

# Inhaltsverzeichnis

	Seite
Vorwort . . . . .	V
Literaturverzeichnis . . . . .	XV

Rz. Seite

## Einleitung

I. Einführung . . . . .	1	1
II. Checkliste der wichtigsten IT-sicherheitsrechtlichen Pflichten . . . . .	4	2

## A. IT-Sicherheit in der Unternehmensorganisation

I. Vorbemerkung . . . . .	9	7
II. Bedeutung für Unternehmen . . . . .	10	7
1. IT als Risikofaktor . . . . .	12	8
a) Interne und externe Risiken . . . . .	15	8
b) Risikoanalyse . . . . .	19	10
c) Typische Sicherheitsversäumnisse . . . . .	22	11
2. IT-Compliance . . . . .	23	12
3. Nachteile durch Sicherheitsdefizite . . . . .	27	13
III. IT-Sicherheitspflichten der Geschäftsleitung . . . . .	32	14
1. Grundlagen der Verantwortlichkeit von Vorstand bzw. Geschäftsführung . . . . .	34	15
a) Besonderheiten der Aktiengesellschaft . . . . .	36	16
b) Ressortverantwortlichkeit für IT-Sicherheit . . . . .	37	16
2. Pflicht zur Früherkennung bestandsgefährdender Risiken . . . . .	40	17
a) Geeignete Maßnahmen zur Früherkennung . . . . .	41	18
b) Implementierung eines Früherkennungs- und Überwachungssystems . . . . .	46	19
c) ... als Bestandteil eines allgemeinen Risikomanagementsystems . . . . .	49	20
3. Weitere Compliance-Pflichten . . . . .	52	21
a) Compliance-Pflichten mit IT-Sicherheitsbezug . . . . .	53	21
b) Umsetzung durch die Geschäftsleitung . . . . .	54	22
4. Umfang der Geschäftsleitungspflichten . . . . .	56	23
a) Anzuwendender Sorgfaltsmaßstab . . . . .	57	23
b) Ermessensspielraum: Business Judgement Rule . . . . .	62	25
IV. Pflicht zur Buchführung . . . . .	66	27
1. Zulässiger Umfang elektronischer Buchführung . . . . .	68	28
2. Sicherungspflichtige Daten und IT-Systeme . . . . .	71	29
3. Anforderungen an die IT-Sicherheit der Buchführung . . . . .	72	30
4. Umsetzung der Anforderungen: Internes Kontrollsystem . . . . .	73	31
5. Besonderheiten für an der US-Börse notierte Unternehmen . . . . .	76	32
V. Rechtslage im Konzern . . . . .	80	33
1. Konzernweite Compliance-Pflicht . . . . .	81	33
2. Konzernweite Überwachungspflicht . . . . .	84	34

	Rz.	Seite
VI. Einbeziehung des Betriebsrats . . . . .	89	36
1. Mitwirkungsrechte . . . . .	90	36
2. Mitbestimmungsrechte . . . . .	92	37
<b>B. IT-Sicherheit als vertragliche Pflicht</b>		
I. Vorbemerkung . . . . .	96	41
II. IT-Sicherheit als Hauptleistungspflicht . . . . .	97	41
1. Verträge mit IT-Sicherheitsbezug . . . . .	98	41
a) Hohe Praxisrelevanz: Outsourcing-Verträge . . . . .	100	43
b) Unternehmen als Schuldner oder Gläubiger von IT-Sicherheitsleistungen . . . . .	103	45
2. „Sichere“ IT-Produkte . . . . .	105	46
a) Verträge über die dauerhafte Überlassung von IT-Produkten . . . . .	107	46
aa) Allgemeine Anforderungen . . . . .	108	47
bb) Besonderheiten bei Verbraucherverträgen . . . . .	116	49
b) Verträge über die zeitweise Überlassung von IT-Produkten . . . . .	125	52
c) Fazit: Anbieterseitige Pflichten zur Anpassung des IT-Sicherheitsstandards . . . . .	131	54
III. IT-Sicherheit als Nebenpflicht . . . . .	134	55
IV. Hinweise zur Vertragsgestaltung . . . . .	139	57
V. Übersicht zu typischen Fallgruppen . . . . .	142	58
<b>C. IT-Sicherheit zum Schutz von Geschäftsgeheimnissen . . . . .</b>	<b>144</b>	<b>61</b>
<b>D. IT-Sicherheitsdefizite als Rechtsbruch</b>		
I. Vorbemerkung . . . . .	156	67
II. Informationssicherheitsrechtliche Vorschriften als Marktverhaltensregelungen . . . . .	158	67
1. Datenschutzrecht . . . . .	160	68
2. Vorgaben des BSI-Gesetzes . . . . .	161	69
III. Wettbewerbsrechtliche Verletzungsfolgen . . . . .	162	69
<b>E. Datenschutz und IT-Sicherheit</b>		
I. Vorbemerkung . . . . .	164	71
II. Rechtsentwicklung und Rechtsquellen . . . . .	165	71
1. DSGVO und BDSG . . . . .	167	72
2. Bereichsspezifisches Datenschutzrecht . . . . .	169	73
III. Anwendungsbereich . . . . .	175	75
1. Sachlicher Anwendungsbereich . . . . .	176	75
a) Personenbezogene Daten . . . . .	177	75
b) Anonymisierung als Mittel zum Ausschluss der Anwendbarkeit der DSGVO . . . . .	178	76
2. Persönlicher Anwendungsbereich . . . . .	181	78
a) Verantwortlicher . . . . .	182	78

