

Inhaltsübersicht

<i>Vorwort</i>	V
<i>Bearbeiterverzeichnis</i>	VII
<i>Inhaltsverzeichnis</i>	XIII
<i>Abkürzungsverzeichnis</i>	XXXIX
<i>Literaturverzeichnis</i>	XLV
1. Kapitel Begriffsbestimmungen Compliance: Bedeutung und Notwendigkeit	1
2. Kapitel Grundlagen für Compliance	15
3. Kapitel Compliance-Organisation in der Praxis	101
4. Kapitel Risikobereiche	199
5. Kapitel Risikomanagement und Umgang mit besonderen Risikosituationen	583
6. Kapitel Compliance und Strafrecht	681
7. Kapitel Compliance und Aufsichtsrecht	733
Anhang	773
<i>Stichwortverzeichnis</i>	797

Inhaltsverzeichnis

<i>Vorwort</i>	V
<i>Bearbeiterverzeichnis</i>	VII
<i>Inhaltsübersicht</i>	XI
<i>Abkürzungsverzeichnis</i>	XXXIX
<i>Literaturverzeichnis</i>	XLV

1. Kapitel

Begriffsbestimmungen Compliance: Bedeutung und Notwendigkeit

I. Einführung	1
II. Ausgangslage und Historie	2
III. Haftungsrisiken von Unternehmen und Management	3
1. BGH-Rechtsprechung zur Haftung von Aufsichtsratsmitgliedern	3
2. Gesteigerte Verantwortung des Managements für seine Mitarbeiter	4
3. Stetiger Anstieg von Haftungsrisiken	4
4. Zunehmende Insolvenzen	4
5. Business Judgement Rule	5
6. Allgemeine Regeln	6
IV. Gesetzliche Grundlagen und unternehmerische Pflichten	7
V. Bedeutung einer Compliance-Organisation	10
VI. Compliance-Funktionen	11

2. Kapitel

Grundlagen für Compliance

A. Deutschland	15
I. Rechtliche Grundlagen der Compliance	15
1. Die Geschäftsleiterverantwortung als wesentliche Rechtsgrundlage der Compliance (§ 93 AktG, § 43 GmbHG)	16
1.1 Die Legalitätspflicht des Geschäftsleiters	16
1.2 Folgerungen für die Compliance-Organisation	17
1.3 Enthftung durch Zertifizierung?	19
1.4 Rechtsformspezifische Besonderheiten	20
2. Strafrechtliche Organisationspflichten	21
3. Spezialgesetzliche Compliance-Pflichten	23
4. Rechtsvergleichender Ausblick: Die USA als „Mutterland“ der Compliance?	24
4.1 Kapitel 8 der US Federal Sentencing Guidelines	25
4.2 Sarbanes Oxley Act	26
5. Rechtsvergleichender Ausblick: Das Vereinigte Königreich als Treiber für die Fortentwicklung europäischer Compliance?	27

II.	Grundsätze ordnungsgemäßer Compliance	28
1.	Compliance als Leitungsaufgabe	29
2.	Grundsatz der Risikoadäquanz	29
3.	Compliance als Organisationsaufgabe	29
4.	Grundsatz der Ausdrücklichkeit und der Schriftlichkeit	30
5.	Compliance als Schulungsaufgabe	31
6.	Überwachung und Kontrolle	32
III.	Ausblick	34
B. Österreich		34
I.	Einführung	34
II.	Die Grundsätze ordnungsgemäßer Compliance	35
1.	Zwecksetzungen von Compliance	35
1.1	Schutzzweck	35
1.2	Beratungs- und Informationszweck	36
1.3	Überwachungszweck	36
1.4	Marketing-Zweck	36
2.	Zielsetzung	36
3.	Managementverantwortung	36
4.	Unabhängigkeit	36
5.	Stellung im Unternehmen	37
6.	Ausstattung/Ressourcen	37
7.	Aufgabenbereiche	38
7.1	Entwicklung, Formulierung und Evaluierung interner Richtlinien und Verfahren	38
7.2	Laufende Überwachung aller einschlägigen Vorschriften (inklusive Schulung/Beratung)	38
III.	Allgemeines Gesellschaftsrecht und „Corporate Governance“	38
1.	Einleitung	38
2.	Haftung der Organe	39
3.	Geschäftsleiterberichtspflichten	42
4.	Österreichischer Corporate Governance Kodex	43
5.	Gesellschaftsrechtliche Compliance	44
IV.	Unternehmensstrafrecht	45
1.	Zurechnung von Entscheidungsträgern und Mitarbeitern zu den Verbänden	45
2.	Die Zurechnungskriterien	45
3.	Maßnahmen zur Verhinderung von Bestrafungen des Verbandes („Strafrechtliches Risikomanagement“)	46
3.1	Gefahrenanalyse:	46
3.2	Möglichkeiten der Risikoverminderung:	46
3.3	Strategie für den Ernstfall:	46
4.	Strafraahmen	47
V.	Verwaltungsstrafgesetze	47

VI.	Emittenten-Compliance	48
1.	Grundsätze für die Informationsweitergabe im Unternehmen	49
1.1	Einrichtung von Vertraulichkeitsbereichen	49
1.2	Umgang mit compliance-relevanten Informationen	50
1.3	Weitergabe von compliance-relevanten Informationen	50
2.	Organisatorische Maßnahmen zur Verhinderung einer missbräuchlichen Verwendung oder Weitergabe von compliance-relevanten Informationen	51
2.1	Sperrfristen und Handelsverbote	51
2.2	Übermittlung von „Directors, Dealings“-Meldungen	52
2.3	Insider-Listen	52
2.4	Compliance-Richtlinie	52
2.5	Compliance-Verantwortlicher	52
VII.	Wettbewerbsrechtliche Compliance	53
1.	Allgemeines	53
2.	Wettbewerbsbeschränkungen (Kartelle)	54
2.1	Definition von Kartellen	54
2.2	Zivilrechtliche Rechtsfolgen eines Verstoßes gegen das Kartellverbot	54
3.	Missbrauch einer marktbeherrschenden Stellung	55
4.	Zusammenschlüsse	55
5.	Behörden und Verfahren	56
5.1	Kartellgericht und Kartellobergericht	56
5.2	Bundeswettbewerbsbehörde (BWB)	56
5.3	Bundeskartellanwalt (BKA)	56
6.	Rechtsdurchsetzung	57
7.	Wettbewerbsrechtliche Compliance-Programme	57
VIII.	Datenschutzrechtliche Compliance	59
1.	Grundrecht auf Datenschutz	60
2.	Allgemeine Grundsätze und die Zulässigkeit der Verwendung von Daten	60
3.	Die Übermittlung von Daten	61
4.	Exkurs: Videoüberwachung	61
5.	Heranziehen von Dienstleistern	62
6.	Whistleblower-Hotlines	62
7.	Datengeheimnis	63
8.	Publizität der Datenanwendungen	63
9.	Informations- und Offenlegungspflicht des Auftraggebers	63
10.	Datensicherungsmaßnahmen	64
11.	Die Rechte der Betroffenen	65
11.1	Das Recht auf Auskunft	65
11.2	Recht auf Richtigstellung und Löschung	65
11.3	Widerspruchsrecht	65
12.	Kontrollorgane	65
12.1	Datenschutzbehörde	65
12.2	Der Datenschutzrat	66

