeitergespräche.....	187	121
5.2.1.	Krankenrückkehrgespräche	188	124
5.2.2.	Standardisierung im Unternehmen	188	125
5.3.	Arbeitszeugnisse und Performance-Management	188	128
5.3.1.	Arbeitszeugnisse	188	129
5.3.2.	Performance-Management	189	133
5.3.3.	Zugriffsrechte, Speicherfristen, Auftragsverarbeitung	190	136
5.4.	Mitarbeiterprofile (Persönlichkeitsprofile).....	190	139
5.4.1.	Erhebung von Softskills auf Grundlage einer Einwilligung.....	191	141
5.4.2.	Datenschutz-Folgenabschätzung.....	192	144
5.4.3.	Beauftragung von Dienstleistern	192	148
5.5.	Mitarbeiterbefragungen	193	149
5.5.1.	Anonyme Befragungen.....	193	152
5.5.2.	Personenbezogene Befragungen	194	155
5.5.3.	Best Practice.....	195	160
5.6.	360 Grad-Feedback.....	196	167
5.6.1.	Personenbezogene Datenerhebung.....	197	170
5.6.2.	Informationspflichten	198	175
5.6.3.	Datenschutz-Folgenabschätzung.....	198	177

9.4.2.	Whistleblowing/Hinweisgebersysteme.	231	317
	Vorgaben der Aufsichtsbehörden (Art. 29-Datenschutzgruppe und Düsseldorfer Kreis)	233	325
	Erheblichkeit des Vorwurfes	234	327
	Keine anonymen Hinweise	234	330
	Schutz der Identität des Hinweisgebers	235	331
	Dokumentationspflichten.	235	332
	Informationspflichten.	235	333
	Löschpflichten.	236	334
	Beachtung des Trennungsprinzips.	237	338
9.4.3	Einhaltung von Hygienevorschriften	237	339
9.4.4.	Bondatenanalysen	238	341
	Präventive Zwecke	238	342
	Repressive Zwecke	239	346
9.4.5	Tankkartenkontrolle	241	355
9.5.	Sonstiges	242	357
9.5.1.	Informationspflichten.	242	357
9.5.2.	Mitbestimmungsrechte	242	360
10.	Verarbeitung von Gesundheitsdaten	243	361
10.1.	Rechtliche Grundlagen	243	362
	Exkurs: Schweigepflichtentbindungserklärung	247	373
10.2.	Betriebsärztliche Untersuchungen.	248	376
10.2.1.	Arbeitsmedizinische Vorsorge	248	378
10.2.2.	Einstellungsuntersuchungen	250	385
10.3.	Eignungstests	250	388
10.4.	Betriebliches Eingliederungsmanagement.	252	392
11.	Betriebsrat und Datenschutz	257	405
11.1.	Stellung des Betriebsrats im Betriebsverfassungsgesetz. ...	257	406
11.2.	Aufgaben des Betriebsrats	257	409
11.3.	Verwendung von Beschäftigtendaten im BetrVG	258	414
11.3.1.	Subsidiarität des BDSG gegenüber dem BetrVG..	258	414
11.3.2.	Subsidiarität des BDSG gegenüber Betriebsvereinbarungen	259	419
11.3.3.	Betriebsvereinbarungen nach der DSGVO	261	428
11.4.	Stellung des Betriebsrats im BDSG	264	442
11.5.	Verantwortung des Betriebsrats für den Datenschutz.	266	458
11.5.1.	Pflichten nach dem BDSG	266	459
11.5.2.	Datensicherheit	267	467
11.5.3.	Verfahrensverzeichnis durch den Betriebsrat	268	471
11.6.	Verwendung von Beschäftigtendaten durch den Betriebsrat.	268	473
11.6.1.	Zugriff auf Daten der Personalverwaltung.	268	473
11.6.2.	Speichern von Beschäftigtendaten	269	478
11.6.3.	Veröffentlichung von Beschäftigtendaten.	269	480

11.7.	Kontrolle des Betriebsrats durch den Datenschutzbeauftragten	270	481
Teil D			
	Verarbeitung von Kundendaten	271	
1.	CRM-Systeme	273	1
1.1.	Aktuelle und bisherige Regelungen	273	3
1.2.	Erfüllung eines Vertrages	273	5
1.3.	Vorvertragliche Maßnahmen	275	12
1.4.	Erforderlichkeit	277	16
1.5.	Einzelne Kategorien von Daten	277	19
1.6.	Nutzung innerhalb eines Konzerns	278	23
2.	Marketing und Werbung	283	36
2.1.	Regelungen in der DSGVO	283	37
2.2.	Verschiedene Werbemaßnahmen	284	40
2.2.1.	Postalische Werbung	284	41
	Allgemeines	284	42
	Anwendungsfälle	285	46
2.2.2.	Elektronische Bewerbung (E-Mail und Fax)	287	56
	Notwendigkeit einer Einwilligung	287	57
	Nachweisbarkeit der Einwilligung	290	74
	Nachweis der Einwilligung bei Double-Opt-In-Verfahren	291	85
	Anwendungsfälle	292	88
	E-Mail-Werbung nach der ePrivacy-Verordnung	297	111
2.2.3.	Telefonische Bewerbung	298	114
	Mutmaßliche Einwilligung	298	115
	Ausdrückliche Einwilligung	298	116
	Verfall der Einwilligungserklärung	298	117
	Telefonische Werbung nach ePrivacy-Verordnung	299	120
2.3.	Widerspruchsrecht	299	121
2.3.1.	Werbewidersprüche (postalische Werbung)	299	124
2.3.2.	Widerruf der Einwilligung (elektronisch, Fax oder Telefon)	300	128
2.4.	Dokumentationspflichten	300	131
2.5.	Geldbußen	301	132
3.	Kundenbindungssysteme	302	134
3.1.	Kundenbindung versus Datenschutz	302	134
3.2.	Datenverarbeitung zur Programmabwicklung	305	153
3.2.1.	Verarbeitung der Stammdaten	305	154
3.2.2.	Verarbeitung von Programmdateien	306	159
3.3.	Datenverarbeitung für Werbung und Marktforschung	306	162
3.3.1.	Verarbeitung von Stamm- und Programmdateien	307	165
3.3.2.	Grenzen der Einwilligung	308	170
3.4.	Betroffenenrechte der Kundenkartenteilnehmer	311	183

3.5.	Kundenkartensysteme in der Praxis	312	188
4.	Unternehmenskauf	314	197
4.1.	Einwilligung und Betriebsübergang	314	198
4.2.	Datenaustausch vor einer Transaktion (Due-Diligence-Phase)	314	199
4.3.	Informationspflichten gegenüber der betroffenen Person .	316	207
4.4.	Vollzug einer Transaktion.	318	211
5.	Bonitätsmanagement (einschl. Scoring)	320	215
5.1.	Beteiligte des Bonitätsmanagements	321	221
5.2.	Datenübermittlung an eine Auskunftfei.	321	226
5.2.1.	Rechtsgrundlage	322	227
5.2.2.	Zulässigkeit der Übermittlung bestimmter Datenkategorien	323	231
5.2.3.	Zusammenspiel von Rechtsgrundlage und Einwilligung	328	254
5.3.	Allgemeine Bonitätsbewertung	329	258
5.3.1.	Informationsquellen	329	259
5.3.2.	Zulässigkeit allgemeiner Bonitätsbewertung	329	263
5.4.	Bonitätsbewertung mittels Scoring-Verfahren	331	271
5.4.1.	Einsatzbereiche	333	283
5.4.2.	Zulässigkeit des internen Scorings	335	297
5.4.3.	Zulässigkeit des externen Scorings	339	318
5.5.	Auskunfteien	340	323
5.5.1.	Abgrenzung zum internen Scoring	340	324
5.5.2.	Anwendbare Regelungen bei Auskunftstätigkeit .	340	326
5.6.	Datenschutz-Folgenabschätzung.	341	329
5.7.	Bestellung eines Datenschutzbeauftragten	342	333
5.8.	Konsultation der Aufsichtsbehörde.	342	334
5.9.	Rechte der betroffenen Person.	342	337
5.9.1.	Auskunftsrecht der betroffenen Person	342	338
5.9.2.	Informationspflichten gegenüber der betroffenen Person	344	345
5.9.3.	Widerspruchsrecht der betroffenen Person	345	349
5.9.4.	Verbot automatisierter Einzelentscheidung	346	353
5.10.	Best Practice.	349	369