	Rz.	Seite
b) Auftragsverarbeiter . . . . .	184	79
3. Räumlicher Anwendungsbereich . . . . .	185	79
a) DSGVO . . . . .	186	79
b) BDSG . . . . .	189	81
IV. Datenschutzrechtliche IT-Sicherheitsvorgaben . . . . .	192	82
1. IT-Sicherheitsstandard . . . . .	193	82
a) Technische und organisatorische Maßnahmen . . . . .	196	83
b) Mindestschutzanforderungen . . . . .	200	86
c) Selbstregulierung und präventive Sicherheitsmaßnahmen . . . . .	206	88
aa) Datenschutz durch Technikgestaltung und durch daten- schutzfreundliche Voreinstellungen . . . . .	207	89
bb) Zertifizierungen und Verhaltensregeln . . . . .	209	90
d) Schrems II . . . . .	210	90
2. Weitere datenschutzrechtliche Informations-Sicherheitsvorgaben . . . . .	213	91
a) Verzeichnis von Verarbeitungstätigkeiten . . . . .	214	92
b) Datenschutz-Folgenabschätzung . . . . .	216	92
c) Datenschutzbeauftragter . . . . .	217	93
3. Meldepflichten bei Datenschutzverletzungen . . . . .	221	94
a) Meldung gegenüber der Datenschutzaufsichtsbehörde . . . . .	222	94
b) Benachrichtigung der betroffenen Personen . . . . .	227	96
c) Exkurs: Checkliste „To-dos bei Data Breaches“ . . . . .	230	97
V. Verletzungsfolgen . . . . .	232	100
1. Festsetzung von Bußgeldern für Datenschutzverstöße . . . . .	233	101
2. Strafrechtliche Sanktionen . . . . .	239	103
3. Hinweise zur Kommunikation mit den Aufsichtsbehörden . . . . .	240	104
 <b>F. Branchenspezifische Regelungen: Vorgaben des BSI-Gesetzes</b>		
I. Vorbemerkung . . . . .	243	107
II. Rechtsentwicklung und Rechtsquellen . . . . .	244	107
1. Nationale Gesetzgebung: BSI-Gesetz und IT-Sicherheitsgesetz (2.0) . . . . .	245	107
2. NIS-Richtlinie . . . . .	248	108
III. Regelungssystematik des BSI-Gesetzes . . . . .	250	109
IV. IT-Sicherheitspflichten nach dem BSI-Gesetz . . . . .	253	110
1. Pflichten von KRITIS-Betreibern . . . . .	254	110
a) Adressaten . . . . .	255	110
aa) KRITIS-Dienstleistungen und Anlagen . . . . .	260	112
bb) KRITIS-Versorgungsgrad . . . . .	263	113
b) IT-Sicherheitsstandard . . . . .	265	114
aa) Einhaltung der Vorgaben . . . . .	267	115
bb) Einhaltung des „Stand der Technik“ . . . . .	269	116
cc) Branchenspezifische Standards . . . . .	270	117
dd) Angriffserkennungssysteme . . . . .	272	117
ee) Nachweis der Einhaltung . . . . .	274	118
c) Meldepflichten gegenüber dem BSI . . . . .	277	119
aa) Meldepflichtige Störungen . . . . .	280	120