13. Schadenersatz	66
14. Strafbestimmungen	66
IX. Antikorruptionsrecht	67
1. Der „private Sektor“	67
2. Der „öffentliche Sektor“	69
2.1 Bestechlichkeit (§ 304 StGB Geschenkkannahme durch Amts- träger, Schiedsrichter oder Sachverständige für pflichtwidrige Vornahme oder Unterlassung einer Amtshandlung)	69
2.2 Vorteilsannahme (§ 305 StGB Geschenkkannahme durch Amts- träger, Schiedsrichter oder Sachverständige für pflichtgemäße Vornahme oder Unterlassung einer Amtshandlung)	70
2.3 Vorteilsnahme zur Beeinflussung (§ 306 StGB)/ Vorteilszuwendung zur Beeinflussung (§ 307b StGB)	70
X. Geldwäsche	71
XI. Compliance der österreichischen Kreditwirtschaft und Versicherungsunternehmen	73
1. Wertpapieraufsichtsgesetz (WAG)	73
1.1 Organisatorische Anforderungen	74
1.2 Wohlverhaltensregeln § 40f WAG	74
2. Aufsichtsreform 2007	75
2.1 Aufsichtsratsvorsitzende	75
2.2 Prüfungsausschuss des Aufsichtsrates	76
2.3 Interne Revision	76
3. Der Standard Compliance Code der österreichischen Kreditwirtschaft (SCC)	77
4. Konzeption und Gliederung des SCC 2008	77
5. Standard Compliance Code der Österreichischen Versicherungswirtschaft (SCCV)	79
C. Schweiz	79
I. Einführung	79
II. Unternehmensstrafrecht und Compliance-Management	81
1. Unternehmensstrafrecht	81
2. Elemente der Compliance-Organisation	83
III. Korruptionsrecht	84
1. Verbotene Handlungen	84
2. Erlaubte Praktiken: Gesetzlicher Anspruch oder Sozialadäquanz ...	86
3. Internationale Abkommen	87
IV. Kartellrecht	87
1. Gesetzliche Grundlagen	87
2. Praxis	88
3. Behörden	88
4. Die Sanktionen	89

V.	Finanzmarktregulierung und Geldwäscherei	89
	1. Finanzmarktrecht in der Schweiz	89
	2. Regeln für börsenkotierte Unternehmen	90
	3. Geldwäscherei	92
VI.	Datenschutz	94
	1. Gesetzliche Grundlage	94
	2. Behörde	96
VII.	Arbeitsrecht	96
	1. Beschäftigung ausländischer Arbeitnehmer	96
	2. Weitere Regelungsbereiche	97
VIII.	Erwerb von Grundstücken/Umweltschutz	97
	1. Überblick	97
	2. Grundstückserwerb	98
	3. Altlasten	98
	4. Umweltverträglichkeitsprüfung	98

3. Kapitel

Compliance-Organisation in der Praxis

A.	Compliance-Programm und praktische Umsetzung	101
I.	Einführung	101
II.	Compliance und Wertekultur: „Tone from the Top“	101
III.	Fundamente der Compliance-Organisation	102
	1. Compliance-Abteilung vs. Compliance-Funktion	102
	2. Compliance-Abteilung im Konzern	102
	2.1 Organisatorische Angliederung	102
	2.2 Schnittstellen zu anderen Funktionen	104
	3. Compliance Officer	104
	3.1 Persönlichkeitsmerkmale	104
	3.2 Aufgaben	106
IV.	Instrumente eines Compliance-Programmes	109
	1. Risk Assessment als Standortbestimmung auf der Risikolandkarte	109
	2. Verhaltenskodices und Richtlinienwesen	110
	3. Kommunikation	113
	3.1 Internet, Intranet	113
	3.2 Hinweisgebersystem („Whistleblowing Hotline“)	114
	3.3 Öffentlichkeitsarbeit	117
	4. Schulungen	118
	4.1 Präsenzs Schulungen vs. E-Learning	119
	4.2 Reputationstraining	120
	5. Kontrollen	121
	5.1 Control Testings und Audits	121
	5.2 „Mock Dawn Raids“	122
	6. Kooperation mit Behörden	123

V.	Compliance-Programm als dynamisches Strategieelement	124
1.	Risiko „Restrisiko“	124
2.	Notfallstrategie	124
3.	Optimierbarkeit von Compliance-Systemen	125
B.	Die Prüfung von Compliance Management-Systemen nach IDW PS 980 ..	125
I.	Einleitung	125
II.	Was – der Prüfungsgegenstand	127
III.	Wer – potenzielle Prüfer	129
IV.	Wie – Ziel und Vorgehen bei der Prüfung	131
1.	Konzeptionsprüfung	131
2.	Angemessenheitsprüfung	132
3.	Wirksamkeitsprüfung	133
4.	Grenzen der Wirksamkeitsprüfung	135
V.	Warum – Gründe für eine Prüfung	135
VI.	Rechtliche Bedeutung des IDW PS 980 für das Haftungsrecht	136
VII.	Prüfbereitschaft	139
1.	Die CMS-Beschreibung als Prüfungsgrundlage	139
2.	Herstellen der operativen Prüfbereitschaft	140
3.	Festlegung des Prüfungsumfangs	141
VIII.	Die Prüfung der Grundelemente eines CMS	142
1.	Compliance-Kultur	142
1.1	Definition	142
1.2	Prüfung	143
2.	Compliance-Risiken	144
2.1	Definition	144
2.2	Prüfung	145
3.	Compliance-Ziele	146
3.1	Definition	146
3.2	Prüfung	147
4.	Compliance-Programm	148
4.1	Definition	148
4.2	Prüfung	148
5.	Compliance-Organisation	151
5.1	Definition	151
5.2	Prüfung	151
6.	Compliance-Kommunikation	153
6.1	Definition	153
6.2	Prüfung	153
7.	Compliance-Überwachung und Verbesserung	154
7.1	Definition	154
7.2	Prüfung	155

C. Corporate Responsibility als Schlüssel für Compliance	156
I. Einführung	156
II. Schnelle Veränderung und Unsicherheit erzeugen Handlungsbedarf	159
III. Management als Vorbild	160
IV. Dezentralität bereitet die strukturelle Grundlage für Vertrauen	162
1. Fokussierung	163
2. Marktnähe	163
3. Motivation	163
4. Transparenz und Ergebnisverantwortung	164
5. Anpassungskraft	164
V. Corporate Responsibility (CR) und Compliance können zusammen zusätzliche Werte schaffen	165
VI. Handlungsansätze aus der Unternehmenspraxis	166
1. Initiative „Responsible Care“	166
2. „Business in the Community“ – Initiative der Wirtschaft in Großbritannien	168
3. Schulprogramme von GE und IBM	168
4. Gemeinsam Korruption bekämpfen	169
D. Risikomanagement im Kontext Compliance – Grundlagen, Prozesse, Verantwortlichkeiten und Methoden	170
I. Einführung	170
II. Die Entstehung des modernen Risikobegriffs	171
III. Risiko ist ein Konstrukt unserer Wahrnehmungen	172
IV. Grundlagen des Risikomanagements	174
1. Definition und Abgrenzung des Risikobegriffs	174
2. Die Risikolandkarte im Unternehmen	175
3. Drei Verteidigungslinien in der Praxis	179
4. Der Risikomanagement-Prozess in der Praxis	180
4.1 Strategisches Risikomanagement	180
4.2 Risikoidentifikation	183
4.3 Risikobewertung	184
4.4 Risikosteuerung	186
V. Standards im Risikomanagement	189
1. Überblick	189
2. Der Risiko-Management-Prozess als PDCA-Zyklus basierend auf der ISO 31000	190
3. COSO ERM	193
VI. Regulatorische und gesetzliche Grundlagen	194
VII. Fazit und Ausblick	197