Teil E

	Datenverarbeitung im Internet und Intranet	351	
1.	Webseiten	353	1
1.1.	Anwendbares Recht	353	3
1.2.	Informationspflichten	354	6
1.2.1.	Pflichtangaben nach § 5 TMG	354	7
	Rechtliche Grundlagen	354	7
	Platzierung auf Webseiten	354	8
	Platzierung in Apps.	355	11

	Pflichtangaben	356	13
1.2.2.	Pflichtangaben nach § 55 RStV	356	14
1.2.3.	Zusätzliche Pflichtangaben nach der DL-InfoV ..	357	17
1.2.4.	Neue Informationspflichten.....	357	18
1.3.	Datenschutzerklärung.....	357	20
1.3.1.	Rechtliche Grundlagen.....	357	20
1.3.2.	Platzierung auf der Webseite	358	21
1.3.3.	Inhalt	358	24
1.4.	Disclaimer	359	28
1.4.1.	Haftung für Inhalte.....	360	30
1.4.2.	Haftung für Links.....	360	32
1.4.3.	Wahrung des Urheberrechts.....	360	35
1.5.	Einwilligung auf Webseiten	361	36
1.5.1.	Voraussetzungen der Einwilligung	361	38
1.5.2.	Einwilligung bei Kindern.....	362	39
1.5.3.	Widerrufbarkeit.....	363	44
1.6.	Der Einsatz von Cookies	364	48
1.6.1.	Unklare Rechtslage.....	364	49
1.6.2.	Formen der Einwilligung.....	366	58
1.6.3.	Cookie-Varianten	367	64
1.6.4.	Voraussetzungen an den Einsatz von Cookies....	368	67
1.7.	Tracking-Tools.....	369	73
1.7.1.	Unterschiede	369	75
1.7.2.	Unklare Rechtsgrundlage.....	370	78
1.7.3.	Nutzerverhalten	372	87
1.7.4.	Retargeting.....	373	89
1.7.5.	Conversion Tracking.....	374	93
1.8.	Device Fingerprinting.....	374	97
1.9.	Newsletter	375	101
1.9.1.	Rechtliche Grundlage	376	102
1.9.2.	Rechtskonforme Umsetzung.....	376	103
1.10.	Kontaktformular	377	108
1.11.	Tell-a-Friend-Funktion.....	378	113
1.12.	Social-Media-Plugins	378	116
1.13.	Veröffentlichung von Mitarbeiterdaten und -fotos	379	119
1.13.1.	Allgemeine Mitarbeiterdaten	379	121
1.13.2.	Mitarbeiterfotos.....	379	124
1.14.	Gästebuch und Foren	380	128
1.15.	Bewerbungsportal	381	133
1.15.1.	Online-Registrierung bzw. Profilerstellung.....	382	134
1.15.2.	Speicherung bzw. Aufbewahrung im Unternehmen.....	383	138
1.16.	Rechtspflichten zur Sicherung von Webseiten	384	141
1.16.1.	Technische und organisatorische Maßnahmen....	384	142
1.16.2.	Verschlüsselte Übertragung	386	149

1.17.	Recht auf Datenübertragbarkeit	387	154
2.	Soziale Netzwerke	390	164
2.1.	Social-Media-Auftritt des Unternehmens.....	390	167
2.1.1.	Grundsätzliche Fragestellungen.....	391	168
2.1.2.	Impressum	394	176
	Exkurs: Snapchat.....	396	182
2.1.3.	Datenschutzerklärung.....	396	185
2.1.4.	Analysemöglichkeiten.....	397	188
	Mitgelieferte Analysen	397	189
	Implementierung eigener Analysemöglichkeiten..	399	195
2.1.5.	Nutzung des Application Interface	399	196
	Nicht öffentlich verfügbare Daten	399	198
	Öffentlich verfügbare Daten	400	202
2.1.6.	Absicherung des Social-Media-Auftritts.....	400	203
	Verwaltung durch eine Person.....	401	204
	Verwaltung durch mehrere Personen	401	205
	Zugriff für Drittanwendungen.....	401	207
2.1.7.	Veröffentlichung von Fotos	402	209
2.1.8.	Freundfinder	402	211
2.1.9.	Besonderheiten für Behörden	403	213
2.1.10.	Einwilligung.....	403	215
2.2.	Social-Media-Plugins und eingebettete Inhalte	403	216
2.2.1.	Problemstellung.....	404	219
2.2.2.	Reine Verlinkung.....	405	223
2.2.3.	Platzhaltergrafiken	405	225
2.2.4.	Webserverlösung.....	406	228
2.2.5.	Datenschutzeinstellungen bei der Einbindung... ..	407	230
2.3.	Marketing auf Social-Media-Plattformen	408	235
2.3.1.	Werbung per Direktnachricht	408	239
2.3.2.	Pinnwandveröffentlichungen.....	409	242
2.3.3.	Gesponserte Beiträge und Anzeigenwerbung ...	409	243
2.3.4.	Kampagnenziele	409	245
2.3.5.	Allgemeine Zielgruppendefinitionen.....	410	248
	Zielgruppendefinition anhand öffentlich verfügbarer Daten	410	249
	Zielgruppendefinition anhand demografischer Daten	412	256
	Interessenbasierte Zielgruppendefinition	413	258
	Verhaltensbasierte Zielgruppendefinition.....	413	259
	Standortbasierte Zielgruppendefinition	414	263
2.3.6.	Custom Audiences mit Personenlisten	414	264
2.3.7.	Retargeting – Custom Audiences from your Website.....	416	266
2.3.8.	Conversion Tracking.....	418	276
2.3.9.	Lookalike Audiences.....	419	279

2.4.	Social-Media-Recruiting	421	281
2.4.1.	Passives Recruiting	421	282
2.4.2.	Aktives Recruiting	421	283
2.5.	Nutzung von Social-Media-Diensten	422	285
2.5.1.	Social Login	422	286
2.5.2.	Facebook WLAN-Hotspot	423	288
2.5.3.	Bluetooth Low Energy Beacons	423	290
2.5.4.	Messenger und Messenger Bots	424	293
2.6.	Unternehmensinterne Social-Media-Nutzung	425	298
2.6.1.	Social-Media-Monitoring	425	298
2.6.2.	Social Media im Intranet	427	304
2.7.	Künftige Entwicklungen	427	305
3.	Intranet-Portale	429	308
3.1.	Datenschutzrechtliche Rahmenbedingungen	430	312
3.2.	Veröffentlichung von Kontaktdaten	431	319
3.3.	Veröffentlichung von Bildnissen	432	321
3.4.	Veröffentlichung von Qualifikationen und Lebensläufen ..	433	326
3.5.	Veröffentlichung von Geburtstagen	434	328
3.6.	Kalenderfunktion	434	331
3.7.	Unternehmensinterne Kommunikationsplattformen am Beispiel von Skype for Business	435	334
3.7.1.	Funktionen von Skype for Business	435	334
3.7.2.	Protokollierungsfunktion/Historie	435	337
3.7.3.	Dienstliche und private Nutzung von Skype for Business	436	341
	Rein dienstliche Nutzung	436	341
	Erlaubnis der privaten Nutzung	437	347
3.7.4.	Status- und Präsenzinformationen der Mitarbeiter	439	355
3.8.	Unternehmensinterne Intranet-Anwendungen am Bei- spiel von MS Yammer	440	361
3.8.1.	MS Yammer als Social-Media-Anwendung	440	361
3.8.2.	Datenschutzrechtliche Rahmenbedingungen	440	365
3.9.	Künftige Entwicklungen	442	372

