

Inhaltsverzeichnis

	Seite
Vorwort	V
Literaturverzeichnis	XIII

	Rz.	Seite
Einleitung		
I. Einführung	1	1
II. Checkliste der wichtigsten IT-sicherheitsrechtlichen Pflichten	4	2
A. IT-Sicherheit im Unternehmen		
I. Vorbemerkung	9	5
II. Bedeutung für Unternehmen	10	5
1. IT als Risikofaktor	12	5
a) Interne und externe Risiken	14	6
b) Risikoanalyse	18	7
c) Typische Sicherheitsversäumnisse	21	9
2. IT-Compliance	22	9
3. Nachteile durch Sicherheitsdefizite	27	10
III. IT-Sicherheitspflichten der Geschäftsleitung	32	12
1. Grundlagen der Verantwortlichkeit von Vorstand bzw. Geschäftsführung	34	12
a) Besonderheiten der Aktiengesellschaft	36	13
b) Ressortverantwortlichkeit für IT-Sicherheit	37	13
2. Pflicht zur Früherkennung bestandsgefährdender Risiken	40	14
a) Geeignete Maßnahmen zur Früherkennung	41	14
b) Implementierung eines Früherkennungs- und Überwachungssystems	44	16
c) ... als Bestandteil eines allgemeinen Risikomanagementsystems . . .	47	17
3. Weitere Compliance-Pflichten	50	17
a) Compliance-Pflichten mit IT-Sicherheitsbezug	51	18
b) Umsetzung durch die Geschäftsleitung	52	18
4. Umfang der Geschäftsleitungspflichten	54	19
a) Anzuwendender Sorgfaltsmaßstab	55	20
b) Ermessensspielraum: Business Judgement Rule	58	21
IV. Pflicht zur Buchführung	61	23
1. Zulässiger Umfang elektronischer Buchführung	63	23
2. Sicherungspflichtige Daten und IT-Systeme	66	24
3. Anforderungen an die IT-Sicherheit der Buchführung	67	25
4. Umsetzung der Anforderungen: internes Kontrollsystem	68	26
5. Besonderheiten für an der US-Börse notierte Unternehmen	70	26
V. Rechtslage im Konzern	72	28

	Rz.	Seite
1. Konzernweite Compliance-Pflicht	73	28
2. Konzernweite Überwachungspflicht	76	29
VI. Einbeziehung des Betriebsrats	79	30
1. Mitwirkungsrechte	80	31
2. Mitbestimmungsrechte	82	31
VII. IT-Sicherheit als vertragliche Pflicht	87	33
1. IT-Sicherheit als Hauptleistungspflicht	88	33
a) Verträge mit IT-Sicherheitsbezug	89	34
b) „Sichere“ IT-Produkte	96	37
2. IT-Sicherheit als Nebenpflicht	108	42
3. Hinweise zur Vertragsgestaltung	112	43
4. Übersicht zu typischen Fallgruppen	115	44
VIII. IT-Sicherheit als wettbewerbsrechtliche Pflicht	115	46
1. IT-Sicherheit zum Schutz von Betriebsgeheimnissen	116	46
2. IT-Sicherheitsdefizite als Rechtsbruch	120	48
a) IT-sicherheitsrechtliche Vorschriften als Marktverhaltens- regelungen	122	48
b) Wettbewerbsrechtliche Verletzungsfolgen	126	50
IX. Praktische Umsetzung: IT-Sicherheitskonzept des Unternehmens	127	51
1. Benennung betrieblicher Beauftragter für IT-Sicherheit	129	51
a) Abgrenzung verschiedener betrieblicher Beauftragter	132	52
b) Stellung des IT-Sicherheitsbeauftragten	133	54
c) Haftung des IT-Sicherheitsbeauftragten	136	55
d) Aufgaben des IT-Sicherheitsbeauftragten	146	58
e) Kriterien zur Auswahl des IT-Sicherheitsbeauftragten	148	59
2. Einrichtung eines IT-Risikomanagementsystems	149	59
a) Vorteile des IT-Risikomanagementsystems	151	60
b) Struktur des IT-Risikomanagementsystems	154	61
c) Vorgehensweise bei der Schaffung des IT-Risikomanagement- systems	160	62
3. Implementierung von IT-Betriebsrichtlinien	167	64
a) Schaffung eines internen Handlungsstandards	168	64
b) Zentrale Elemente von IT-Betriebsrichtlinien	170	64
c) Praxisrelevante Problemfelder	173	66
4. Notfallkonzept und Verhalten im Falle von IT-Sicherheitsvorfällen	186	71
a) Konzeption und Inhalt	187	71
b) Verhalten bei und Bewältigung von IT-Sicherheitsvorfällen	190	72
5. Nutzung technischer Regelwerke	191	73
a) BSI-Grundschutzkatalog	192	73
b) ISO/IEC 27001	194	74
c) IT Infrastructure Library (ITIL)	196	75
B. Allgemeine Haftung für IT-Sicherheit		
I. Vorbemerkung	197	77
II. Haftungsverhältnisse im Unternehmen	198	77