4. Kapitel Risikobereiche

A. Kartellrecht	199
I. Einleitung	200
II. Pflicht zur Gesetzestreue und zur Durchführung von kartellrechtlichen Compliance-Maßnahmen	202
III. Kartellrechtlicher Sanktionskanon und Compliance	207
IV. Grundlagen des Kartellrechts	209
1. Überblick über das europäische und deutsche Kartellverbot	209
2. Die Freistellung vom Kartellverbot	210
3. Missbrauchsaufsicht	211
4. Fusionskontrolle	212
V. Legal Management und Legal Judgement im Kartellrecht	213
1. Einführung eines Kartellrechts-Compliance-Programms	213
1.1 Kartellrechtliche Risikoanalyse	215
1.2 Implementierung geeigneter Compliance-Maßnahmen	216
1.2.1 Compliance-Organisation	217
1.2.2 Kartellrechtliche Compliance-Schulungen	217
1.2.3 Beratung	218
1.2.4 Compliance-Regelwerk	218
1.2.5 Kontrollmaßnahmen	218
2. Maßnahmen bei Identifizierung kartellrechtsrelevanter Vorgänge	219
2.1 Absehen von Maßnahmen infolge einer rechtlichen Prüfung	219
2.2 Abhilfemaßnahmen	221
2.3 Klärung der Rechtslage mit Kartellbehörden	221
2.4 Kronzeugenantrag	222
2.5 Disziplinarische Maßnahmen gegen Verstoßverantwortliche	223
VI. Ausblick	
B. „Dawn Raids“ – Verhaltensregeln in kartellrechtlichen Ermittlungsverfahren	224
I. Einführung	224
II. Befugnisse und Grenzen in kartellrechtlichen Ermittlungsverfahren	225
III. „Dawn Raids Legal Risk Management“	229
IV. Verhaltensregeln bei Nachprüfung und Durchsuchung	231
1. Ankunft der Ermittler	232
2. Durchführung der Untersuchung	237
2.1 Bücher und sonstige Geschäftsunterlagen	238
2.2 Mündliche Erklärungen	242
2.3 Checkliste: Zeugen- und Beschuldigtenvernehmungen im Bußgeldverfahren	245

3. Abschluss	246
4. Nach Beendigung der Untersuchung	246
V. Muster	248
C. Korruption	255
I. Einführung	255
II. Compliance-Anforderungen – Abgrenzung von legaler Kundenpflege und Korruption	258
1. Umgang mit Amtsträgern im Inland	258
2. Umgang mit Amtsträgern im Ausland	262
3. Umgang mit privaten Geschäftspartnern im In- und Ausland	262
4. Sonderbereich Gesundheitswesen	266
5. Sonderbereich Organisierter Sport	267
D. Geldwäsche	268
I. Einleitung	268
1. Begriffsbestimmungen	268
1.1 Geldwäsche	268
1.2 Terrorismusfinanzierung	269
2. Internationale Vorgaben	269
2.1 Financial Action Task Force on Money Laundering	269
2.2 Europäische Union	269
3. Nationale Vorschriften	270
3.1 Gesetze	270
3.2 Rundschreiben der BaFin	271
3.3 Auslegungs- und Anwendungshinweise	271
II. Pflichten für Institute und Versicherungsunternehmen	271
1. Risikomanagement	272
1.1 Risikoanalyse	272
1.2 Interne Sicherungsmaßnahmen	273
1.2.1 Interne Grundsätze, Verfahren und Kontrollen	274
1.2.2 Geldwäschebeauftragter	274
1.2.3 Gruppenweite Umsetzung	275
1.2.4 Neue Produkte und Technologien	276
1.2.5 Zuverlässigkeitsprüfung	276
1.2.6 Schulung	277
1.2.7 Überprüfung durch die Interne Revision	277
2. Besondere Vorgaben für Kreditinstitute	277
3. Kundensorgfaltspflichten	278
3.1 Allgemeine Sorgfaltspflichten	278
3.2 Vereinfachte Sorgfaltspflichten	280
3.3 Verstärkte Sorgfaltspflichten	280
3.4 Ausführung von Sorgfaltspflichten durch Dritte	282
3.5 Auslagerung	282
4. Verdachtsmeldewesen	283
5. Geldbußen und persönliche Haftbarkeit	284

III.	Vorgaben für weitere Verpflichtete	284
1.	Interne Sicherungsmaßnahmen	284
2.	Kundensorgfaltspflichten	286
3.	Besondere Anforderungen an einzelne Verpflichtete	286
3.1	Veranstalter und Vermittler von Glücksspielen	286
3.2	Zahlungsinstitute und E-Geld-Institute	287
3.3	Güterhändler	288
E.	Arbeitsrecht	289
I.	Einführung	289
II.	Inhalte und Grenzen eines Verhaltenskodex bzw. eines Compliance Management Systems	290
1.	Inhalte	290
2.	Grenzen	292
2.1	Allgemeines Persönlichkeitsrecht, Art. 2 Abs. 1 GG i.V. mit Art. 1 Abs. 1 GG	292
2.2	Betriebliche Mitbestimmung, § 87 Abs. 1 Nr. 1 BetrVG	292
3.	Einhaltung von Compliance-Regeln	293
3.1	Überwachung der E-Mail- und Internetnutzung	293
3.1.1	Kontrolle dienstlicher E-Mail- und Internetnutzung	293
3.1.2	Kontrolle gestatteter privater E-Mail- und Internetnutzung	294
3.1.3	Gesetzeskonforme E-Mail-Kontrolle	294
3.1.4	Kollektivrechtliche Regelungen	294
3.2	Telefonüberwachung	294
3.2.1	Telefonüberwachung nur bei dienstlich gestatteter Nutzung	295
3.2.2	Telefonüberwachung bei gestatteter Privatnutzung	295
3.2.3	Kollektivrechtliche Regelungen	295
3.3	Systematischer Datenabgleich („Screening“)	295
3.4	Repressive Maßnahmen	296
III.	Implementierung eines Verhaltenskodex	297
1.	Direktionsrecht	297
2.	Arbeitsvertrag	298
3.	Betriebsvereinbarung/Dienstvereinbarung/Regelungsabrede/ Tarifvertrag	299
IV.	Arbeitsrechtliche Stellung des Compliance Officers	300
1.	Position des Compliance Officers	300
2.	Kündigungsschutz des Compliance Officers	302
3.	Haftung des Compliance Officers	305
3.1	Arbeitsrechtliche Haftungsgrundsätze	305
3.2	Strafrechtliche Haftung	306
3.3	Konsequenzen aus der haftungsrechtlichen Lage	306