Teil F

	Videoüberwachung im Unternehmen	443	
1.	Personenbeziehbarkeit und Verarbeitung von Bilddaten	445	1
2.	Rechtliche Grundlagen für Unternehmen	448	8
2.1.	Videoüberwachung mit Einwilligung	449	11
2.2.	Videoüberwachung aufgrund rechtlicher Verpflichtung ...	450	14
2.3.	Videoüberwachung im öffentlichen Interesse	450	16
2.4.	Videoüberwachung aufgrund Interessenabwägung	454	33
2.4.1.	Nachweisbarer Zweck der Videoüberwachung ...	455	36
2.4.2.	Verhältnismäßigkeit der Videoüberwachung	455	38
2.5.	Videoüberwachung von Beschäftigten	458	47

2.6.	Videüberwachung von Kindern	460	53
2.7.	Verdeckte Videüberwachung	461	57
3.	Sicherheitsmaßnahmen für Videosysteme.	463	59
3.1.	Hinweisschilder	463	60
3.2.	Löschung der Bilddaten	465	67
3.3.	Sonstige technische und organisatorische Pflichten	466	72
4.	Beispiele aus der Praxis	468	74
4.1.	Supermärkte und Einkaufszentren	468	74
4.2.	Gastronomie	468	77
4.3.	Banken, Spielhallen, Tankstellen	469	79
4.4.	Krankenhäuser, Arztpraxen und Heime	470	82
4.5.	Wohnobjekte und Hotels	470	85
4.6.	Baustellen	471	87
4.7.	Abfallbeseitigung, Müllcontainer	472	88
4.8.	Parkplätze, Parkhäuser, Kennzeichenerfassung	472	89
4.9.	Öffentliche Verkehrsmittel	472	91
4.10.	Dashcams in Unternehmensfahrzeugen	473	93
4.11.	Außenfassaden und Perimeterschutz	473	94
4.12.	Rechenzentren und Serverräume	474	96

Teil G

	Rechtliche Grundlagen der Informationssicherheit	475	
1.	Datenschutzgrundverordnung	477	1
1.1.	Technische und organisatorische Maßnahmen	477	2
1.1.1.	Unterschiede zum Bundesdatenschutzgesetz	477	4
1.1.2.	Verantwortlicher und Auftragsverarbeiter	478	7
1.1.3.	Eignung der Maßnahmen, Angemessenheit des Schutzniveaus	478	9
1.1.4.	Stand der Technik	479	12
1.1.5.	Implementierungskosten	479	14
1.1.6.	Eintrittswahrscheinlichkeit und Schwere des Risikos	480	17
1.1.7.	Art, Umfang, Umstände und Zweck der Verar- beitung	481	20
1.1.8.	Sicherheitsziele	483	29
1.1.9.	Datenschutz durch Technikgestaltung	484	35
1.2.	Pseudonymisierung	486	43
1.3.	Anonymisierung	488	48
1.4.	Verschlüsselung	489	50
1.5.	Durchführung von Tests	490	53
1.6.	Nachweispflichten	490	55
1.6.1.	Genehmigte Verhaltensregeln	491	58
1.6.2.	Genehmigte Zertifizierungsverfahren	491	62
2.	IT-Sicherheitsgesetz, europäische NIS-Richtlinie	494	70
2.1.	Betreiber kritischer Infrastrukturen	494	72

2.2.	Betreiber von Webseiten	496	80
2.3.	Anbieter digitaler Dienste	497	84
3.	Bereichsspezifische Normen	498	88
3.1.	Energiewirtschafts- und Messstellenbetriebsgesetz	498	89
3.2.	Kreditwesengesetz	498	92
3.3.	Glücksspielstaatsvertrag	500	95

Teil H

	IT-Sicherheitsmanagement im Unternehmen	501	
1.	Vorgehensweise	503	1
2.	Merkmale eines ISMS	505	10
2.1.	Management-Prinzipien	505	14
2.2.	Ressourcen	507	15
2.3.	Mitarbeiter	507	19
2.4.	Strategie	507	20
3.	ISO/IEC 27001 und IT-Grundschutz	510	26
3.1.	Unterschiede und Gemeinsamkeiten	510	26
3.2.	ISO/IEC 27000-er Normenreihe	511	33
3.2.1.	ISO/IEC 27001 als Basisnorm	512	36
3.2.2.	ISO/IEC 27002	513	38
3.2.3.	ISO/IEC 27004 für Messbarkeit	513	39
3.2.4.	ISO/IEC 27005 für Risikomanagement	513	41
3.2.5.	ISO/IEC 27011 für Telekommunikationsunter- nehmen	514	46
3.2.6.	ISO/IEC 27017 und ISO/IEC 27018 für Cloud- Dienste	514	47
3.2.7.	ISO/IEC TR 27019 für die Energiewirtschaft	514	48
3.2.8.	ISO/IEC 27799 für das Gesundheitswesen	515	49
3.3.	ISO 27001 auf der Basis von IT-Grundschutz	515	50
3.3.1.	Strukturanalyse	516	54
3.3.2.	Schutzbedarfsfeststellung	517	56
3.3.3.	Modellierung der IT-Grundschutz-Bausteine	517	57
3.3.4.	IT-Grundschutz-Check	517	59
3.3.5.	Ergänzende Risikoanalyse	517	60
3.3.6.	Modernisierung des IT-Grundschutzes	518	61
4.	Bedeutung von Zertifikaten	520	70

Teil I

	Technische und organisatorische Maßnahmen	523	
1.	Übergreifende Aspekte	525	1
1.1.	Behandlung von Sicherheitsvorfällen	525	1
1.1.1.	Incident Management	525	2
1.1.2.	Problem Management	526	7
1.1.3.	Notfall Management	526	10
1.2.	Hardware und Software Management	527	15

1.2.1.	Change Management.	527	16
1.2.2.	Asset Management	529	25
1.2.3.	Patch Management, Update Management	529	29
1.3.	Personal Management	530	34
1.3.1.	Sensibilisierung und Schulung	530	37
1.3.2.	Ein- und Austrittsprozess	531	41
1.3.3.	Sicherheitsüberprüfung.	532	47
1.4.	Datensicherung	533	49
1.4.1.	Datenart, Häufigkeit der Datensicherungen, Anzahl der Generationen	533	53
1.4.2.	Art der Datensicherung	534	56
1.4.3.	Speichermedien	535	59
1.4.4.	Aufbewahrung der Speichermedien	535	63
1.4.5.	Zeitpunkt der Erstellung	536	68
1.4.6.	Wiederherstellung der Datensicherungen.	537	71
1.4.7.	Einsatz eines Datensicherungssystems	537	72
1.5.	Archivierung	537	74
1.5.1.	Infrastruktur	538	76
1.5.2.	Speichermedien	538	78
1.5.3.	Dateiformate	539	81
1.5.4.	Einsatz elektronischer Signaturen	539	84
1.5.5.	Funktionstests	540	88
1.5.6.	Datensicherung des Archivsystems.	540	90
1.6.	Datenlöschung.	541	91
1.6.1.	Physische Vernichtung	541	93
1.6.2.	Digitales Löschen	542	97
	Magnetische Speichermedien	544	99
	Flash-Speicher	545	101
	Löschung von verschlüsselten Daten	545	105
1.6.3.	Einsatz von externen Dienstleistern	546	106
1.7.	Verschlüsselung	546	108
1.7.1.	Grundlagen der Verschlüsselung	546	110
	Symmetrische Verfahren.	546	110
	Asymmetrische Verfahren	547	114
	Algorithmen und Schlüssellängen	547	118a
	Schlüsselaustausch.	548	119
	Hash-Verfahren	549	123
1.7.2.	Anwendungen von Verschlüsselung	551	134
	Elektronische Signatur	551	135
	Transport-Verschlüsselung	552	142
	Ende-zu Ende-Verschlüsselung.	554	148
	Speicher-Verschlüsselung	554	152
1.7.3.	Schlüsselmanagement	555	155
1.8.	Getrennte Test- und Produktivsysteme	556	158
1.8.1.	Anonymisierte Testdaten	556	159