	Rz.	Seite
bb) Meldefrist . . . . .	286	121
cc) Inhalt und Form der Meldung . . . . .	288	122
d) Einsatz kritischer Komponenten . . . . .	293	123
e) Bußgelder . . . . .	299	125
f) Zivilrechtliche Haftung . . . . .	301	126
2. Pflichten von Unternehmen im besonderen öffentlichen Interesse . . . . .	305	127
a) Adressaten . . . . .	306	127
b) IT-Sicherheitsstandard . . . . .	310	128
c) Registrierung gegenüber dem BSI . . . . .	313	129
d) Meldepflichtige Störungen . . . . .	315	130
aa) Meldefrist . . . . .	318	131
bb) Inhalt und Form der Meldung . . . . .	319	131
e) Bußgelder . . . . .	321	131
3. Pflichten der Anbieter digitaler Dienste . . . . .	323	132
a) Adressaten . . . . .	324	132
b) IT-Sicherheitsstandard . . . . .	331	135
c) Meldepflichten . . . . .	334	136
d) Bußgelder . . . . .	340	137
4. Auswirkungen des BSI-Gesetzes auf Hersteller von IT-Produkten . . . . .	343	138
a) Hersteller kritischer Komponenten . . . . .	344	139
b) Mitwirkungspflichten der Hersteller bei Störungen der IT-Sicherheit . . . . .	346	139
c) IT-Sicherheitskennzeichen . . . . .	348	140
d) Warnungen und Empfehlungen des BSI an die Öffentlichkeit . . . . .	354	142
e) Untersuchungsrechte des BSI . . . . .	357	142
f) Bußgelder . . . . .	360	143
 <b>G. Sonstige branchenspezifische Vorschriften zur IT-Sicherheit</b>		
I. Vorbemerkung . . . . .	361	145
II. IT-Sicherheitspflichten von Telemedienanbietern . . . . .	362	145
1. Adressaten . . . . .	363	145
2. IT-Sicherheitsstandard . . . . .	366	146
a) Pflichtenumfang . . . . .	373	148
b) Abgrenzung zum BSI-Gesetz . . . . .	377	150
3. Verletzungsfolgen . . . . .	380	150
III. IT-Sicherheitspflichten im Telekommunikationsbereich . . . . .	383	151
1. Adressaten . . . . .	384	152
2. IT-Sicherheitsstandard . . . . .	391	153
3. Sicherheitsbeauftragter und Sicherheitskonzept . . . . .	400	156
4. Meldepflichten . . . . .	404	158
a) Meldepflichten zu Sicherheitsvorfällen nach § 168 Abs. 1 TKG . . . . .	405	158
aa) Meldepflichtige Ereignisse . . . . .	405	158
bb) Inhalt und Form der Meldung . . . . .	408	159
cc) Benachrichtigung der Öffentlichkeit . . . . .	411	160
b) Datenschutzrechtliche Meldepflichten gem. § 169 TKG . . . . .	413	160