F. Datenschutz	307
I. Einführung	307
II. Entwicklung des Datenschutzrechtes	307
III. Anwendungsbereich des Datenschutzrechts	310
1. Heutige gesetzliche Grundlagen	310
2. Anwendungsbereich der DSGVO	310
3. Personenbezogene Daten	311
4. Besondere personenbezogene Daten	312
5. Automatisierte und manuelle Verarbeitung etc. von Daten	312
IV. Rollen nach BDSG und DSGVO	313
1. Verantwortliche Stelle nach BDSG	313
2. Neue Rollen nach DSGVO	313
V. Datenschutzrechtliche Pflichten von privaten Unternehmen	314
1. Formelle Anforderungen	315
1.1 Bestellung von Datenschutzbeauftragten	315
1.1.1 Anforderungen nach BDSG	315
1.1.2 Anforderungen nach DSGVO	317
1.2 Verfahrensmeldungen	318
1.2.1 Meldepflichten gegenüber den Datenschutzaufsichtsbehörden	318
1.2.2 Erstellung der Verfahrensübersicht	319
1.2.3 Öffentliches Verzeichnis	321
1.3 Vorabkontrolle und Folgenabschätzung	321
1.4 Verpflichtung auf das Datengeheimnis	324
1.5 Einführung und Einhaltung von technischen und organisatorischen Maßnahmen	324
2. Grundlagen des Datenschutzrechts	326
2.1 Transparenz der Datenverarbeitung	327
2.2. Grundsatz der Datenvermeidung und der Datensparsamkeit	329
2.3. Direkterhebung bei dem Betroffenen	330
2.4 Zweckbindung	330
3. Zulässigkeit des Umgangs mit Daten	331
3.1 Gesetzliche Erlaubnis	332
3.1.1 Umgang mit Daten von Kunden etc	332
3.1.2. Umgang mit Beschäftigtendaten	334
3.1.3. Umgang mit besonderen personenbezogenen Daten, Daten betreffend Straftaten und Daten Minderjähriger	338
3.1.4. Einführung besonderer Verfahren (Videoüberwachung, GPS, RFID, Biometrie etc.)	338
3.2 Einwilligung	340
3.2.1 Einwilligung nach BDSG	340
3.2.2. Einwilligung nach DSGVO	341

3.3	Austausch von personenbezogenen Daten	342
3.3.1	Übermittlung von Daten nach BDSG	343
3.3.2	Übermittlung von Daten nach DSGVO	343
3.3.3	Auftragsdatenverarbeitung	344
4.	Wahrung der Rechte der Betroffenen	348
4.1	Auskunftsrechte	348
4.2	Berichtigung, Sperrung und Löschung etc. von Daten	349
4.3	Erweiterte Rechte der Betroffenen nach DSGVO	349
4.3.1	Generelle Pflichten des Verantwortlichen	349
4.3.2	Recht auf Auskunft	350
4.3.3	Recht auf Berichtigung	350
4.3.4	Pflicht zur Löschung bzw. „Recht auf Vergessenwerden“	350
4.3.5	Recht auf Einschränkung der Verarbeitung	351
4.3.6	Mitteilungspflicht über Berichtigung etc.	352
4.3.7	Recht auf Datenübertragbarkeit	352
4.3.8	Widerspruchsrechte	353
VI.	Haftungsrisiken	353
1.	Schadensersatzansprüche nach dem BDSG und der DSGVO	354
2.	Vertragliche Ansprüche	355
3.	Deliktische Ansprüche	356
4.	Ordnungswidrigkeit und Straftat	356
5.	Maßnahmen der Datenschutzaufsichtsbehörden	357
6.	Besondere Informationspflichten bei Datenschutzverstößen	358
VII.	Maßnahmen zur Sicherstellung von datenschutzrechtlicher Compliance	359
1.	Datenschutz-Audit	359
1.1	Gesetzliche Vorgaben für Audits	360
1.2	Datenschutzgütesiegel	361
2.	Aufbau einer Datenschutzorganisation	361
3.	Datenschutzrichtlinien/Code of Conduct	362
4.	Konzepte zum Datenschutz	363
5.	Schulung der Mitarbeiter	364
6.	Whistleblowing-Hotlines	364
VIII.	Ausblick	365
G. Intellectual Property		366
I.	Einführung	366
II.	Überblick IP-Compliance	366
1.	Sicherung, Pflege und Verteidigung eigener IP-Rechte	366
2.	Recherche und Analyse fremder IP-Rechte	367
3.	IP-Vertragsmanagement	368
4.	Unternehmenskommunikation	369

III.	IP-Compliance im Produktzyklus	370
1.	IP-Compliance in der Forschung und Entwicklung	370
a)	Schutz von Entwicklungsergebnissen	370
aa)	Arbeitnehmer und freie Mitarbeiter als Erfinder	371
bb)	Arbeitnehmer und freie Mitarbeiter als Urheber	372
cc)	Arbeitnehmer und freie Mitarbeiter als Know-how Träger	372
b)	Recherche von Drittrechten am Produkt	373
c)	Auftragsforschung und Forschungsk Kooperationen	374
2.	IP-Compliance im Einkauf	375
a)	AGB	375
b)	Bezug von Graumarktware	376
c)	Prüfung der Verkehrsfähigkeit	376
3.	IP-Compliance in der Herstellung	376
4.	IP-Compliance in Marketing und Vertrieb	377
a)	Werbung	377
aa)	Unlautere und irreführende Werbung	377
bb)	Unzulässige vergleichende Werbung	378
cc)	Werbung in regulierten Industrien	378
b)	Verbraucher- Informationspflichten	379
c)	Regulatorische Absatzverbote	379
d)	Vertrieb von veränderter Markenware	379
IV.	IP-Compliance-Checkliste	380
H. Steuern		380
I.	Einführung	380
II.	Steuerstrafrechtliche- und bußgeldrechtliche Tatbestände	382
III.	Persönliche Haftung für Steuerschuld des Unternehmens	385
1.	Umfang der Haftung und Haftungsbescheid	385
2.	Haftungsnorm des § 69 AO	386
2.1	Haftungsschuld	386
2.2	Der Haftungsschuldner	386
2.3	Pflichtverletzung	387
2.4	Schaden und Kausalität	388
2.5	Verschulden und Enthftung	389
3.	Haftungsnorm des § 71 AO	389
IV.	Strafbefreiende Selbstanzeige	390
1.	Allgemeines	390
2.	Abermalige Neuregelung der Selbstanzeige (§ 371 AO)	391
3.	Vollständigkeitsgebot und zehnjähriger Berichtigungszeitraum	392
3.1	Grundlagen	392
3.2	Der zehnjährige Berichtigungszeitraum i.S.d. § 371 Abs. 1 S. 2 AO	393
3.3	Geringfügige Abweichungen i.S.d. BGH-Rechtsprechung	394