	Rz.	Seite
1. Haftung der Geschäftsleitung gegenüber der Gesellschaft	199	77
a) Grundlagen der Vorstands-Haftung in der AG	200	77
b) Grundlagen der Geschäftsführer-Haftung in der GmbH	205	80
c) Praxislösung: D&O-Versicherung	207	81
d) Haftungsbeschränkung durch Zuweisung von Verantwortlichkeiten	209	81
e) Exkurs: Haftung des Aufsichtsrats der AG	215	83
2. Haftung der Geschäftsleitung gegenüber den Aktionären bzw. Gesellschaftern	217	84
III. Haftung des Unternehmens gegenüber Dritten	221	86
1. Haftung der Geschäftsleitung im Außenverhältnis	222	86
a) Geringe Praxisrelevanz: Vertragsrecht	223	86
b) Gesteigerte Praxisrelevanz: Deliktsrecht	224	87
2. Vertragliche Haftung des Unternehmens	227	88
a) Grundlagen der vertraglichen Haftung	228	88
b) Möglichkeiten des Haftungsausschlusses	240	94
3. Deliktische Haftung des Unternehmens	253	98
a) Haftung nach § 823 Abs. 1 BGB	254	98
b) Haftung nach § 823 Abs. 2 BGB wegen der Verletzung eines Schutzgesetzes	261	102
c) Haftung nach § 831 BGB für Verrichtungsgehilfen	265	104
4. Verschuldensunabhängige Produkthaftung	267	105
IV. Inanspruchnahme von Cyber-Angreifern	271	107
1. Anspruchsgrundlagen	272	107
2. Anspruchssicherung und Vorgehen im Falle von Cyber-Angriffen	274	108
V. Ordnungswidrigkeiten- und Strafrecht	277	109
1. Haftung der Geschäftsleitung	278	110
a) § 130 OWiG – Verletzung der Aufsichtspflicht im Unternehmen	279	110
b) § 266 StGB – Unternehmerische Fehlentscheidungen als Untreue?	283	112
2. Haftung des Unternehmens	286	113
3. Haftung des IT-Sicherheitsbeauftragten	288	114
C. Datenschutz und IT-Sicherheit		
I. Vorbemerkung	290	117
II. Rechtsentwicklung und Rechtsquellen	291	117
1. DSGVO und BDSG-neu	293	118
2. Bereichsspezifisches Datenschutzrecht	295	118
III. Anwendungsbereich	298	120
1. Sachlicher Anwendungsbereich	299	120
a) Personenbezogene Daten	300	120
b) Anonymisierung als Mittel zum Ausschluss der Anwendbarkeit der DSGVO	301	121
2. Persönlicher Anwendungsbereich	302	121
a) Verantwortlicher	303	121
b) Auftragsverarbeiter	305	122

	Rz.	Seite
3. Räumlicher Anwendungsbereich	306	122
a) DSGVO	307	123
b) BDSG-neu	310	124
IV. Datenschutzrechtliche IT-Sicherheitsvorgaben	312	125
1. IT-Sicherheitsstandard	313	125
a) Technische und organisatorische Maßnahmen	315	125
b) Mindestschutzanforderungen	318	128
c) Selbstregulierung und präventive Sicherheitsmaßnahmen	321	130
2. Weitere datenschutzrechtliche IT-Sicherheitsvorgaben	325	132
a) Verzeichnis von Verarbeitungstätigkeiten	326	132
b) Datenschutz-Folgenabschätzung	328	132
c) Datenschutzbeauftragter	329	133
3. Meldepflichten bei Datenschutzverletzungen	332	134
a) Meldung gegenüber der Datenschutzaufsichtsbehörde	333	134
b) Benachrichtigung der betroffenen Personen	336	136
V. Verletzungsfolgen	338	136
1. Festsetzung von Bußgeldern für Datenschutzverstöße	339	137
2. Strafrechtliche Sanktionen	340	137
3. Hinweise zur Kommunikation mit den Aufsichtsbehörden	341	138
 D. Vorgaben des IT-Sicherheitsgesetzes, des NIS-Richtlinien-		
Umsetzungsgesetzes und anderer Gesetze		
I. Vorbemerkung	342	139
II. Rechtsentwicklung und Rechtsquellen	343	139
1. Nationale Gesetzgebung: BSIG und IT-SiG	344	139
2. NIS-Richtlinie und deren Umsetzung in Deutschland	346	140
III. Grundzüge der Vorgaben aus IT-SiG und NIS-Umsetzungsg und Regelungssystematik	348	140
IV. IT-Sicherheitspflichten nach dem BSIG	351	141
1. Pflichten von KRITIS-Betreibern	352	141
a) Adressaten	353	142
b) IT-Sicherheitsstandard	362	146
c) Meldepflichten gegenüber dem BSI	370	149
d) Verletzungsfolgen nach dem BSIG	381	152
e) Zivilrechtliche Haftung	383	153
2. Pflichten der Anbieter digitaler Dienste	386	154
a) Adressaten	387	154
b) IT-Sicherheitsstandard	393	157
c) Meldepflichten	396	158
d) Verletzungsfolgen	401	159
3. „Mittelbare“ Auswirkungen des BSIG auf die Hersteller von IT-Produkten und -Systemen	403	160
a) Warnungen und Empfehlungen des BSI an die Öffentlichkeit	404	160
b) Untersuchungsrechte des BSI	406	161
c) Mitwirkungspflichten der Hersteller bei Störungen der IT-Sicherheit	408	161

