

Inhaltsverzeichnis

	Seite
Vorwort	V
Literaturverzeichnis	XVII

	Rz.	Seite
Einleitung		
I. Einführung	1	1
II. Checkliste der wichtigsten informationssicherheitsrechtlichen Pflichten	4	2
A. IT-Sicherheit in der Unternehmensorganisation		
I. Vorbemerkung	10	7
II. Bedeutung für Unternehmen	11	7
1. IT als Risikofaktor	13	8
a) Interne und externe Risiken	16	8
b) Risikoanalyse	20	10
c) Typische Sicherheitsversäumnisse	23	12
2. IT-Compliance	24	12
3. Nachteile durch Sicherheitsdefizite	28	14
III. IT-Sicherheitspflichten der Geschäftsleitung	34	15
1. Grundlagen der Verantwortlichkeit von Vorstand bzw. Geschäftsführung	36	16
a) Besonderheiten der Aktiengesellschaft	39	17
b) Ressortverantwortlichkeit für IT-Sicherheit	40	18
2. Pflicht zur Früherkennung bestandsgefährdender Risiken	43	18
a) Geeignete Maßnahmen zur Früherkennung	44	19
b) Implementierung eines Früherkennungs- und Überwachungssystems	49	20
c) ... als Bestandteil eines allgemeinen Risikomanagementsystems	52	21
d) Risikomanagementsystem bei börsennotierten Gesellschaften	55	22
3. Weitere Compliance-Pflichten	56	23
a) Compliance-Pflichten mit IT-Sicherheitsbezug	57	23
b) Umsetzung durch die Geschäftsleitung	58	24
4. Umfang der Geschäftsleitungspflichten	60	25
a) Anzuwendender Sorgfaltsmaßstab	61	25
b) Ermessensspielraum: Business Judgement Rule	66	27
IV. Pflicht zur Buchführung	70	29
1. Zulässiger Umfang elektronischer Buchführung	72	30
2. Sicherungspflichtige Daten und IT-Systeme	75	32

	Rz.	Seite
3. Anforderungen an die IT-Sicherheit der Buchführung	76	32
4. Umsetzung der Anforderungen: Internes Kontrollsystem	77	33
5. Besonderheiten für an der US-Börse notierte Unternehmen . . .	80	34
V. Rechtslage im Konzern	84	35
1. Konzernweite Compliance-Pflicht	85	36
2. Konzernweite Überwachungspflicht	88	37
VI. Einbeziehung des Betriebsrats	93	38
1. Mitwirkungsrechte	94	39
2. Mitbestimmungsrechte	96	39
 B. IT-Sicherheit als vertragliche Pflicht		
I. Vorbemerkung	100	43
II. Informationssicherheit als Hauptleistungspflicht	101	43
1. Verträge mit Informationssicherheitsbezug	102	43
a) Hohe Praxisrelevanz: Outsourcing-Verträge	104	45
b) Unternehmen als Schuldner oder Gläubiger von Informa- tionssicherheitsleistungen	107	47
2. „Sichere“ IT-Produkte	109	48
a) Verträge über die dauerhafte Überlassung von IT-Produkten	111	49
aa) Allgemeine Anforderungen	112	49
bb) Besonderheiten bei Verbraucherverträgen	121	52
cc) Besonderheiten im B2B2C-Verhältnis	130	55
dd) Besonderheiten im B2B-Verhältnis	134	58
b) Verträge über die zeitweise Überlassung von IT-Produkten . .	136	59
c) Fazit: Anbieterseitige Pflichten zur Anpassung des IT-Sicher- heitsstandards	142	61
III. Informationssicherheit als Nebenpflicht	146	62
IV. Hinweise zur Vertragsgestaltung	152	65
V. Übersicht zu typischen Fallgruppen	157	67
 C. Informationssicherheit zum Schutz von Geschäfts- geheimnissen		
	159	71
 D. IT-Sicherheitsdefizite als Rechtsbruch		
I. Vorbemerkung	171	79
II. Informationssicherheitsrechtliche Vorschriften als Marktverhal- tensregelungen	173	79
1. Datenschutzrecht	175	80
2. Vorgaben des Produktsicherheitsrechts	178	82
3. Vorgaben des BSI-Gesetzes	179	82
III. Wettbewerbsrechtliche Verletzungsfolgen	180	82