3.4 Teilselbstanzeige bei Umsatzsteuervoranmeldungen und Lohnsteueranmeldungen	395
3.4.1 Problematik aufgrund der Neuregelung durch das Schwarzgeldbekämpfungsgesetz	395
3.4.2 Neue Gesetzesregelung	396
4. Folgen bei Nichtzahlung bzw. teilweiser Zahlung	397
5. Sperrgründe im Rahmen der Selbstanzeige und § 398a AO	398
5.1 Grundlagen	398
5.2 Prüfungsanordnung	399
5.2.1 Erweiterung des Personenkreises mit Wirkung zum 1.1.2015	400
5.2.2 Beschränkung in sachlicher und zeitlicher Hinsicht mit Wirkung zum 1.1.2015	400
5.3 Betragsgrenze in Höhe von 25 000 EUR und § 398a AO	401
5.3.1 Gesetzliche Regelung	401
5.3.2 Bestimmung der Grenze und Berechnung des Zuschlags	402
5.3.3 § 398a AO in Drittbegünstigungsfällen	403
6. Bußgeldbefreiende Selbstanzeige nach § 378 Abs.3 AO	404
V. Berichtigungspflicht nach § 153 AO	404
1. Allgemeines	404
2. Verpflichteter Personenkreis	405
3. Abgrenzung zur Selbstanzeige	405
4. Zeitpunkt der Anzeige und Berichtigung	408
VI. OWiG/Verbandsgeldbuße/Abschöpfung	408
1. § 30 OWiG	408
2. § 29a OWiG/Verfall	410
3. Pflichten i.S.v. § 30 OWiG/130 OWiG	411
VII. Betriebsprüfung/Steuerfahndung	412
1. Betriebsprüfung	412
2. Steuerfahndung	415
3. Maßnahmen im Vorfeld von Ermittlungsmaßnahmen	415
4. Verhaltensregeln bei einer Durchsuchung	416
VIII. Umsatzsteuer	419
1. Ausstellung und Aufbewahrung von Rechnungen/Bußgeld bei Verstößen	420
2. Rechtzeitige Zahlung	420
3. Umsatzsteuerprüfungen	421
3.1 Umsatzsteuernachschau	422
3.2 Umsatzsteuer-Sonderprüfung	424
4. Nachweispflichten bei innergemeinschaftlichen Lieferungen	430
4.1 Voraussetzungen einer innergemeinschaftlichen Lieferung	431
4.2 Nachweispflicht unternehmerische Tätigkeit Vertragspartner	431
4.3 Belegnachweis	431
4.4 Buchnachweis	433

4.5	Objektive Nachweismöglichkeiten bei Mängeln des Beleg- oder Buchnachweises	434
4.6	EuGH-Rechtsprechung/Wichtige Indizwirkung der Umsatzsteuer-Identifikationsnummer	435
4.7	Zeitpunkt des Belegnachweises	436
4.8	Rechnungsmuster für eine innergemeinschaftliche Lieferung	436
5.	Umsatzsteuerbetrug/Versagung von Vorsteuerabzug/Versagung der Steuerfreiheit für innergemeinschaftliche Lieferungen	437
5.1	Versagung der Steuerbefreiung bei innergemeinschaftlichen Lieferungen/Verschärfte EuGH-Rechtsprechung/Italmoda	437
5.2	Vorsteuerabzug	440
6.	§ 14c-Fälle	445
6.1	Unrichtiger Steuerausweis (§ 14c Abs.1 UStG)	445
6.2	Unberechtigter Steuerausweis (§ 14c Abs.2 UStG)	446
7.	Checkliste	447
IX.	Funktionsverlagerungen	447
1.	Begriffsbestimmung	447
2.	Personalentsendungen	449
3.	Funktionsverdopplung	449
4.	Nutzungsüberlassung	450
5.	Verstoß gegen Europarecht	450
X.	Probleme bei Verrechnungspreisen	450
1.	Verrechnungspreismethoden	451
1.1	Preisvergleichsmethode	451
1.2	Wiederverkaufspreismethode	452
1.3	Kostenaufschlagsmethode	452
2.	Grundlagen/Dokumentationspflichten	453
2.1	Local File	453
2.2	Master File	454
2.3	Country-by-Country-Reporting (CbCR) und wirtschaftliche Risiken	455
2.3.1	Mitteilungspflicht nach § 138a Abs.1 AO	456
2.3.2	Mitteilungspflicht nach § 138a Abs.3 AO	456
2.3.3	Mitteilungspflicht nach § 138a Abs.4 AO	457
2.3.4	Inhalt des länderbezogenen Berichts	457
2.3.5	Angaben in der Steuererklärung	458
2.3.6	Form und Frist	459
2.3.7	Ordnungswidrigkeit nach § 379 Abs.4 AO und rechtliche Risiken	459
XI.	Steuerliche Behandlung von Strafverteidigerkosten	460
1.	Einkommensteuer	460
2.	Umsatzsteuer	462
2.1	Überblick	462
2.2	Vorlage zum EuGH und Entscheidung des BFH	463
2.3	Praxisfolgen	464
XII.	Checkliste für Ihre steuerliche Compliance	465

I. Umweltrecht	467
I. Einführung	467
II. Rechtsquellen der Compliance-Anforderungen im Umweltrecht	468
III. Der Umweltschutzbeauftragte	469
1. Allgemeines	469
2. Gesetzliche Vorgaben an Umweltschutzbeauftragte	470
2.1 Immissionsschutzbeauftragter (§§ 53 ff. BImSchG/5. BImSchV)	471
2.1.1 Bestellung des Immissionsschutzbeauftragten	471
2.1.2 Unterstützungspflicht des Anlagenbetreibers	471
2.1.3 Fachkunde des Immissionsschutzbeauftragten	471
2.1.4 Zuverlässigkeit des Immissionsschutzbeauftragten	472
2.1.5 Fortbildungspflicht des Immissionsschutzbeauftragten	472
2.1.6 Aufgaben (Beratungs- und Hinweisfunktion) des Immissionsschutzbeauftragten	472
2.1.7 Beteiligungspflicht des Anlagenbetreibers	473
2.1.8 Benachteiligungs- und Kündigungsverbot	474
2.2 Störfallbeauftragter (§§ 58a ff. BImSchG/5. BImSchV)	474
2.3 Gewässerschutzbeauftragter (§§ 64 ff. Wasserhaushaltsgesetz)	475
2.4 Abfallbeauftragter (§§ 59, 60 Kreislaufwirtschaftsgesetz)	476
2.5 Strahlenschutzbeauftragter (§§ 31 ff. Strahlenschutzverordnung/§§ 13 ff. Röntgenverordnung)	477
2.6 Ämterhäufung	478
2.7 Erleichterungen bei auditierten Unternehmen	478
2.8 Kurzüberblick über die Haftung der Umweltbeauftragten	479
2.8.1 Strafrechtliche Verantwortlichkeit	480
2.8.2 Zivilrechtliche Verantwortlichkeit	480
3. Resümee und Ausblick	480
J. Produktsicherheit und Produkthaftung	481
I. Einführung	481
II. Produktsicherheit	482
1. Maßgebliche Normen	482
2. Anwendungsbereich des ProdSG	482
2.1 Adressaten	483
2.2 Produktbegriff	483
2.3 Inverkehrbringen	484
3. Pflichten und Compliance	485
3.1 Pflichten beim Inverkehrbringen	485
3.1.1 Gewährleistung der Sicherheit	485
3.1.2 Information der Anwender	490
3.2 Pflichten nach dem Inverkehrbringen: Produktbeobachtungs- und Rückruffpflichten	491
3.2.1 Produktbeobachtungspflicht	491
3.2.2 Notwendige Konsequenzen bei Entdeckung neuer Produktrisiken	494
3.2.3 Behördliche produktsicherheitsrechtliche Anordnungen	497