1.8.2.	Freigabeverfahren	557	163
1.9.	Cloud Computing	557	165
1.9.1.	Formen von Cloud Services	558	167
1.9.2.	Vertragliche Verpflichtung des Cloud-Dienste- anbieters	559	170
1.9.3.	Authentisierung der Anwender	560	177
1.9.4.	Verschlüsselung der übermittelten Daten	560	179
1.9.5.	Verschlüsselung der gespeicherten Daten	560	180
1.9.6.	Normen und Standards	561	182
2.	Infrastruktur	563	187
2.1.	Zutrittskontrollsysteme	563	191
2.2.	Brandschutzmaßnahmen	565	198
2.3.	Maßnahmen gegen Über- und Unterspannung	566	204
2.4.	Klimageräte	568	210
2.5.	Vermeidung wasserführender Leitungen	568	212
3.	IT-Systeme	569	213
3.1.	Serversysteme	569	214
3.1.1.	Allgemeine Maßnahmen zur Serverhärtung	569	215
3.1.2.	Serverspezifische Härtingsmaßnahmen	571	220
	Mailserver	571	221
	Webserver	572	223
	Datenbankserver	573	224
3.2.	Clientsysteme	574	225
3.2.1.	Allgemeine Maßnahmen zur Clienthärtung	574	226
3.2.2.	Anwendungsspezifische Maßnahmen zur Client-Härtung	575	227
	Webbrowser	575	227
	Mailclient	576	229
3.3.	Mobile Endgeräte und Mobile Device Management	576	230
3.4.	Verteilung und Verwaltung privilegierter Zugänge	577	234
4.	Netze	578	236
4.1.	Internetanbindung	579	238
4.1.1.	Firewall	579	239
4.1.2.	Intrusion Detection/Prevention Systeme	579	241
4.1.3.	Demilitarisierte Zonen	580	243
4.1.4.	VPN	580	245
	Site-to-Site und End-to-Site	580	247
	Tunnel- und Transport-Modus	581	251
	MPLS	581	252
4.2.	Intranet	582	254
4.2.1.	Network Access Control	582	255
4.2.2.	VLAN	583	259
4.2.3.	WLAN	584	261
4.3.	Verzeichnisdienste	585	257
4.3.1.	LDAP und Kerberos	585	268

4.3.2.	Active Directory	586	270
4.3.3.	Linux/UNIX-Domains	587	275
4.4.	Administration.....	588	276
4.4.1.	Monitoring.....	588	277
4.4.2.	Security Information and Event Management	588	280
5.	Anwendungen	590	284
5.1.	Identifizierung, Authentisierung und Autorisierung.....	590	286
5.1.1.	Identifizierung.....	590	287
5.1.2.	Authentisierung.....	591	290
	Passwortqualität	591	291
	Passwort-Tresore.....	592	294
	Single-Sign-On-Verfahren	592	296
	Zwei-Faktor-Authentisierung	593	299
	Session Management bei Web-Applikationen	594	300
5.1.3.	Autorisierung.....	594	304
5.2.	Berechtigungs- und Rollenkonzepte.....	595	306
5.3.	Mandantentrennung	596	311
5.4.	Protokollierung von Anwendungsaktivitäten	597	316

Teil J

	Penetrationstest	599	
1.	Vorgehensweise	601	1
1.1.	Kickoff	602	5
1.2.	Durchführung der Tests	602	9
1.2.1.	Automatisierte Scans	602	9
1.2.2.	Erweiterte Tests und manuelle Prüfungen	603	12
1.3.	Auswertung und Dokumentation	604	16
1.4.	Ergebnispräsentation.....	604	16a
1.5.	Prüfung der Verbesserungsmaßnahmen	604	17
2.	Testszzenarien	605	19
2.1.	Black-Box.....	605	20
2.2.	White-Box	605	21
2.3.	Grey-Box	605	22
3.	Testmodule und Prüfungsthemen	607	23
3.1.	Systeme und Netzwerke	607	24
3.1.1.	Einsatz veralteter Software.....	608	28
3.1.2.	Verfügbarkeit von administrativen Zugängen	608	29
3.1.3.	Verwendung von trivialen Kennwörtern	609	30
3.1.4.	Ausgabe von sensiblen Informationen	609	31
3.1.5.	Test der Verschlüsselung.....	609	32
3.1.6.	Überprüfung von Zugriffsrechten.....	610	34
3.1.7.	Test der Netzanmeldung.....	610	35
3.1.8.	Man-In-The-Middle-Angriffe	611	36
3.2.	Anwendungen	611	37
3.2.1.	Auswertung von Fehlermeldungen.....	611	39

3.2.2.	Überprüfung der Verschlüsselung	612	40
3.2.3.	Überprüfung der Registrierung und Authentisierung	612	41
3.2.4.	Ausweitung von Zugriffsrechten	613	43
3.2.5.	Manipulation des Session-Managements	613	44
3.2.6.	Cross-Site-Scripting	614	45
3.2.7.	Replay-Angriffe	615	47
3.2.8.	Injection	616	49
	Stichwortverzeichnis		619

TEIL B

Datenschutzmanagement im Unternehmen

1. Der betriebliche Datenschutzbeauftragte

Der betriebliche Datenschutzbeauftragte hat in den letzten Jahrzehnten gerade im Hinblick auf die dauerhaft unterbesetzten Aufsichtsbehörden im deutschen Datenschutz eine herausragende Rolle als innbetriebliches bzw. innerbehördliches Instrument des Datenschutzmanagements erlangt. Dabei ist die „Figur“ des Datenschutzbeauftragten keine rein deutsche Erfindung – sie ist (vermutlich) nur aus unserer Sicht mehr und besser geeignet, Datenschutz in Unternehmen umzusetzen, als es behördliche Kontrollen, Anhörungen und Bußgelder vermögen. Das mag aber auch an der Art und Weise der Aufgabenwahrnehmung der Aufsichtsbehörden liegen, die, das darf aus vielen Jahren Erfahrung gesagt werden, häufig (Ausnahmen bestätigen auch hier die Regel!) eher an der dogmatischen Durchsetzung von Gesetznormen als an praxisnahen Lösungen interessiert sind – wenn diese nicht in jeder Hinsicht einer wortlautkonformen Umsetzung der Normen entsprechen. 1

Aus Sicht jedes Datenschutzbeauftragten, ganz gleich ob die Aufgabe intern, in Voll- oder Teilzeit oder extern wahrgenommen wird, sollte daher – durchaus in Abgrenzung und auch zum Teil als Korrektiv gegenüber dem Prüfungsansatz der zuständigen Aufsichtsbehörden – Datenschutz mit Augenmaß angestrebt werden. Eine in jeder Hinsicht über das ganze Unternehmen, alle Abteilungen hinweg und ggfls. sogar konzernweit 100%ige Einhaltung und Erfüllung sämtlicher Datenschutzanforderungen ist aus Praktiker-Sicht nahezu unerreichbar. Daher werden in diesem Buch als zentraler Maßstab Best-Practice-Ansätze vorgestellt und erläutert – diesen ist die Eigenschaft des Kompromisses immanent – des Kompromisses zwischen dem, was rechtlich geboten und was innerbetrieblich und vor allem auch finanziell machbar und möglich ist. 2