	Rz.	Seite
E. Datenschutz und IT-Sicherheit		
I. Vorbemerkung	182	85
II. Rechtsgrundlagen	183	85
1. DSGVO und BDSG	183	85
2. Bereichsspezifisches Datenschutzrecht	185	86
III. Anwendungsbereich	190	87
1. Sachlicher Anwendungsbereich	191	87
a) Personenbezogene Daten	192	88
b) Anonymisierung als Mittel zum Ausschluss der Anwend- barkeit der DSGVO	193	88
2. Persönlicher Anwendungsbereich	196	90
a) Verantwortliche	197	90
b) Auftragsverarbeiter	200	91
3. Räumlicher Anwendungsbereich	201	92
a) DSGVO	202	92
b) BDSG	205	93
IV. Datenschutzrechtliche Informationssicherheitsvorgaben	208	95
1. Informationssicherheitsstandard	209	95
a) Technische und organisatorische Maßnahmen	212	96
b) Mindestschutzanforderungen	217	98
c) Selbstregulierung und präventive Sicherheitsmaßnahmen	223	101
aa) Datenschutz durch Technikgestaltung und durch daten- schutzfreundliche Voreinstellungen	224	101
bb) Zertifizierungen und Verhaltensregeln	226	102
d) Schrems II	227	103
2. Weitere datenschutzrechtliche Informationssicherheitsvorgaben	230	104
a) Verzeichnis von Verarbeitungstätigkeiten	231	104
b) Datenschutz-Folgenabschätzung	233	105
c) Datenschutzbeauftragter	234	106
3. Meldepflichten bei Datenschutzverletzungen	238	107
a) Meldung gegenüber der Datenschutzaufsichtsbehörde	239	108
b) Benachrichtigung der betroffenen Personen	244	110
c) Exkurs: Checkliste „To-dos bei Data Breaches“	248	111
V. Verletzungsfolgen	250	114
1. Festsetzung von Bußgeldern für Datenschutzverstöße	251	115
2. Strafrechtliche Sanktionen	256	118
3. Hinweise zur Kommunikation mit den Aufsichtsbehörden	257	118
F. NIS2/BSI-Gesetz/KRITIS-DachG		
I. Rechtsentwicklung und Rechtsquellen	260	121
1. Nationale Gesetzgebung: BSI-Gesetz und IT-Sicherheitsgesetz (2.0)	261	121
2. Europäische Gesetzgebung: NIS-, NIS2- und CER-Richtlinie	264	122