	Rz.	Seite
aa) Benachrichtigungspflichten bei Datenschutzverletzungen . . .	414	161
bb) Dokumentationspflichten bei Datenschutzverletzungen . . .	416	161
c) Informationspflicht bei von Nutzern ausgehenden Beeinträchtigungen . . . . .	417	162
5. Verletzungsfolgen . . . . .	420	162
a) Bußgelder . . . . .	421	162
b) Schadensersatz und Unterlassung . . . . .	423	163
IV. IT-Sicherheitspflichten von Energieversorgern . . . . .	427	165
1. Adressaten . . . . .	428	165
2. IT-Sicherheitsstandard . . . . .	429	165
a) Betreiber von Energieversorgungsnetzen . . . . .	430	166
b) Betreiber von Energieanlagen . . . . .	434	167
c) Systeme zur Angriffserkennung . . . . .	437	168
3. Meldepflichten . . . . .	438	169
4. Verletzungsfolgen . . . . .	441	169
V. IT-Sicherheitspflichten im Atomenergiebereich . . . . .	443	170
1. Adressaten . . . . .	444	170
2. IT-Sicherheitsstandard . . . . .	446	170
3. Meldepflichten . . . . .	447	171
4. Verletzungsfolgen . . . . .	448	171
VI. IT-Sicherheitspflichten im Gesundheitswesen . . . . .	450	172
1. IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung . . . . .	453	173
2. IT-Sicherheitspflichten für Krankenhäuser . . . . .	456	174
3. IT-Sicherheitspflichten in der Telematikinfrastruktur . . . . .	461	175
a) Adressaten . . . . .	461	175
b) IT-Sicherheitsstandard . . . . .	462	175
c) Meldepflichten . . . . .	465	176
d) Verletzungsfolgen . . . . .	466	176
4. IT-Sicherheitspflichten für Hersteller digitaler Gesundheits- und Pflegeanwendungen . . . . .	467	177
a) Hersteller digitaler Gesundheitsanwendungen . . . . .	467	177
b) Hersteller digitaler Pflegeanwendungen . . . . .	472	178
VII. IT-Sicherheit im Versicherungsbereich . . . . .	476	179
1. Adressaten . . . . .	477	179
2. IT-Sicherheitspflichten . . . . .	478	180
3. Verletzungsfolgen . . . . .	483	181
VIII. IT-Sicherheit im Finanz- und Bankwesen . . . . .	485	182
1. IT-Sicherheitspflichten im Bankensektor . . . . .	486	182
a) Allgemeine IT-Sicherheitspflichten . . . . .	486	182
b) Auslagerung von IT-Prozessen . . . . .	491	184
c) Verletzungsfolgen . . . . .	493	185
2. IT-Sicherheitspflichten im Online-Zahlungsverkehr . . . . .	494	186
3. IT-Sicherheitspflichten für Zahlungs- und E-Geld-Institute . . . . .	495	186
4. IT-Sicherheitspflichten für Identifizierungsdienstleistungen . . . . .	496	187

	Rz.	Seite
5. IT-Sicherheitspflichten von Wertpapierdienstleistungsunternehmen . . . . .	498	187
6. Besondere Pflichten von Börsenträgern . . . . .	499	188
IX. IT-Sicherheitspflichten nach dem Geldwäschegesetz . . . . .	501	189
 <b>H. Allgemeine Haftung für IT-Sicherheit</b>		
I. Vorbemerkung . . . . .	508	191
II. Haftungsverhältnisse im Unternehmen . . . . .	509	191
1. Haftung der Geschäftsleitung gegenüber der Gesellschaft . . . . .	510	191
a) Grundlagen der Vorstands-Haftung in der AG . . . . .	511	192
b) Grundlagen der Geschäftsführer-Haftung in der GmbH . . . . .	519	195
c) Praxislösung: D&O-Versicherung . . . . .	521	195
d) Haftungsbeschränkung durch Zuweisung von Verantwortlichkeiten . . . . .	523	196
aa) Horizontale Delegation: Ressortverantwortlichkeiten . . . . .	524	196
bb) Vertikale Delegation . . . . .	528	197
e) Exkurs: Haftung des Aufsichtsrats der AG . . . . .	531	198
2. Haftung der Geschäftsleitung gegenüber den Aktionären bzw. Gesellschaftern . . . . .	533	199
III. Haftung des Unternehmens gegenüber Dritten . . . . .	538	201
1. Haftung der Geschäftsleitung im Außenverhältnis . . . . .	539	201
a) Geringe Praxisrelevanz: Vertragsrecht . . . . .	540	202
b) Gesteigerte Praxisrelevanz: Deliktsrecht . . . . .	541	202
2. Vertragliche Haftung des Unternehmens . . . . .	544	204
a) Grundlagen der vertraglichen Haftung . . . . .	545	204
aa) Pflichtverletzung . . . . .	546	205
bb) Vertretenmüssen und Beweislast . . . . .	550	206
cc) Haftung für das Verhalten anderer . . . . .	553	208
dd) Schaden . . . . .	554	208
ee) Anspruchsreduzierendes Mitverschulden . . . . .	555	208
b) Möglichkeiten des Haftungsausschlusses . . . . .	561	210
aa) Praxisrelevante Regelungsfelder . . . . .	563	211
bb) Unwirksamkeit nach speziellen gesetzlichen Regelungen . . . . .	565	212
cc) Individualvertragliche Unwirksamkeit und AGB-Recht . . . . .	566	213
(1) Gesetzliche Klauselverbote für Verbraucherverträge . . . . .	567	213
(2) Ausstrahlungswirkung der Klauselverbote . . . . .	568	214
3. Deliktische Haftung des Unternehmens . . . . .	572	215
a) Haftung nach § 823 Abs. 1 BGB . . . . .	573	215
aa) Deliktischer Schutz des Rechts am eingerichteten und ausgeübten Gewerbebetrieb . . . . .	574	216
bb) Verkehrssicherungspflichten . . . . .	578	217
cc) Insbesondere: Verkehrssicherungspflichten bzgl. fehlerhafter IT-Produkte . . . . .	580	218
dd) Weitere Anspruchsvoraussetzungen . . . . .	582	220

