



# **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 Schirrmacher, Dr. Uwe Schläger, Felix Schmidt, Markus  
Schönmann, Stefan R. Seiter, Daniel Stolper, Oliver Stutz,  
Jan-Christoph Thode, Sven Venzke-Caprarese,  
Ralf von Rahden

**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](http://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

## **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 verbunden 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 Beschäftigertaten 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 unternehmenseigenen Intranets. Kapitel F stellt dar, in welchem Umfang Videosysteme nach der neuen Datenschutz-Grundverordnung betrieben werden können.

Der zweite Hauptteil des Handbuchs beginnt in Kapitel G mit einer Darstellung der rechtlichen Grundlagen der IT-Sicherheit. In Kapitel H werden die Eckpfeiler eines Informations sicherheits-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 an gemessenen 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.
<b>Teil A</b>		
<b>Datenschutzrechtliche Grundlagen .....</b>	1	
<b>1. Geschichte des Datenschutzrechts .....</b>	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 informationelle 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 – Datenschutzgesetze 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
<b>2. Datenschutzrecht in Deutschland und in der EU .....</b>	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.	Lösichung . . . . .	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
<b>Teil B</b>			
<b>Datenschutzmanagement im Unternehmen .....</b>		91	
1.	<b>Der betriebliche Datenschutzbeauftragte .....</b>	93	1
1.1.	Bestellpflicht .....	93	3
1.1.1.	Europarechtliche Regelung mit nationaler Öffnungsklausel .....	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 Datenschutzbeauftragten durch eine Unternehmensgruppe .....	99	29
	Unternehmensgruppe .....	100	31
	Sofern von jeder Niederlassung aus leicht erreicht 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 Informationspflichten . . . . .	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.	<b>Verzeichnis von Verarbeitungstätigkeiten</b> . . . . .	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.	<b>Datenschutz-Folgenabschätzung</b> . . . . .	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.	<b>Verpflichtung auf das Datengeheimnis</b> . . . . .	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.	<b>Meldepflicht bei Datenpannen</b> . . . . .	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.	<b>Outsourcing</b> . . . . .	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 Auftragsverarbeitung . . . . .	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
<b>7.</b>	<b>Kontrolle des Datenschutzes . . . . .</b>	<b>143</b>	<b>175</b>
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
<b>8.</b>	<b>Datenlöschung . . . . .</b>	<b>146</b>	<b>186</b>
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
<b>9.</b>	<b>Datenweitergabe im Konzern . . . . .</b>	<b>150</b>	<b>198</b>
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**

	<b>Verarbeitung von Beschäftigtendaten . . . . .</b>	<b>163</b>	
<b>1.</b>	<b>Regelungen zum Beschäftigtendatenschutz . . . . .</b>	<b>165</b>	<b>1</b>
1.1.	Öffnungsklausel . . . . .	165	4
1.2.	Regelungen im BDSG-neu . . . . .	166	7
1.3.	Betriebsvereinbarungen . . . . .	167	17
<b>2.</b>	<b>Bewerbermanagement . . . . .</b>	<b>169</b>	<b>20</b>
2.1.	Zulässigkeit der Verarbeitung im Bewerbungsverfahren . . .	169	22
2.1.1.	Fragerrecht 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.	<b>Personalakten</b> . . . . .	176	58
3.1.	Inhalte . . . . .	176	61
3.2.	Zugriffsrechte . . . . .	177	67
3.3.	Aufbewahrungsduer . . . . .	178	69
3.4.	Rechte des Mitarbeiters . . . . .	179	78
3.5.	Best Practice . . . . .	180	83
4.	<b>Zeiterfassung</b> . . . . .	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.	<b>Personalentwicklung</b> . . . . .	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