1.1. Bestellpflicht

1.1.1. Europarechtliche Regelung mit nationaler Öffnungsklausel

Lange Zeit war in den Beratungen zwischen Kommission, Rat und Parlament umstritten, ob und unter welchen Voraussetzungen überhaupt eine obligatorische Bestellung eines Datenschutzbeauftragten in den Gesetzestext aufgenommen werden sollte. Der Verordnungsgeber hat, das zeigen u.a. die Erwägungsgründe, die Bestellung eines Datenschutzbeauftragten auch nur als quasi ultima-ratio für besonders „riskante bzw. intensive, risikobehaftete“ Verarbeitungen verstanden: Zentrales Instrument der internen Datenschutzkontrolle soll nach dem Verständnis und auch nach dem Kontext der Regelungen zunächst die Datenschutz-Folgenabschätzung (Art. 35) sein¹. Erst wenn dieses Kontrollinstrument, welches ja ohnehin erst 3

¹ Vgl. dazu unten Rn. 104 ff.

bei einem vermuteten hohen Risiko der Verarbeitung für die persönlichen Rechte und Freiheiten durchzuführen ist, nicht mehr ausreicht, soll „in jedem Fall“ – so die für eine Rechtsnorm ungewöhnliche Formulierung – ein Datenschutzbeauftragter bestellt werden.

- 4 Die Überlegungen, unter welchen Voraussetzungen dies geschehen soll, reichten während der Beratungen von Mindestumsätzen der verantwortlichen Stellen bis hin zur Festlegung bestimmter Unternehmensgrößen, die mithilfe der Mitarbeiter-Anzahl bestimmt werden sollten (250 Mitarbeiter/500 Mitarbeiter u.Ä.). Ge- einigt hat man sich nun auf die nachfolgend genannten Voraussetzungen, die, um es offen zu sagen, wenig praxisnah sind, da die Kriterien so allgemein formuliert sind, dass hierunter verschiedenste Tätigkeiten subsumiert werden können – oder auch nicht.
- 5 Auch wird in den Formulierungen und vor allem der Öffnungsklausel in Abs. 4 deutlich, dass bis zum Schluss Uneinigkeit bei den Beratungen herrschte, ob die Grundverordnung die Voraussetzungen für die Bestellungen eines Datenschutz- beauftragten abschließend regeln sollte. Im Ergebnis hat der deutsche Gesetzge- ber von der Möglichkeit der Öffnungsklausel in Art. 37 Abs. 4 DSGVO mit § 38 BDSG-neu Gebrauch gemacht und letztlich die bisherige Regelung beibehalten:

„... benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens **zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten be- beschäftigen**. Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach **Artikel 35** der Verordnung (EU) 2016/679 unterliegen, oder verarbeiten sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungs- forschung, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen.“
- 6 Wie ist bei der Prüfung, ob ein Datenschutzbeauftragter (überhaupt) bestellt wer- den muss, nun vorzugehen? Die Prüfungsreihenfolge ist letztlich durch den Ge- setzeswortlaut vorgegeben: Zunächst sind die Bestellpflichten des Art. 37 Abs. 1 DSGVO zu prüfen. Soweit hier keine Bestellpflicht bejaht wird, ist gem. Art. 37 Abs. 4 DSGVO in Verbindung mit Vorschriften des nationalen Rechts (s.o.) zu prüfen, ob es hier Sondertatbestände gibt, die dennoch eine Bestellpflicht vorse- hen. Das nationale Recht ist hier zwar subsidiär, erfasst aber im Ergebnis einen we- sentlich größeren Kreis von Unternehmen, so dass sich diese Subsidiarität in der Praxis eher gegenteilig auswirken dürfte.
- 7 Zunächst nun zu den Vorgaben der DSGVO: Neu ist hier neben den sonstigen Vorgaben (dazu gleich mehr), dass die Bestellpflicht nicht nur den für die Verarbei- tung Verantwortlichen trifft, sondern auch den Auftragsverarbeiter. Diese Aufhe- bung der nach bisherigem deutschen Recht klaren Trennung zwischen verantwor- tlicher Stelle (und damit Adressat von Bußgeldvorschriften bei Nichtbeachtung) und Auftragsverarbeiter folgt logisch der sich durch die gesamte Grundverord- nung ziehenden Quasi-Gleichstellung von verantwortlicher Stelle und Auftrags-

verarbeiter. Auch dies ist, ebenso wie das nachfolgend erläuterte grundsätzlich neue Bestell-Kriterium, aus praktischer Sicht zu begrüßen, da mittlerweile die Auslagerung von IT-Dienstleistungen und Datenverarbeitung auf Externe einen erheblich größeren Umfang eingenommen hat, als noch vor 5 bis 10 Jahren. Die zunehmend komplexere Vernetzung nicht nur von Daten, sondern auch von Anwendungen in der Cloud wird mittelfristig ohnehin wohl dazu führen, dass ein Großteil der Unternehmen keine bzw. kaum noch eigene IT mehr vorhalten. Vor diesem Hintergrund ist eine Quasi-Gleichstellung von verantwortlicher Stelle und Auftragsverarbeiter im Hinblick auf die Bestellpflicht ohne Zweifel mehr als sinnvoll.

1.1.2. Bestellpflicht nach Art. 37 DSGVO

Anders als das bisherige Bundesdatenschutzgesetz macht Art. 37 DSGVO die Bestellpflicht nicht mehr von der Anzahl der im Unternehmen mit Datenverarbeitung beschäftigten Mitarbeiter abhängig, sondern von der Art, dem Umfang und dem Zweck der Verarbeitungsvorgänge. 8

Dieser (neue) Ansatz und die damit verbundene Abkehr vom Kriterium der Größe des Unternehmens bzw. der Anzahl der Mitarbeiter trägt der Tatsache Rechnung, dass auch zahlenmäßig kleine Unternehmen mit zeitgemäßer IT personenbezogene Daten in erheblichem Umfang verarbeiten können. Im Hinblick auf das Schutzgut des Datenschutzrechts ist dies ein sinnvoller Ansatz, da auf diese Weise die Bestellpflicht an die „Kernmaterie“ gebunden wird, nämlich die eigentlich stattfindende Datenverarbeitung. Aus praktischer Sicht jedoch wird die Beantwortung der Frage, ob Unternehmen nun zur Bestellung eines Datenschutzbeauftragten verpflichtet sind, gegenüber der bisherigen deutschen Rechtslage erheblich erschwert – was letztlich an den unklaren Formulierungen des Gesetzestextes liegt. Zu den Voraussetzungen der Reihe nach: 9

Bestellpflicht für Behörden und öffentliche Stellen

Art. 37 Abs. 1 DSGVO postuliert eine Bestellpflicht für Behörden und öffentliche Stellen mit Ausnahme von Gerichten, die in ihrer gerichtlichen Tätigkeit handeln. Diese Regelung behält im Wesentlichen die bisherige nationale Regelung des § 4f Abs. 1 BDSG-alt bei – allerdings mit dem Unterschied, dass das Kriterium „automatisierte Datenverarbeitung“ nun nicht mehr fallspezifisch gilt (wie bisher im BDSG), sondern grundsätzlich vor die Klammer gezogen wurde und in Art. 2 Abs. 1 DSGVO (u.a.) Grundvoraussetzung des sachlichen Anwendungsbereiches der Verordnung überhaupt ist. 10

Ähnlich bisheriger – vor allem landesrechtlicher – Regelungen können Behörden oder öffentliche Stellen auch gemeinsam einen Datenschutzbeauftragten bestellen, wenn dies im Rahmen ihrer Organisation und Größe möglich und praktikabel ist (Abs. 3). 11

Die Bestellpflicht für Behörden und öffentliche Stellen gilt – und dies hat durchaus Konsequenzen für bisher bestehende Sonderregelungen einzelner Bundesländer – 12

sowohl für Bundesbehörden und öffentliche Stellen des Bundes, aber auch für die der Länder. Und damit tritt für einige Bundesländer im Hinblick auf die Bestellpflicht eine Neuerung ein.