4. Besondere Pflichten der Unternehmensleitung	499
5. Rechtsfolgen der Non-Compliance	500
III. Produkthaftung	501
1. Maßgebliche Normen	501
2. Anwendungsbereich	502
3. Pflichten und Compliance	504
3.1 Pflichten beim Inverkehrbringen	504
3.1.1 Der Konstruktionsfehler (Compliance mit Konstruktionspflichten)	505
3.1.2 Der Fabrikationsfehler (Compliance mit Fabrikationspflichten)	508
3.1.3 Der Instruktionsfehler (Compliance mit Instruktionspflichten)	508
3.2 Pflichten nach dem Inverkehrbringen	511
4. Rechtsfolgen der Non-Compliance	513
IV. Zusammenfassung	515
K. Compliance als Instrument nachhaltigen Vertriebs	515
I. Einführung	515
II. Risk Assessment	516
III. Analyse des Vertriebsprozesses	517
1. Vertriebserlaubnisse	518
1.1 Allgemeines	518
1.2 Sonderfall Finanzwirtschaft	519
1.2.1 Vertriebspartner	519
1.2.2 Vertriebserlaubnisse und Risikomanagement	524
2. Verkaufsbezogene Verhaltenspflichten	524
2.1 Versicherungsvertrieb	525
2.1.1 Vermittler	525
2.1.2 Versicherungsunternehmen	525
2.2 Exkurs Kapitalmarktvertrieb	527
3. Vertriebssysteme	529
3.1 Handelsvertreter	530
3.1.1 Handelsvertretervertrag	530
3.1.2 Handelsvertreter und Scheinselbstständigkeit	531
3.1.3 Compliance-Pflichten gegenüber dem Handelsvertreter ..	533
3.2 Franchising	535
3.2.1 Compliance im vorvertraglichen Stadium	536
3.2.2 Compliance im laufenden Franchiseverhältnis	537
3.2.3 Compliance nach Vertragsbeendigung	537
3.3 Vertragshändler	538
3.4 Compliance-relevante Gestaltungen in Vertriebsverträgen	539
3.4.1 Kartellverbote	539
3.4.2 Compliance-Klauseln	542

4. Sales Compliance	544
4.1 Werbung	545
4.2 Marketingformen	545
4.2.1 E-Mail-Werbung	545
4.2.2 Telefonakquise	547
4.2.3 Moderne Akquisemethoden	549
4.3 Compliance-Aktivitäten zur Risikominimierung	550
5. Hospitality Compliance	551
5.1 Wesen der Korruption	551
5.2 Rechtsfolgen der Korruption	552
5.3 Risikoanalyse	552
5.4 Maßnahmen der Korruptionsbekämpfung	553
5.4.1 Verbindliches Richtlinienwesen	553
5.4.2 Sanktionierung von Verstößen	554
5.4.3 Compliance Audits	555
5.4.4 Business Partner Screenings	555
6. Compliance im Export	556
6.1 Rahmenbedingungen	556
6.2 Exportkontrolle	557
6.2.1 Handelsgegenstandsbezogene Restriktionen	557
6.2.2 Empfängerbezogene Restriktionen	558
6.2.3 Länderbezogene Restriktionen	559
3.1 Compliance-Maßnahmen in der Außenwirtschaft	560
6.3.1 Ausfuhrverantwortlicher und Exportkontroll- beauftragter	560
6.3.2 Zollrechtliche Besonderheiten	561
6.3.3 Compliance-Organisation	561
IV. Fazit	562
L. Anti Financial Crime – Risikobereiche für Kreditinstitute	562
I. Überblick über etablierte Elemente der Anti Financial Crime (AFC)-Prävention	563
II. Aktuelle Herausforderungen der AFC-Prävention	566
III. Know Your Customer (KYC)	571
IV. Verdachtsmeldewesen	572
V. Transaction Monitoring	574
VI. Transaktionen ohne eigenen Kunden	575
VII. Gefährdungsanalyse	576
VIII. Organisation und Prozesse	577
IX. Zentrale Stelle § 25h KWG	578
X. Three Lines of Defence	579
XI. Investigation by Incidents	580
XII. Was darf eine AFC-Organisation kosten?	581
XIII. Fazit	582
XXX	

5. Kapitel

Risikomanagement und Umgang mit besonderen Risikosituationen

A. Datenschutz im globalen Konzern	583
I. Einführung	583
II. Bestimmung und Management von Datenschutzrisiken	584
1. Bestimmung der Risikofaktoren	585
1.1 Geschäftskontext	586
1.2 Auswirkung für die Betroffenen	586
1.3 Handelnde Personen	586
1.4 Externe Faktoren	586
1.5 Kontrollumgebung	587
1.6 Erfahrung mit aufgetretenen Vorfällen	587
1.7 Bewertungsmaßstäbe	587
2. Klassifizierung der zu verarbeitenden Daten	588
2.1 Personenbezug	589
2.2 Besonders schützenswerte personenbezogene Daten	589
2.3 Informationswert und Vertraulichkeit der Daten	590
2.4 Unkritische und öffentlich zugängliche Daten	590
3. Einordnung der betroffenen Systeme, Anwendungen und Prozesse	590
3.1 Datenschutzrelevante Systeme und Anwendungen	591
3.2 Verfahrensübersicht	591
4. Festlegung angemessener Schutz- bzw. Vorsorgemaßnahmen	591
4.1 Risikobewertung und Angemessenheit des Schutzes	592
4.2 Regelmäßige Risikoüberprüfung	592
4.3 Durchführung von „Privacy Impact Assessments“	593
III. Konzerndatenschutz	593
IV. Anzuwendende Gesetze und Anforderungen	595
V. Globale Datenschutz-Prinzipien	596
VI. Datenschutzrichtlinien mit internationaler Ausprägung	598
1. Anwendung globaler Datenschutzprinzipien und Grundsätze	599
2. Nationale, supranationale und regulatorische Besonderheiten	601
VII. Risikosituation „Datentransfer in Länder ohne angemessenes Datenschutzniveau“	602
VIII. Datensicherheit als Bestandteil des Datenschutzes	605
IX. Ausblick	606
B. IT/elektronische Kommunikation	608
I. Einführung	608