---

5.7.	Outplacement .....	198	179
5.7.1.	Durchführung auf Grundlage einer Einwilligung .....	199	180
5.7.2.	Outsourcing als Funktionsübertragung .....	199	182
<b>6.</b>	<b>Nutzung von Internet, E-Mail und Telefon .....</b>	<b>200</b>	<b>183</b>
6.1.	Internet- und E-Mail-Nutzung .....	200	184
6.1.1.	Wahrung des Fernmeldegeheimnisses .....	200	185
6.1.2.	Erlaubnis der privaten Nutzung .....	201	191
6.1.3.	Verbot der privaten Nutzung .....	202	193
6.1.4.	Nicht-Regelung und Duldung der privaten Nutzung .....	204	203
6.1.5.	Notwendigkeit unternehmensinterner Regelungen .....	204	207
6.2.	Telefonie .....	208	220
6.2.1.	Verarbeitung von Verkehrsdaten .....	208	221
	Erlaubnis der privaten Nutzung .....	208	222
	Verbot der privaten Nutzung .....	209	225
	Notwendigkeit unternehmensinterner Regelungen .....	209	229
6.2.2.	Aufzeichnung von Inhaltsdaten .....	210	231
<b>7.</b>	<b>Ortung von Mitarbeitern .....</b>	<b>213</b>	<b>239</b>
7.1.	Ortung von Mobiltelefonen/GPS-Ortung .....	213	240
7.2.	Betriebsvereinbarung/Einwilligung .....	213	243
7.3.	Gesetzliche Grenzen .....	214	246
7.4.	Transparenzpflichten .....	216	253
7.5.	Aufdeckung von Straftaten .....	216	255
7.6.	Sonstige Anforderungen .....	216	256
<b>8.</b>	<b>Auskunftsersuchen von Behörden und sonstigen Dritten .....</b>	<b>218</b>	<b>257</b>
8.1.	Spezialgesetzliche Normen .....	218	258
8.2.	Einwilligung .....	218	260
8.3.	Berechtigtes Interesse an einer Datenherausgabe .....	218	261
8.4.	Rahmenbedingungen und Umfang einer Datenherausgabe .....	219	262
<b>9.</b>	<b>Compliance-Maßnahmen .....</b>	<b>221</b>	<b>267</b>
9.1.	Der Begriff Compliance .....	222	270
9.1.1.	Abgrenzung zu Revisionsmaßnahmen .....	223	280
9.1.2.	Compliance „Kerndisziplinen“ .....	224	285
9.1.3.	Rechtsgrundlagen für Compliance-Prüfungen .....	225	290
9.2.	Konfliktpotential zum Datenschutz .....	225	292
9.3.	Datenschutzrechtliche Erlaubnisnormen .....	226	296
9.3.1.	Entstehung einer speziellen Norm zum Beschäftigtendatenschutz .....	227	300
	Projekt „Babylon“ der Deutschen Bahn .....	227	301
	Der Lidl-„Skandal“ .....	228	302
	BDSG-Novelle 2009 .....	228	304
9.3.2.	Verarbeitung von Beschäftigtendaten bei Compliance-Prüfungen .....	229	306
9.4.	Best Practise .....	230	312
9.4.1.	E-Mail-Screening .....	230	312

9.4.2.	Whistleblowing/Hinweisgebersysteme . . . . .	231	317
	Vorgaben der Aufsichtsbehörden (Art. 29-Datenschutzgruppe und Düsseldorfer Kreis) . . . . .	233	325
	Erheblichkeit des Vorwurfs . . . . .	234	327
	Keine anonymen Hinweise . . . . .	234	330
	Schutz der Identität des Hinweisgebers . . . . .	235	331
	Dokumentationspflichten . . . . .	235	332
	Informationspflichten . . . . .	235	333
	Löschaftspflichten . . . . .	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
<b>10. Verarbeitung von Gesundheitsdaten</b>	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
<b>11. Betriebsrat und Datenschutz</b>	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
<b>Teil D</b>		
<b>Verarbeitung von Kundendaten .....</b>	<b>271</b>	
<b>1. CRM-Systeme .....</b>	<b>273</b>	<b>1</b>
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
<b>2. Marketing und Werbung .....</b>	<b>283</b>	<b>36</b>
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
<b>3. Kundenbindungssysteme .....</b>	<b>302</b>	<b>134</b>
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 Programmdaten .....	306	159
3.3. Datenverarbeitung für Werbung und Marktforschung .....	306	162
3.3.1. Verarbeitung von Stamm- und Programmdaten ..	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
<b>4.</b>	<b>Unternehmenskauf . . . . .</b>	<b>314</b>	<b>197</b>
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
<b>5.</b>	<b>Bonitätsmanagement (einschl. Scoring) . . . . .</b>	<b>320</b>	<b>215</b>
5.1.	Beteiligte des Bonitätsmanagements . . . . .	321	221
5.2.	Datenübermittlung an eine Auskunftei . . . . .	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 Auskunfeitfähigkeit .	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**