	Rz.	Seite
b) Haftung nach § 823 Abs. 2 BGB wegen der Verletzung eines Schutzgesetzes . . . . .	583	220
c) Haftung nach § 831 BGB für Verrichtungsgehilfen . . . . .	588	222
4. Verschuldensunabhängige Produkthaftung . . . . .	590	223
IV. Inanspruchnahme von Cyber-Angreifern . . . . .	595	225
1. Anspruchsgrundlagen . . . . .	596	225
2. Anspruchssicherung und Vorgehen im Falle von Cyber-Angriffen . .	598	226
V. Ordnungswidrigkeiten- und Strafrecht . . . . .	602	228
1. Haftung der Geschäftsleitung . . . . .	603	228
a) § 130 OWiG – Verletzung der Aufsichtspflicht im Unternehmen	604	229
aa) Vorliegen von Aufsichtsdefiziten . . . . .	605	229
bb) Ahndung von Aufsichtsdefiziten . . . . .	606	230
b) § 266 StGB – Unternehmerische Fehlentscheidungen als Untreue? . . . . .	608	231
2. Haftung des Unternehmens . . . . .	612	232
3. Haftung des IT-Sicherheitsbeauftragten . . . . .	615	233
 <b>I. Praktische Umsetzung: IT-Sicherheitskonzept des Unternehmens</b>		
I. Vorbemerkung . . . . .	618	235
II. Benennung betrieblicher Beauftragter für IT-Sicherheit . . . . .	620	235
1. Abgrenzung verschiedener betrieblicher Beauftragter . . . . .	624	237
2. Stellung des IT-Sicherheitsbeauftragten . . . . .	626	238
3. Haftung des IT-Sicherheitsbeauftragten . . . . .	630	240
a) Geringe Praxisrelevanz: Haftung des internen IT-Sicherheitsbeauftragten . . . . .	631	240
b) Höhere Praxisrelevanz: Haftung des externen IT-Sicherheitsbeauftragten . . . . .	637	242
4. Aufgaben des IT-Sicherheitsbeauftragten . . . . .	639	243
5. Kriterien zur Auswahl des IT-Sicherheitsbeauftragten . . . . .	641	244
III. Einrichtung eines Informationssicherheitsmanagementsystems . . . . .	643	245
1. Vorteile des Informationssicherheitsmanagementsystems . . . . .	646	245
2. Struktur des Informationssicherheitsmanagementsystems . . . . .	649	246
3. Vorgehensweise bei der Schaffung des Informationssicherheitsmanagementsystems . . . . .	650	248
IV. Implementierung von IT-Betriebsrichtlinien . . . . .	658	250
1. Schaffung eines internen Handlungsstandards . . . . .	659	250
2. Zentrale Elemente von IT-Betriebsrichtlinien . . . . .	661	251
3. Praxisrelevante Problemfelder . . . . .	664	253
a) Private Internetnutzung . . . . .	665	253
b) Bring your own Device . . . . .	671	255
c) Social-Media-Nutzung . . . . .	676	257
d) Mobiles Arbeiten . . . . .	680	258
V. Notfallkonzept und Verhalten im Falle von IT-Sicherheitsvorfällen . . . .	683	259
1. Konzeption und Inhalt . . . . .	684	259
2. Verhalten bei und Bewältigung von IT-Sicherheitsvorfällen . . . . .	687	261

## Inhaltsverzeichnis

---

	Rz.	Seite
VI. Nutzung technischer Regelwerke . . . . .	688	262
1. BSI-Grundschutz . . . . .	689	262
2. ISO/IEC 27001 . . . . .	691	263
3. IT Infrastructure Library (ITIL) . . . . .	693	264
4. Standard-Datenschutzmodell (SDM) . . . . .	694	264
5. ENISA-Empfehlungen . . . . .	695	264
Stichwortverzeichnis . . . . .		267