II.	Quellen für IT-Compliance-Anforderungen	609
1.	Pflichtenkreis der Geschäftsleitungen als Beispiel für eine Rechtsquelle	609
1.1	IT-Risikomanagement als Geschäftsleiterpflicht	609
1.2	Pflichtendelegation als Organisationspflicht	610
1.3	Rechtsfolgen bei Verstoß gegen Geschäftsleiterpflicht	610
2.	IT-Compliance-Anforderungen aus geschäftlichen Anforderungen des Unternehmens	611
3.	Kernhandlungsfelder	611
III.	IT-Sicherheit	613
1.	Begriff der IT-Sicherheit	614
2.	Standards für IT-Sicherheit	615
2.1	IT-Grundschutz-Katalog des BSI	616
2.2	ISO-Norm 17799/27002	616
2.3	Referenzmodelle: CobiT und ITIL	617
3.	Konkrete Sicherheitsmaßnahmen	617
IV.	Elektronischer Rechts- und Geschäftsverkehr	618
1.	Rechtsverbindliche elektronische Kommunikation	619
2.	Enterprise Content Management	620
3.	Geschäftsprozessmanagement: Gestaltung von betrieblicher Kommunikation unter Einhaltung von formal-inhaltlichen Anforderungen	621
V.	Geschäftsprozessmanagement: Elektronische Buch- und Aktenführung	622
1.	Grundsätze für IT-gestützte Buchführungssysteme	622
2.	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen	623
VI.	Lösungskategorie Schulungen	624
VII.	Branchenspezifische Anforderungen	627
1.	Banken- und Finanzdienstleistungsunternehmen	627
2.	Zuverlässigkeitsüberprüfungen nach § 7 LuftSiG	628
VIII.	IT-Compliance im Rahmen der Abschlussprüfung	629
1.	IDW Prüfungsstandard 330	629
2.	SOX 404/Euro-SOX	630
IX.	Vertragliche Compliance/Software Asset Management	630
C.	Hinweisgebersysteme zur Identifikation von Compliance-Verstößen	631
I.	Einleitung	631
1.	Herkunft und Definition	631
2.	Erscheinungsformen des Whistleblowings	632
3.	Begriff des Hinweisgebersystems	632

II.	Rechtsrahmen für Hinweisgebersysteme	633
1.	Sarbanes-Oxley Act und Dodd-Frank Act	633
1.1	Regelungssystem des Sarbanes-Oxley Acts	633
1.2	US Dodd-Frank Act	634
1.3	Anwendbarkeit der US-Regelungen auf Unternehmen in Deutschland	635
2.	UK Bribery Act	635
3.	Gesetzgebung zu Anti-Korruption in Frankreich – Sapin II	636
4.	Rechtspflicht zur Einrichtung eines Hinweisgebersystems nach deutschem Recht	636
5.	Weitere Erwägungen bzgl. der Einführung von Hinweisgebersystemen	637
III.	Ausgestaltung von Hinweisgebersystemen	639
1.	Vorgaben und Leitlinien für die Ausgestaltung von Hinweisgebersystemen	639
1.1	Gesetze	640
1.2	Internationale Institutionen und Beratungsgesellschaften	641
1.3	Literatur	644
2.	Interne Lösungen vs. Outsourcing	645
IV.	Rechtslage und -entwicklung in Deutschland	646
1.	Aktuelle Rechtslage	646
1.1	Strafrechtliche Risiken	646
1.1.1	Verrat von Geschäfts- und Betriebsgeheimnissen (§ 17 UWG)	646
1.1.2	Verletzung von Privatgeheimnissen (§ 203 StGB)	647
1.1.3	Weitere Straftatbestände im Zusammenhang mit der Verletzung von Geheimnissen	648
1.1.4	Falsche Verdächtigung (§ 164 StGB)	648
1.1.5	Ehrverletzungsdelikte (§§ 185 ff. StGB)	649
1.2	Arbeitsrechtliche Aspekte	649
1.3	Datenschutzrechtliche Aspekte	651
2.	Rechtsentwicklung in Deutschland	654
2.1	Hinweisgeberschutz in Deutschland	654
2.2	Ehemalig vorgesehene Änderungen im Datenschutz	655
2.3	EU-Richtlinie zum Schutz von Geschäftsgeheimnissen	655
2.4	EU-Datenschutz-Grundverordnung und Datenschutz-Anpassungs- und -Umsetzungsgesetz	656
D.	Compliance-Due Diligence – dargestellt am Beispiel der Anti-Korruptions-Due Diligence –	657
I.	Warum Compliance-Due Diligence?	657
1.	Normativer und rechtspraktischer Paradigmenwechsel bei der Korruptionsbekämpfung	658
2.	Begriff und Bedeutung der Compliance-Due Diligence	661

II.	Compliance-Due Diligence bei M&A-Transaktionen	663
1.	Planung und Vorbereitung der Compliance-Due Diligence	663
1.1	Ziele der Compliance-Due Diligence	663
1.2	Entscheidung über die Notwendigkeit einer Compliance-Due Diligence	664
1.3	Ermittlung des relevanten Rechtsrahmens	665
1.4	Erstellung eines fokussierten Due Diligence-Planes	665
2.	Durchführung der Compliance-Due Diligence	667
2.1	Praktische Erwägungen	667
2.2	Analyse und Bewertung des Compliance-Programms innerhalb des Zielunternehmens	669
2.3	Ermittlung und Analyse historischer Compliance-Probleme	670
2.4	Ermittlung potentieller Compliance-Probleme	671
3.	Umsetzung der Due Diligence-Ergebnisse	671
3.1	Der Umgang mit aufgedeckten Compliance Problemen vor Vertragsschluss	671
3.1.1	Offenlegung gegenüber Behörden bzw. der Öffentlichkeit	672
3.1.2	Auswirkungen identifizierter Compliance-Probleme auf die geplante Transaktion	673
3.2	Besonderheiten bei der Aufdeckung von Compliance-Problemen zwischen Vertragsschluss und Vertragsvollzug	674
3.3	Das Thema Compliance im Rahmen der Post-Merger Integration	675
4.	Besonderheiten bei Joint Venture-Beziehungen	675
III.	Due Diligence bei Intermediären	677
1.	Planung: Institutionalisierung des Due Diligence-Prozesses	677
2.	Durchführung der Compliance-Due Diligence	678
2.1	Selbstauskunft	678
2.2	Analyse unabhängiger Informationsquellen	678
2.3	Risikobewertung	678
3.	Verwendung von Standardvertragsklauseln	679
4.	Periodische Aktualisierung	680
5.	Compliance-Probleme nach Vertragsschluss	680

6. Kapitel

Compliance und Strafrecht

A.	Unternehmensinterne Untersuchungen in Compliance-Fällen	681
I.	Einführung	681
II.	Definition und Hintergrund	682
III.	Rechtliche Pflicht zur Sachverhaltsaufklärung	684