	<b>Datenverarbeitung im Internet und Intranet . . . . .</b>	<b>351</b>	
<b>1.</b>	<b>Webseiten . . . . .</b>	<b>353</b>	<b>1</b>
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 Unter- nehmen. . . . .	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
<b>2.</b>	<b>Soziale Netzwerke .....</b>	<b>390</b>	<b>164</b>
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.	Freundefinder .....	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.	<b>Intranet-Portale.....</b>	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 Beispiel 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

	<b>Videoüberwachung im Unternehmen .....</b>	443	
1.	<b>Personenbeziehbarkeit und Verarbeitung von Bilddaten.....</b>	445	1
2.	<b>Rechtliche Grundlagen für Unternehmen .....</b>	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.	Videoüberwachung von Kindern.....	460	53
2.7.	Verdeckte Videoüberwachung .....	461	57
<b>3.</b>	<b>Sicherheitsmaßnahmen für Videosysteme.....</b>	<b>463</b>	<b>59</b>
3.1.	Hinweisschilder .....	463	60
3.2.	Lösung der Bilddaten .....	465	67
3.3.	Sonstige technische und organisatorische Pflichten .....	466	72
<b>4.</b>	<b>Beispiele aus der Praxis .....</b>	<b>468</b>	<b>74</b>
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

	<b>Rechtliche Grundlagen der Informationssicherheit .....</b>	<b>475</b>	
<b>1.</b>	<b>Datenschutzgrundverordnung .....</b>	<b>477</b>	<b>1</b>
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 Verarbeitung .....	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
<b>2.</b>	<b>IT-Sicherheitsgesetz, europäische NIS-Richtlinie .....</b>	<b>494</b>	<b>70</b>
2.1.	Betreiber kritischer Infrastrukturen .....	494	72

2.2.	Betreiber von Webseiten .....	496	80
2.3.	Anbieter digitaler Dienste .....	497	84
<b>3.</b>	<b>Bereichsspezifische Normen .....</b>	<b>498</b>	<b>88</b>
3.1.	Energiewirtschafts- und Messstellenbetriebsgesetz .....	498	89
3.2.	Kreditwesengesetz .....	498	92
3.3.	Glückspielstaatsvertrag .....	500	95
<b>Teil H</b>			
<b>IT-Sicherheitsmanagement im Unternehmen .....</b> 501			
<b>1.</b>	<b>Vorgehensweise .....</b>	<b>503</b>	<b>1</b>
<b>2.</b>	<b>Merkmale eines ISMS .....</b>	<b>505</b>	<b>10</b>
2.1.	Management-Prinzipien .....	505	14
2.2.	Ressourcen .....	507	15
2.3.	Mitarbeiter .....	507	19
2.4.	Strategie .....	507	20
<b>3.</b>	<b>ISO/IEC 27001 und IT-Grundschutz .....</b> 510	<b>26</b>	
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 Telekommunikationsunternehmen .....	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.	Schutzbedarfseinstellung .....	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
<b>4.</b>	<b>Bedeutung von Zertifikaten .....</b> 520	<b>70</b>	
<b>Teil I</b>			
<b>Technische und organisatorische Maßnahmen .....</b> 523			
<b>1.</b>	<b>Übergreifende Aspekte .....</b>	<b>525</b>	<b>1</b>
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
	Lösichung 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-Diensteanbieters . . . . .	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
<b>2.</b>	<b>Infrastruktur . . . . .</b>	<b>563</b>	<b>187</b>
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
<b>3.</b>	<b>IT-Systeme . . . . .</b>	<b>569</b>	<b>213</b>
3.1.	Serversysteme . . . . .	569	214
3.1.1.	Allgemeine Maßnahmen zur Serverhärtung . . . . .	569	215
3.1.2.	Serverspezifische Härtungsmaßnahmen . . . . .	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
<b>4.</b>	<b>Netze . . . . .</b>	<b>578</b>	<b>236</b>
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-End . . . . .	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
<b>5. Anwendungen . . . . .</b>	<b>590</b>	<b>284</b>
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

<b>Penetrationstest . . . . .</b>	<b>599</b>	
<b>1. Vorgehensweise . . . . .</b>	<b>601</b>	<b>1</b>
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
<b>2. Testszenarien . . . . .</b>	<b>605</b>	<b>19</b>
2.1. Black-Box. . . . .	605	20
2.2. White-Box . . . . .	605	21
2.3. Grey-Box . . . . .	605	22
<b>3. Testmodule und Prüfthemen . . . . .</b>	<b>607</b>	<b>23</b>
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 Authenti- sierung .....	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