	Rz.	Seite
II. Regelungssystematik des BSI-Gesetzes	267	124
III. IT-Sicherheitspflichten nach dem BSI-Gesetz	270	125
1. Adressaten	272	125
a) KRITIS-Betreiber	276	127
aa) Kritische Anlage	279	127
bb) Betreiber	284	130
b) Anbieter bestimmter digitaler Dienste	286	131
c) Telekommunikationsunternehmen	290	132
d) Einordnung anhand von Schwellenwerten	291	132
aa) Erfasste Sektoren	292	132
bb) Ausnahme für vernachlässigbare Geschäftstätigkeiten . .	295	134
cc) Berechnung der Schwellenwerte	296	135
dd) Besonders wichtige Einrichtungen	301	137
ee) Wichtige Einrichtungen	302	137
e) Einrichtungen der Bundesverwaltung	304	138
f) Ausnahmen	307	139
2. IT-Sicherheitsstandard	312	141
a) Einhaltung der Vorgaben	314	143
b) Einhaltung des „Standes der Technik“	318	145
c) Branchenspezifische Standards	320	146
d) Angriffserkennungssysteme und Nachweise nicht allgemein verpflichtend	323	147
3. Melde- und Unterrichtungspflichten	325	148
a) Meldepflichtig: erheblicher Sicherheitsvorfall	326	148
b) Meldeverfahren: Frist, Inhalt und Form	328	149
aa) Frühe Erstmeldung	330	150
bb) Bestätigungs-/Aktualisierungsmeldung	331	150
cc) Zwischenmeldung	332	151
dd) Abschlussmeldung	333	151
c) Freiwillige Meldungen	335	151
d) Unterrichtung über erhebliche Cyberbedrohungen in einzelnen Sektoren	337	152
e) Reaktion des BSI und Unterrichtungspflichten	339	153
4. Registrierungspflicht	343	154
5. Verantwortlichkeit der Geschäftsleitung	346	155
6. Einsatz kritischer Komponenten	354	158
7. Zusätzliche IT-Sicherheitspflichten für KRITIS-Betreiber	358	160
a) Angriffserkennungssysteme	360	160
b) Erweiterte Registrierungs- und Meldepflicht	362	161
c) Nachweis der Einhaltung	363	161
8. Zusätzliche Regelungen für Anbieter bestimmter digitaler Dienste	366	163
a) Besondere Regelung zur Behördenzuständigkeit	367	163
b) Erweiterter IT-Sicherheitsstandard	369	164
c) Benennung eines EU-Vertreters	371	165

	Rz.	Seite
d) Zusätzliche Registrierungspflicht	372	165
e) Spezieller Maßstab für erhebliche Sicherheitsvorfälle	375	166
f) Domain-Namen-Datenbank	378	167
9. Aufsichtsbefugnisse des BSI	381	168
a) Anordnung von Nachweisen	382	169
b) Überprüfung der Einhaltung	384	169
c) Anordnung konkreter Maßnahmen	385	170
d) Anordnung der Unterrichtung	386	170
e) Sanktionen	387	170
f) Besonderheiten bei Maßnahmen gegenüber wichtigen Einrichtungen	389	171
10. Zivilrechtliche Haftung	391	171
11. Auswirkungen des BSI-Gesetzes auf Hersteller von IT-Produkten	394	172
a) Hersteller kritischer Komponenten	395	172
b) Mitwirkungspflichten der Hersteller bei Störungen der IT-Sicherheit	396	173
c) IT-Sicherheitskennzeichen und Zertifizierung	399	174
d) Warnungen und Empfehlungen des BSI an die Öffentlichkeit	404	175
e) Untersuchungsrechte des BSI	408	177
12. Bußgelder	412	177
IV. Zusätzliche Pflichten für KRITIS-Betreiber nach dem KRITIS-Dachgesetz	415	178
1. Adressaten	416	179
2. Sicherheitspflichten	422	181
a) Risikoanalyse und -bewertung	423	181
b) Resilienzmaßnahmen	425	183
c) Registrierung	428	184
d) Meldepflichten	429	184
e) Geschäftsleitungspflichten	432	185
f) Nachweispflicht	434	186
3. Kritische Einrichtungen von besonderer Bedeutung für Europa	435	186
4. Zuständige Behörde	437	187
5. Verletzungsfolgen	438	188
G. Sonstige branchenspezifische Vorschriften zur IT-Sicherheit		
I. Vorbemerkung	440	189
II. IT-Sicherheitspflichten von Anbietern digitaler Dienste	441	189
1. Adressaten	442	189
2. IT-Sicherheitsstandard	445	191
a) Pflichtenumfang	447	191
b) Abgrenzung zum BSI-Gesetz	456	195
3. Verletzungsfolgen	459	196