IV.	Maßnahmen der Informationsgewinnung und deren Zulässigkeit	685
	1. Allgemeine Grundsätze	685
	2. Vorgehensweise	686
	3. Informationsquellen	686
	3.1 Akten und Personalakten	687
	3.2 E-Mails	688
	3.3 Telefonate	689
	3.4 Überwachen und Durchsuchen des Arbeitsplatzes	690
	3.5 Kommunikation und Mitarbeiterbefragungen	690
	3.6 Whistleblower-Hotlines	695
	3.7 Amnestie-Programme	695
V.	Mitwirkung des Betriebsrates	696
VI.	Schutz und Verwertbarkeit der Untersuchungsergebnisse	696
VII.	Kooperation mit Behörden	697
VIII.	Abschluss der Internen Untersuchung	699
B.	Strafbarkeit von Vorständen, Compliance Officern, Mitarbeitern	699
I.	Einführung	699
II.	Einschlägige straf- und ordnungswidrigkeitenrechtliche Tatbestände im Überblick	700
	1. Tatbestände des materiellen Strafrechts	700
	2. Tatbestände des Ordnungswidrigkeitenrechts	701
III.	Grundsätze straf- und ordnungswidrigkeitenrechtlicher Haftung in Unternehmen	702
	1. Haftungsrisiko für die verantwortlich handelnden natürlichen Personen	702
	2. Haftungsrisiko von juristischen Personen und Personenvereinigungen	702
IV.	Strafbarkeit von Vorständen	704
	1. Unmittelbare Täterschaft	704
	2. Strafbarkeit bei arbeitsteiliger Begehungsweise	704
	2.1 Horizontale Ebene	705
	2.2 Vertikale Ebene	705
	3. Strafbarkeit durch Unterlassen	706
	3.1 Allgemeine Erfolgsabwendungspflichten	707
	3.2 Geschäftsherrenhaftung	708
	3.3 Pflicht zur Einführung von Compliance-Programmen	709
	4. Aufsichtspflichtverletzung	710
V.	Strafbarkeit von Compliance Officern	712
	1. Strafbarkeit im Rahmen der Vorbeugung von Regelverstößen	712
	1.1 Unzureichende Intervention	712
	1.2 Informations- und Beratungstätigkeit	713
	2. Strafbarkeit nach Kenntniserlangung von Regelverstößen	713

VI.	Strafbarkeit von Mitarbeitern	714
1.	Deliktsverwirklichung in eigener Person	714
2.	Verhalten bei Kenntniserlangung von Regelverstößen	715
2.1	Recht zur Meldung von Gesetzesverstößen	715
2.2	Pflicht zur Meldung von Gesetzesverstößen	716
C.	Konsequenzen: Bußgelder, Einziehung, Verfall	716
I.	Einführung	716
II.	Bußgelder	717
1.	Begriff und Rechtsnatur der Geldbuße	717
2.	Bemessung der Geldbuße	718
3.	Hinweise zum Verfahren in Bußgeldsachen	718
4.	Bedeutung der Geldbuße im Wirtschaftsleben	719
4.1	§ 30 OWiG als Grundnorm für die Unternehmensgeldbuße	719
4.2	Geldbußen für Aufsichtspflichtverletzungen, § 130 OWiG	721
4.3	Geldbußen gegen natürliche Personen über die Zurechnung nach § 9 OWiG	722
4.4	Geldbuße gegen Unternehmen im Europäischen Wettbewerbsrecht	723
III.	Einziehung und Verfall	724
1.	Verfall	725
2.	Einziehung	728
3.	Sonderregel für Organe und Vertreter	730
4.	Verfahrensrechtliche Hinweise	730

7. Kapitel

Compliance und Aufsichtsrecht

A.	Einführung	733
B.	Corporate Governance	735
I.	Begriff und Rechtsgrundlagen	735
II.	Besonderheiten des Finanzsektors	736
III.	Compliance im Finanzsektor	736
C.	Sektoren	737
I.	Versicherungen	737
1.	Maßgebliche Rechtsgrundlagen der Compliance-Funktion für Versicherungsunternehmen	737
a)	Einführung	737
b)	Versicherungsaufsichtsrechtliche Vorgaben	738
c)	Weitere branchenspezifische und maßgebliche allgemeine Regelungen	738

2. Anforderungen an die Compliance-Funktion bei Versicherungsunternehmen	739
a) Organisatorische Anforderungen	739
b) Inhaltliche Anforderungen an die Compliance-Funktion	739
3. Anforderungen an die Entscheidungsträger	741
a) „Fit and Proper“-Erfordernis nach der Solvency-II-Richtlinie ...	741
b) Zuverlässigkeit	741
c) Fachliche Anforderungen an Geschäftsleiter	741
d) Anforderungen an Mitglieder von Verwaltungs- und Aufsichtsorganen	742
4. Risikomanagement	742
II. Kreditinstitute	744
1. Wichtigste Rechtsgrundlagen der Compliance-Funktion für Institute	744
a) Organisationsanforderungen – § 25a KWG und MaRisk	744
b) Organisationsanforderungen – § 33 WpHG und MaComp	745
c) Compliance-Anforderungen nach den allgemeinen Gesetzen ...	745
2. Anforderungen an die Compliance-Funktion bei Banken und Finanzinstituten	746
a) Anforderungen an die Organisation	746
aa) Aufgaben der Compliance-Abteilung	746
bb) Aufbau der Compliance-Abteilung	747
cc) Konzernweite Compliance-Funktion	748
b) Anforderungen an die Entscheidungsträger	748
aa) Geschäftsleiter	748
bb) Aufsichtsorgan	751
cc) Vergütung der Risikoträger	752
c) Risikomanagement	754
III. Kapitalverwaltungsgesellschaften	759
1. Anforderungen an die Entscheidungsträger	759
a) Anforderungen die Geschäftsleiter	759
aa) Zuverlässigkeit	759
bb) Fachliche Eignung	760
b) Vergütungsregeln	760
aa) Rechtsgrundlagen	760
bb) Erfasster Personenkreis: Identifizierte Mitarbeiter	762
cc) Transparenzpflichten	763
c) Anforderungen an die Unabhängigkeit der Leitungsorgane von Kapitalverwaltungsgesellschaft und Verwahrstelle	763
2. Anforderungen an die Organisation	764
a) Rechtsgrundlagen	764
b) Bestandteile einer ordnungsgemäßen Geschäftsorganisation	765
c) Die Regelungen der Level-2-VO insbesondere zu den Kontrollverfahren	766

d) Zusätzliche Anforderungen an OGAW- und Publikums-AIF-Kapitalverwaltungsgesellschaften	766
aa) Personalorganisation und -entwicklung	766
bb) Anlegerbeschwerdemanagement	767
cc) Erweiterte Informationspflichten gegenüber Privatanlegern	768
3. Risikomanagement (KAMaRisk)	768
a) Grundlagen	768
b) Risikomanagementsystem auf Gesellschaftsebene	770
aa) Risiken, Geschäfts- und Risikostrategie	770
bb) Risikotragfähigkeitsberechnung	770

Anhang

1. Checkliste: Top Ten einer Compliance-Intranetseite	775
2. Muster „Code of Conduct“	776
3. Muster spezielle Compliance Policies	786
a) Datenschutz	786
b) E-Mail-Verkehr	792
c) Aufbewahrung von Dokumenten	794
<i>Stichwortverzeichnis</i>	797