- 13 Bisher sahen die Landesdatenschutzgesetze eine uneinheitliche Regelung vor, wenn es darum ging, ob Datenschutzbeauftragte für öffentliche Stellen der Länder auch extern, d.h. auf Grundlage eines Dienstleistungsvertrages bestellt werden durften. So sahen noch Landesdatenschutzgesetze in Bayern, Nordrhein-Westfalen und anderen Bundesländern vor, dass öffentliche Stellen, auch wenn sie mit anderen privaten Stellen im Wettbewerb stehen, nur Beschäftigte (der jeweiligen Stelle) zum Datenschutzbeauftragten bestellen können. Art. 37 Abs. 6 DSGVO stellt es den betroffenen verantwortlichen Stellen nun jedoch frei, ob Beschäftigte oder Externe auf der Grundlage eines Dienstleistungsvertrages die Aufgaben des Datenschutzbeauftragten erfüllen. Diese Freiheit umfasst mangels anderweitiger Einschränkung auch den vorstehenden Abs. 1 lit. a des Art. 37, wonach Behörden oder öffentliche Stellen in jedem Fall einen Datenschutzbeauftragten bestellen müssen. Anderweitige Regelungen in den o.g. Landesdatenschutzgesetzen werden danach von dieser europäischen Regelung überstimmt mit dem Ergebnis, dass unabhängig von der Eigenschaft als öffentlicher oder privater Stelle grundsätzlich auch Externe die Aufgaben des Datenschutzbeauftragten wahrnehmen können.

Bestellpflicht aufgrund Art, Umfang und Zweck der Verarbeitungsvorgänge

- 14 So weit, so (zumindest partiell) bekannt. Neu, und zwar in jeder Hinsicht, ist nun die Regelung, dass ein Datenschutzbeauftragter gemäß Art. 37 Abs. 1 lit. b zu bestellen ist, wenn
- „die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Beobachtung von Personen erforderlich machen.“
- 15 Der Verordnungsgeber hat den Anwendern zwar in über 130 Erwägungsgründen Auslegungshilfen für einen Großteil der Vorschriften mit auf den Weg gegeben, für diese neue Klausel (nachfolgend zwecks einfacherer Zitierweise nur „Personen-Beobachtung“ genannt) hingegen fehlt (fast) jegliche Art von Information, welche Anwendungsfälle hiervon eigentlich umfasst sein sollen. Lediglich der Begriff Kerntätigkeit wird in Erwägungsgrund 97 dahingehend umschrieben, dass es sich bei der fraglichen Datenverarbeitung um die Haupttätigkeit der verantwortlichen Stelle handeln muss, nicht um eine Nebentätigkeit.
- 16 Es verbleiben damit im Ergebnis die klassischen juristischen Auslegungsmöglichkeiten, mit denen nachfolgend, soweit anwendbar, versucht wird, die Anwendungsfälle einzugrenzen.
- 17 In systematischer und auch teleologischer Hinsicht, also mit Blick auf den Regelungszusammenhang und den Sinn und Zweck der Regelung, soll die „Personen-Beobachtung“ eine Art hochriskante (Ausnahme-)Verarbeitung darstellen, deren Risiken sich nicht mehr mit der Datenschutz-Folgenabschätzung (Art. 35) und

einer ggf. hierzu ergänzend herangezogenen vorherigen Konsultation der Aufsichtsbehörde (Art. 33) beherrschen lassen. Dies ist insoweit nachvollziehbar, als die Datenschutz-Folgenabschätzung eine eher schlaglichtartige (Einmal-)Bewertung darstellt, die Kontrolle eines Datenschutzbeauftragten aber eine kontinuierliche ist – und diese Kontroll-Kontinuität bei der regelmäßigen Beobachtung von Personen sinnvoll und erforderlich ist. Voraussetzung ist also, dass die fragliche Verarbeitung mindestens den Risikograd des Art. 35 aufweist, also aufgrund der Art, des Umfangs und der Umstände ein hohes Risiko für die persönlichen Rechte und Freiheiten beinhaltet – und zusätzlich regelmäßig und systematisch stattfindet. Wenn man nun ergänzend die grammatische Auslegung hinzuzieht, verbleibt die Frage, welche das Kerngeschäft des Unternehmens bildende Tätigkeit die umfangreiche, regelmäßige und systematische Beobachtung von Personen erfordert.

Ohne gedankliche Klimmzüge kann man hierunter **Auskunfteien** subsumieren, jedenfalls diejenigen, die Verbraucherbewertungen vornehmen: Unternehmen, die geschäftsmäßig (vermögens- oder verhältnisrelevante) personenbezogene Daten zum Zweck der Übermittlung erheben, speichern oder verändern, erfordern genau diese Art der Datenverarbeitung: Eine umfangreiche, regelmäßige und systematische Beobachtung von Personen. Vom Wortsinn her kann dies (aufgrund der fraglos ungewöhnlichen Formulierung „Beobachtung von Personen“) zwar in ähnlicher Weise partiell auch für **Detekteien** gelten – allerdings bedarf es hier aufgrund der verschiedenen Tätigkeitsfelder dieser Branche einer genauen Analyse, ob solche Beobachtungen auch die „Kerntätigkeit“ bilden und tatsächlich auch systematisch und regelmäßig stattfinden bzw. den erforderlichen Umfang einnehmen. 18

Im Übrigen darf der Anwendungsbereich der Bestellpflicht nicht zu eng auf Unternehmen beschränkt werden, die nach allgemeinem Verständnis der Kategorie Auskunfteien unterfallen – auch ohne Auskunftei zu sein, können ähnliche Dienstleistungen erbracht werden, die eine regelmäßige und systematische Personen-Beobachtung zum Geschäftszweck haben. 19

Soweit **Warndienste**, also geschäftsmäßig organisierte Datenbank-Betreiber, die Kunden gegen Gebühr bestimmte selektive Informationen von Betroffenen bereitstellen (z.B. sog. Mieterwarndienste) ähnliche Tätigkeiten wie Auskunfteien wahrnehmen, können diese bei Vorliegen der sonstigen quantitativen Voraussetzungen ebenfalls dem Tatbestand unterfallen. 20

Erfasst werden dürften von der neuen Regelung auch ähnliche Dienstleister, wie z.B. Betreiber von **Bewertungsportalen** im Internet, wenn mit diesen Personen (z.B. Ärzte, Lehrer) bewertet werden. Geschäftszweck solcher Portale ist es, ein Interesse der Nutzer an den Bewertungen von Personen zu erzeugen und damit hohe Zugriffszahlen auf die entsprechenden Seiten zu generieren, um dann über Werbeanzeigen bzw. deren -erlöse Umsatz zu erzeugen. 21

Auch **soziale Netzwerke** dürften den Tatbestand ausfüllen: Der Geschäftszweck dieser Anbieter besteht, ähnlich (aber in größerem Stil als Bewertungsportale) darin, Nutzer und deren von sich aus übermittelte bzw. dort veröffentlichte Daten möglichst umfassend zu beobachten, um dann Werbekunden passgenaue – in der 22

Regel pseudonyme – Profile bzw. Profilgruppen als werberelevante Zielgruppe zu verkaufen. Dass der Werbetreibende hier seine potenziellen Kunden zunächst nicht identifizieren, sondern nur seine Zielgruppe über Merkmale (z.B. weiblich, unter 40 Jahre alt, Single, Mutter etc.) bestimmen kann, ändert nichts daran, dass der Betreiber der Plattform sämtliche Daten personenbezogen verarbeitet und die Personen so auch, im Wortsinne des Tatbestands, systematisch und regelmäßig beobachtet.