	Rz.	Seite
III. IT-Sicherheitspflichten im Telekommunikationsbereich	462	196
1. Adressaten	463	197
2. IT-Sicherheitsstandard	470	198
3. Sicherheitsbeauftragter und Sicherheitskonzept	480	202
4. Meldepflichten	484	204
a) Meldepflichten zu Sicherheitsvorfällen nach § 168 Abs. 1 TKG	484	204
aa) Meldepflichtige Ereignisse	485	204
bb) Inhalt und Form der Meldung	488	205
cc) Reaktion der BNetzA und des BSI	489	206
dd) Benachrichtigung der Öffentlichkeit	490	206
b) Datenschutzrechtliche Meldepflichten gem. § 169 TKG	492	207
aa) Benachrichtigungspflichten bei Datenschutzver- letzungen	493	207
bb) Dokumentationspflichten bei Datenschutzver- letzungen	495	208
c) Informationspflicht bei von Nutzern ausgehenden Beeinträchtigungen	496	208
5. Verletzungsfolgen	499	209
a) Bußgelder	500	209
b) Schadensersatz und Unterlassung	502	210
IV. IT-Sicherheitspflichten von Energieversorgern	506	211
1. Adressaten	507	212
2. IT-Sicherheitsstandard	508	212
3. Nachweispflichten	511	213
4. Registrierungspflicht	514	214
5. Melde- und Unterrichtungspflichten	516	215
6. Geschäftsleitungspflichten	517	215
7. Verletzungsfolgen	518	215
V. IT-Sicherheitspflichten im Atomenergiebereich	521	217
1. Adressaten	522	217
2. IT-Sicherheitsstandard	523	217
3. Meldepflichten	524	218
4. Verletzungsfolgen	525	218
VI. IT-Sicherheitspflichten im Gesundheitswesen	527	219
1. IT-Sicherheit in der vertragsärztlichen und vertragszahn- ärztlichen Versorgung	529	220
2. IT-Sicherheitspflichten für Krankenhäuser	533	221
3. IT-Sicherheitspflichten für Kranken- und Pflegekassen	538	222
4. IT-Sicherheitspflichten für den Cloud-Einsatz im Gesundheits- wesen	541	224
5. IT-Sicherheitspflichten in der Telematikinfrastruktur	543	226
a) Adressaten	543	226
b) IT-Sicherheitsstandard	544	226

	Rz.	Seite
c) Meldepflichten	547	227
d) Verletzungsfolgen	548	228
6. IT-Sicherheitspflichten für Hersteller digitaler Gesundheits- und Pflegeanwendungen	549	228
a) Hersteller digitaler Gesundheitsanwendungen	549	228
b) Hersteller digitaler Pflegeanwendungen	552	229
VII. IT-Sicherheit im Finanz- und Versicherungsbereich	556	231
1. Adressaten	559	231
2. IT-Sicherheitspflichten für Finanzunternehmen	560	232
a) IKT-Risikomanagement	561	232
b) Behandlung, Klassifizierung und Meldung IKT-bezogener Vorfälle	568	236
aa) Klassifizierung von Vorfällen und Cyberbedrohungen	571	237
bb) Meldung an Behörden	575	240
cc) Unterrichtung der Kunden und der Öffentlichkeit	579	242
dd) Zahlungsbezogene Betriebs- oder Sicherheitsvorfälle	580	242
c) Betriebsstabilität	581	243
d) Steuerung der Risiken durch IKT-Drittdienstleister	584	244
3. Unmittelbare IT-Sicherheitspflichten für „kritische“ IKT-Drittdienstleister	589	246
4. Verhältnis zu anderen Gesetzen	595	248
5. Übergangsregeln für IT-Sicherheit im Bankwesen	597	249
a) Allgemeine IT-Sicherheitspflichten	599	250
b) Auslagerung von IT-Prozessen	604	252
6. Verletzungsfolgen	606	253
VIII. IT-Sicherheitspflichten nach dem Geldwäschegesetz	609	254
 H. Produktsicherheitsrechtliche Anforderungen an die IT-Sicherheit		
I. Vorbemerkung	616	257
II. Struktur der Produktsicherheitsrechts	618	258
III. Anforderungen an bestimmte Produkte	625	261
1. Cyber Resilience Act (CRA)	625	261
a) Anwendungsbereich	625	261
b) Herstellerpflichten	630	263
aa) Risikobewertung	630	263
bb) Grundlegende Cybersicherheitsanforderungen	631	263
cc) Schwachstellenmanagement	633	265
dd) Konformitätsbewertung	636	266
ee) Technische Dokumentation, EU-Konformitäts- erklärung und CE-Kennzeichnung	644	268
ff) Informations- und Meldepflichten	645	269
c) Möglichkeit zur Benennung eines EU-Vertreters	649	270