	Rz.	Seite
V. IT-Sicherheitspflichten nach dem TMG	409	162
1. Adressaten	410	162
2. IT-Sicherheitsstandard	412	163
a) Pflichtenumfang	414	163
b) Abgrenzung zum BSIG	417	165
3. Verletzungsfolgen	420	166
VI. IT-Sicherheitspflichten nach dem TKG	422	167
1. Adressaten	423	167
2. IT-Sicherheitsstandard	426	168
3. Sicherheitsbeauftragter und Sicherheitskonzept	429	169
4. Meldepflichten	432	170
a) Meldepflichtige Ereignisse	433	171
b) Inhalt und Form der Meldung	435	172
c) Benachrichtigung der Öffentlichkeit	437	172
5. Datenschutzrechtliche IT-Sicherheitsvorgaben gem. § 109a TKG	438	172
a) Benachrichtigungspflichten bei Datenschutzverletzungen	439	173
b) Dokumentationspflichten bei Datenschutzverletzungen	443	174
6. Verletzungsfolgen	444	174
a) Bußgelder	445	174
b) Schadensersatz und Unterlassen	447	175
VII. IT-Sicherheitspflichten nach dem EnWG	449	176
1. Adressaten	450	176
2. IT-Sicherheitsstandard	451	176
a) Betreiber von Energieversorgungsnetzen	452	177
b) Betreiber von Energieanlagen	455	178
3. Meldepflichten	457	179
4. Verletzungsfolgen	459	179
VIII. IT-Sicherheitspflichten nach dem AtG	460	180
1. Adressaten	461	180
2. IT-Sicherheitsstandard	463	180
3. Meldepflichten	464	181
4. Verletzungsfolgen	465	181
IX. IT-Sicherheitspflichten nach dem SGB V	466	182
1. Adressaten	467	182
2. IT-Sicherheitsstandard	468	182
3. Meldepflichten	469	183
4. Verletzungsfolgen	470	183
E. Sonstige branchenspezifische Vorschriften zur IT-Sicherheit		
I. Vorbemerkung	471	185
II. IT-Sicherheit im Versicherungsbereich	472	185
1. Adressaten	473	185
2. IT-Sicherheitspflichten	474	185
3. Verletzungsfolgen	477	186
III. IT-Sicherheit im Finanz- und Bankwesen	478	187
1. Allgemeine Pflichten im Bankensektor	479	187

	Rz.	Seite
2. Besondere Pflichten von Wertpapierdienstleistungsunternehmen . . .	484	189
3. Besondere Pflichten von Börsenträgern	485	190

Seite

Anhang: Wichtigste Vorschriften zur IT-Sicherheit

I. AktG – Aktiengesetz	191
II. AtG – Atomgesetz	194
III. AO – Abgabenordnung	198
IV. BDSG-neu – Bundesdatenschutzgesetz i.d.F. ab 25.5.2018	200
V. BetrVG – Betriebsverfassungsgesetz	204
VI. BGB – Bürgerliches Gesetzbuch	206
VII. BörsG – Börsengesetz	208
VIII. BSIG – Gesetz über das Bundesamt für Sicherheit in der Informations- technik	209
IX. DSGVO – Datenschutz-Grundverordnung	215
X. EnWG – Energiewirtschaftsgesetz	228
XI. GmbHG – Gesetz betreffen die Gesellschaften mit beschränkter Haftung	231
XII. GWG – Geldwäschegesetz	232
XIII. HGB – Handelsgesetzbuch	233
XIV. KWG – Kreditwesengesetz	234
XV. OWiG – Gesetz über Ordnungswidrigkeiten	238
XVI. ProdHaftG – Produkthaftungsgesetz	240
XVII. ProdSG – Produktsicherheitsgesetz	241
XVIII. SGB V – Sozialgesetzbuch Fünftes Buch – Gesetzliche Krankenversicherung . .	242
XIX. StGB – Strafgesetzbuch	248
XX. TKG – Telekommunikationsgesetz	250
XXI. TMG – Telemediengesetz	256
XXII. UWG – Gesetz gegen den unlauteren Wettbewerb	259
XXIII. VAG – Versicherungsaufsichtsgesetz	260
XXIV. WpHG – Wertpapierhandelsgesetz	262
Stichwortverzeichnis	267