- 23 Die vorgenannte Aufzählung soll und kann in keiner Weise abschließend sein. Die genannten Beispiele sollen daher eher nur die Richtung vorgeben, in die eine Interpretation dieser speziellen Bestellpflicht tendieren kann. Wie so oft, bleibt es der Prüfung dem konkreten Einzelfall überlassen, ob eine Bestellpflicht vorliegt – und später der Auslegung der Aufsichtsbehörden (und Gerichte).

Bestellpflicht wegen der Verarbeitung besonders sensibler Daten

- 24 Soweit die vorhergehende Voraussetzung hinsichtlich der Bestimmung ihrer Kriterien in der Praxis vermutlich erhebliche Schwierigkeiten bereiten dürfte, sollte die Voraussetzung des Art. 37 Abs. 1 lit. c weniger Probleme aufwerfen. Hiernach ist ein Datenschutzbeauftragter zu bestellen, wenn

„die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gem. Art. 9 oder von Daten über strafrechtliche Verurteilungen und Straftaten gem. Art. 10 besteht.“

- 25 Praktikern, die bisher mit dem BDSG gearbeitet haben, kommt diese (Art der) Regelung fraglos vertraut vor – denn der Gesetzgeber verweist die Anwender hier nicht nur auf eigene Definitionen – hier in Art. 9 und 10 mit den entsprechenden Definitionen in Art. 4, sondern regelt die Bestellungs voraussetzung auch deutlich konkreter und somit praxisnäher als in Art. 37 Abs. 1 lit. b.
- 26 Art. 9 der DSGVO sieht die Verarbeitung der besonders sensiblen Daten nur im Rahmen eines – quasi geschachtelten – Verbots mit Erlaubnisvorbehalt vor. Bereits aus dieser Gesetzessystematik, die die Verarbeitung dieser Daten nur in sehr eng begrenzten Ausnahmefällen überhaupt zulässt, ist zu entnehmen, dass diese Verarbeitung zwangsläufig von einem Datenschutzbeauftragten begleitet werden muss. Allerdings gilt die Voraussetzung nicht per se, wenn besondere Kategorien von Daten verarbeitet werden, sondern nur, wenn diese Verarbeitung umfangreich erfolgt. Aufgrund des Regelungszusammenhangs darf davon ausgegangen werden, dass der Gesetzgeber diesem Kriterium dasselbe Verständnis zugrunde legen wollte wie im Abschnitt zuvor bei der Bestimmung der „umfangreichen Beobachtung (...) von Personen“. Insoweit kann zur Vermeidung von Wiederholungen hierzu auf die obigen Ausführungen² verwiesen werden.
- 27 Um das Kriterium zu erfüllen, muss der für die Verarbeitung Verantwortliche die Verarbeitung dieser Daten als Kerntätigkeit vornehmen. Auch diese Anforderung

² Vgl. oben Rn. 17 ff.

wurde bereits zuvor im Kontext von Art. 35 Abs. 1 lit. b erläutert³. Beispiele hierfür sind Medizinische (Gen-)Datenbanken, die von privaten Unternehmen (mit) betrieben werden, Parteien, Gewerkschaften, Softwareunternehmen, die biometrische Daten zur Authentisierung verwenden (soweit sie tatsächlich Zugriff auf diese Daten haben), Krankenhäuser in privater Trägerschaft, Arztpraxen.

Aufgrund der sehr speziellen Art von Daten über strafrechtliche Verurteilungen und Straftaten gem. Art. 10 und auch aufgrund der Tatsache, dass diese Daten im Wesentlichen von Behörden und Gerichten verarbeitet wird, wird diese Fallgruppe wenig praxisrelevant sein. Vorstellbare Adressaten sind hier z.B. Dienstleister, die für Behörden entsprechende Daten im Auftrag verarbeiten oder private Vereinigungen von Opfern von Straftaten. 28

1.1.3. Gemeinsame Bestellung eines Datenschutzbeauftragten durch eine Unternehmensgruppe

Ein weiterer Baustein im neuen, kleinen Konzernprivileg der DSGVO⁴ bildet Art. 37 Abs. 2: Hiernach ist es Konzernen nunmehr erlaubt, einen Datenschutzbeauftragten für die gesamte Unternehmensgruppe zu bestellen, wenn dieser von jeder Niederlassung aus leicht erreicht werden kann. Diese Regelung, ebenso wie ein wirkliches Konzernprivileg, war auch vor dem Hintergrund einer etwaigen neuen nationalen Regelung überfällig. Dass es für die Bestellung des Datenschutzbeauftragten in einem Unternehmensgeflecht jeweils auf die einzelne juristische Person ankam, war zwar gesetzestheoretisch logisch, in der Praxis aber nur schwer vermittelbar bzw. hat letztlich unnötigen Papieraufwand verursacht, wenn für jedes Konzernunternehmen eine Bestellsurkunde auszufertigen war. 29

Die neue Regelung hat Vor- und Nachteile. Vorteile bestehen fraglos darin, dass die Neigung von Konzernen, einen Datenschutzbeauftragten einheitlich zu bestellen, sicherlich größer sein dürfte, als wenn dies für diverse Unternehmen separat erfolgen müsste. Damit einhergehend können, wenn sich das Know-how über Unternehmensprozesse und deren datenschutzrechtliche Bewertung in einer Person konzentriert, durchaus Synergieeffekte einstellen. Allerdings muss hierbei berücksichtigt werden, dass die Vorschrift nur die Bestellung eines Datenschutzbeauftragten ermöglicht – was nicht damit gleichzusetzen ist, dass die Datenschutzbelange einer Unternehmensgruppe nur durch einen Datenschutzbeauftragten wahrgenommen werden können. Gerade in multinationalen Konzernen ist vielmehr die Einrichtung einer Datenschutzorganisation gefragt, denen zwar ein Datenschutzbeauftragter als Leitung vorsteht, die aber vom Umfang her je nach Aufgabenspektrum die Größe einer internen Organisationseinheit mit z.T. sogar mehreren Hierarchien einnehmen kann. 30

³ Vgl. oben Rn. 15.

⁴ Vgl. hierzu auch Kapitel B 9.

Unternehmensgruppe

- 31 Unternehmensgruppe wird in Art. 4 Nr. 19 legal definiert, hierbei handelt es sich um eine Gruppe, die aus einem herrschenden Unternehmen und von diesen abhängigen Unternehmen besteht. Interessant ist hierbei, dass die DSGVO nicht auf den Begriff der verbundenen Unternehmen im Sinne des § 15 AktG abstellt, sondern auf den der abhängigen bzw. herrschenden Unternehmen des § 17 AktG. Warum allerdings nicht generell auf verbundene Unternehmen abgestellt wird, lässt sich auch aus dem betreffenden Erwägungsgrund 28 nicht herleiten⁵.

Sofern von jeder Niederlassung aus ... leicht erreicht werden kann.