	Rz.	Seite
d) Pflichten der anderen Wirtschaftsakteure	650	270
aa) Einführerpflichten	652	270
bb) Händlerpflichten	653	271
cc) Pflichten der Verwalter von Open-Source-Software	654	271
2. Allgemeine Produktsicherheitsverordnung (GPSR)	656	272
a) Anwendungsbereich	657	272
b) Cybersicherheit als Teil des allgemeinen Sicherheitsgebots	660	274
c) Pflichten der Wirtschaftsakteure	662	275
3. Zertifizierung unter dem Cybersecurity Act (CSA)	667	276
IV. Spezielle Vorgaben für bestimmte Produktarten	674	280
1. Künstliche Intelligenz	675	281
a) IT-Sicherheits-KI als Hochrisiko-KI-System	676	281
b) IT-Sicherheit als Anforderung an Hochrisiko-KI-Systeme	678	283
c) IT-Sicherheit als Anforderung an GPAI-Modelle	682	284
2. Funkanlagen	685	287
3. Medizinprodukte	692	290
4. Kraftfahrzeuge	697	292
5. Luftfahrzeuge	699	293
 J. Allgemeine Haftung für Informationssicherheit		
I. Vorbemerkung	703	297
II. Haftungsverhältnisse im Unternehmen	704	297
1. Haftung der Geschäftsleitung gegenüber der Gesellschaft	705	297
a) Grundlagen der Vorstandshaftung in der AG	706	298
b) Grundlagen der Geschäftsführerhaftung in der GmbH	714	301
c) Praxislösung: D&O-Versicherung	716	302
d) Haftungsbeschränkung durch Zuweisung von Verantwortlichkeiten	718	302
aa) Horizontale Delegation: Ressortverantwortlichkeiten	719	303
bb) Vertikale Delegation	723	304
e) Exkurs: Haftung des Aufsichtsrats der AG	726	305
2. Haftung der Geschäftsleitung gegenüber den Aktionären bzw. Gesellschaftern	728	305
III. Haftung des Unternehmens gegenüber Dritten	733	307
1. Haftung der Geschäftsleitung im Außenverhältnis	734	308
a) Geringe Praxisrelevanz: Vertragsrecht	735	308
b) Gesteigerte Praxisrelevanz: Deliktsrecht	736	309
2. Vertragliche Haftung des Unternehmens	739	310
a) Grundlagen der vertraglichen Haftung	740	311
aa) Pflichtverletzung	741	311
bb) Vertretenmüssen und Beweislast	745	312
cc) Haftung für das Verhalten anderer	748	314
dd) Schaden	749	314
ee) Anspruchsreduzierendes Mitverschulden	750	315