- 32 Die Anforderung soll lediglich sicherstellen, dass der Datenschutzbeauftragte die bei Unternehmensgruppen im Zweifel häufig fehlende Lokalität durch eine Erreichbarkeit per E-Mail oder Telefon sicherstellen kann. Das Gesetz spricht dabei bewusst nicht von „leicht verfügbar“ im Sinne eines vor-Ort-Seins, sondern nur von „erreichbar“. Dieses Kriterium dürfte allerdings in Zeiten einer täglich wachsenden Vernetzung kein besonderes Gewicht haben.

Formvorschriften

- 33 Wie sieht eine Bestellung eines Datenschutzbeauftragten in der Praxis aus? Hierfür sah weder das vorherige BDSG noch sieht die jetzige DSGVO (bzw. das BDSG-neu) eine besondere Förmlichkeit vor⁶. Voraussetzung für eine (insbesondere auch arbeitsrechtlich) wirksame und nachweisbare Bestellung ist, dass diese schriftlich erfolgt und der bzw. die bestellte Person namentlich benannt, so dass eine Verwechselung ausgeschlossen ist. Auf Seiten des bzw. der Unternehmen sollte jedes Unternehmen vollständig im Rubrum bezeichnet werden, für das der Datenschutzbeauftragte bestellt wird.
- 34 Weiterhin muss das Datum, ab dem die Bestellung wirksam sein soll, angegeben werden. In der Regel wird hier kein Ende-Datum angegeben, denn die Bestellung erfolgt in der Regel unbefristet. Interessant ist in diesem Zusammenhang, dass die DSGVO keinerlei Regelungen zur Abberufung trifft – außer der, dass der Datenschutzbeauftragte wegen seiner Aufgabenwahrnehmung nicht abberufen oder benachteiligt werden kann, (Art. 38 Abs. 3 S. 2, vgl. hierzu Kapitel B 1.7). Nicht ausgeschlossen ist allerdings, dass dies in besonderen Fällen – z.B. um eine festgelegte Übergangszeit zu überbrücken – dennoch geschieht. Falls dies der Fall sein sollte, bedarf es dann nach Ablauf des benannten Zeitraums keiner Abberufung.

5 Hier heißt es lediglich, dass „das herrschende Unternehmen dasjenige sein sollte, dass zum Beispiel aufgrund der Eigentumsverhältnisse, der finanziellen Beteiligung oder der für das Unternehmen geltenden Vorschriften oder der Befugnis, Datenschutzvorschriften umsetzen zu lassen, einen beherrschenden Einfluss auf die übrigen Unternehmen ausüben kann“.

6 Für interne Datenschutzbeauftragte können in einer analogen Anwendung von § 2 NachwG („Gesetz über den Nachweis der für ein Arbeitsverhältnis geltenden wesentlichen Bedingungen“ vom 20.07.1995, BGBl. S. 946) zumindest einige schriftlich zu regelnde Punkte bestimmt werden.

Schließlich, wenig überraschend, muss das Dokument das Datum der Zeichnung sowie die Unterschriften des bzw. der Datenschutzbeauftragten sowie des Vertretungsberechtigten des betreffenden Unternehmens beinhalten. Für eine Unternehmensgruppe muss hier der Vertretungsberechtigte zeichnen, dessen Vertretungsbefugnis diejenigen der anderen Unternehmen aufgrund der Beteiligungs- bzw. Beherrschungsstruktur umfasst. 35

1.1.4. Die Bestellpflicht nach nationalem Recht – § 38 BDSG-neu

Soweit also nach den vorstehenden Regelungen auf jeden Fall ein Datenschutzbeauftragter zu bestellen ist, stellt Abs. 4 klar, dass in anderen als in den benannten Fällen Verantwortliche, Auftragsverarbeiter oder auch Verbände und Vereinigungen einen Datenschutzbeauftragten bestellen können (wer sollte sie daran hindern?). Welchen Regelungsgehalt dieser Satzteil haben soll, bleibt allerdings unklar und hätte nur in dem Fall einen eigenen Aussagegehalt, wenn in bestimmten, gesetzlich bezeichneten Fällen ein Datenschutzbeauftragter tatsächlich nicht benannt werden dürfte. Da dies aber nicht der Fall ist, bleibt nur der zweite Teil des Absatzes relevant, nachdem auch dann ein Datenschutzbeauftragter bestellt werden muss, wenn zwar die Voraussetzungen der DSGVO nicht vorliegen, dafür aber der betreffende Mitgliedsstaat eine Bestellpflicht vorsieht. Der deutsche Gesetzgeber hat, wie anfangs bereits kurz erwähnt, hiervon Gebrauch gemacht und mit § 38 BDSG-neu die bisherigen Regelungen zur Bestellung eines Datenschutzbeauftragten nahezu wortgleich beibehalten. 36

Dies bedeutet in der Praxis, dass für die Frage nach der Bestellpflicht entgegen der gesetzlichen Normenhierarchie zunächst der Blick in § 38 BDSG-neu erforderlich ist. Liegen die dortigen Voraussetzungen vor, 37

- in der Regel ständig mindestens 10 Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt oder
- der Betrieb von Verarbeitungen, die einer Datenschutzfolgenabschätzung unterliegen, oder
- geschäftsmäßige Verarbeitung zum Zweck der Übermittlung, oder
- Verarbeitung zum Zweck der Markt- und Meinungsforschung

ist auch dann ein Datenschutzbeauftragter zu bestellen, wenn die Anforderungen des Art. 37 DSGVO nicht erfüllt sind⁷.

1.2. Mitteilungspflicht gegenüber der Aufsichtsbehörde

Neu und bisher ohne nationales Vorbild ist nun die Mitteilungspflicht des Art. 37 Abs. 7 DSGVO. Danach müssen die Kontaktdaten des Datenschutzbeauftragten veröffentlicht und auch der Aufsichtsbehörde gemeldet werden. Zur Umsetzung der Veröffentlichungspflicht bieten sich natürlich die entsprechenden Webseiten 38

⁷ Zu den Bestellpflichten z.B. Simitis, in Simitis, Bundesdatenschutzgesetz, 8. Auflage 2014, § 4f Rn. 12ff.; Scheja, in: Taeger/Gabel, Bundesdatenschutzgesetz, 2. Auflage 2013, § 4f Rn. 18; Gola/Schomerus, Bundesdatenschutzgesetz, 12. Auflage 2015, § 4f Rn. 7.

▼ Ab dem 25. Mai 2018 finden die Regelungen der Datenschutz-Grundverordnung (DSGVO) und des neuen BDSG Anwendung. Unternehmen sind dann zum Beispiel verpflichtet, transparent und ausführlich zu beschreiben, welche Daten sie für welche Zwecke verarbeiten und wie lange die Daten gespeichert werden. Anders als heute können Verstöße mit empfindlichen Bußgeldern geahndet werden. Dieser Aspekt führt in der Praxis dazu, dass sich viele Unternehmen – zum Teil erstmalig – intensiv mit den datenschutzrechtlichen Vorschriften und ihrer Umsetzung im Unternehmen befassen.

Dieses Handbuch hilft Ihnen bei der Umsetzung der mitunter komplizierten Regelungen der DSGVO und des neuen BDSG. Es zeigt Ihnen praxisorientierte Lösungen für Fragen auf, die sich in den Unternehmen stellen. Weiterhin wird der Themenbereich der Informationssicherheit ausführlich behandelt, der in der Praxis stets zusammen mit dem Datenschutz gedacht werden sollte.

Sämtliche Autoren dieses Handbuchs sind erfahrene Beraterinnen und Berater, die seit Jahren in den Bereichen Datenschutz und Informationssicherheit tätig sind. In diesem Handbuch stellen sie Best Practice-Ansätze vor, wie den neuen gesetzlichen Vorgaben am besten entsprochen werden kann.

Leseprobe, mehr zum Werk unter www.ESV.info/17727



www.ESV.info