	Rz.	Seite
b) Möglichkeiten des Haftungsausschlusses	756	317
aa) Praxisrelevante Regelungsfelder	758	318
bb) Unwirksamkeit nach speziellen gesetzlichen Regelungen .	760	319
cc) Individualvertragliche Unwirksamkeit und AGB-Recht . .	761	319
(1) Gesetzliche Klauselverbote für Verbraucherverträge .	762	320
(2) Ausstrahlungswirkung der Klauselverbote	763	320
3. Deliktische Haftung des Unternehmens	767	321
a) Haftung nach § 823 Abs. 1 BGB	768	322
aa) Deliktischer Schutz des Rechts am eingerichteten und ausgeübten Gewerbebetrieb	769	322
bb) Verkehrssicherungspflichten	773	324
cc) Insbesondere: Verkehrssicherungspflichten bzgl. fehlerhafter IT-Produkte	775	325
dd) Weitere Anspruchsvoraussetzungen	777	326
b) Haftung nach § 823 Abs. 2 BGB wegen der Verletzung eines Schutzgesetzes	778	327
c) Haftung nach § 831 BGB für Verrichtungsgehilfen	782	328
4. Verschuldensunabhängige Produkthaftung	784	329
IV. Inanspruchnahme von Cyber-Angriffern	789	332
1. Anspruchsgrundlagen	790	333
2. Anspruchsicherung und Vorgehen im Falle von Cyber- Angriffen	792	334
V. Ordnungswidrigkeiten- und Strafrecht	796	335
1. Haftung der Geschäftsleitung	797	336
a) § 130 OWiG – Verletzung der Aufsichtspflicht im Unter- nehmen	798	336
aa) Vorliegen von Aufsichtsdefiziten	799	337
bb) Ahndung von Aufsichtsdefiziten	800	338
b) § 266 StGB – Unternehmerische Fehlentscheidungen als Untreue?	802	338
2. Haftung des Unternehmens	806	340
a) Zurechnung von Pflichtverletzung der Geschäftsleitung (§§ 9, 30, 130 OWiG)	806	340
b) Europarechtliche eigenständige Bußgeldhaftung für Unter- nehmen	808	341
3. Haftung des Informationssicherheitsbeauftragten	811	342
K. Praktische Umsetzung: Informationssicherheitskonzept des Unternehmens		
I. Vorbemerkung	814	345
II. Benennung betrieblicher Informationssicherheitsbeauftragter	816	345
1. Abgrenzung verschiedener betrieblicher Beauftragter	820	347
2. Stellung des Informationssicherheitsbeauftragten	822	348
3. Haftung des Informationssicherheitsbeauftragten	826	350

	Rz.	Seite
a) Geringe Praxisrelevanz: Haftung des internen Informationssicherheitsbeauftragten	827	350
b) Höhere Praxisrelevanz: Haftung des externen Informationssicherheitsbeauftragten	833	353
4. Aufgaben des Informationssicherheitsbeauftragten	835	353
5. Kriterien zur Auswahl des Informationssicherheitsbeauftragten	837	354
III. Einrichtung eines Informationssicherheitsmanagementsystems . . .	839	355
1. Vorteile des Informationssicherheitsmanagementsystems	842	356
2. Struktur des Informationssicherheitsmanagementsystems	845	357
3. Vorgehensweise bei der Schaffung des Informationssicherheitsmanagementsystems	846	359
IV. Implementierung von IT-Betriebsrichtlinien	854	361
1. Schaffung eines internen Handlungsstandards	855	361
2. Zentrale Elemente von IT-Betriebsrichtlinien	857	362
3. Praxisrelevante Problemfelder	860	365
a) Private Internetnutzung	861	365
b) Bring your own Device	867	367
c) Social-Media-Nutzung	872	368
d) Mobiles Arbeiten	876	370
V. Notfallkonzept und Verhalten im Falle von IT-Sicherheitsvorfällen	879	371
1. Konzeption und Inhalt	880	371
2. Verhalten bei und Bewältigung von IT-Sicherheitsvorfällen	883	372
VI. Nutzung technischer Regelwerke	884	373
1. BSI-Grundschutz	885	373
2. ISO/IEC 27001	887	375
3. IT Infrastructure Library (ITIL)	889	375
4. Standard-Datenschutzmodell (SDM)	890	376
5. ENISA-Empfehlungen	891	376
Stichwortverzeichnis		379