

Compliance im Unternehmen für Dummies

DAS INHALTS- VERZEICHNIS

» Hier geht's
direkt
zum Buch

Auf einen Blick

Über die Autoren	7
Einführung	21
Teil I: Willkommen in der Welt von Compliance	27
Kapitel 1: Was Sie schon immer über Compliance wissen wollten	29
Teil II: Anforderungen an eine funktionierende Compliance ...	67
Kapitel 2: Compliance-Organisation	69
Kapitel 3: Gefahren im Blick behalten: Die Risikoanalyse	83
Kapitel 4: Compliance- und Verhaltensrichtlinien.....	93
Kapitel 5: Kennen Sie Ihren Geschäftspartner?.....	113
Kapitel 6: Compliance im Personalwesen	125
Kapitel 7: Whistleblowing – das Hinweisgebersystem	137
Kapitel 8: Compliance-Kommunikation, Schulung und Unternehmenskultur	169
Kapitel 9: Überwachung und Kontrolle.....	183
Kapitel 10: Compliance-Programm	195
Kapitel 11: Interne und behördliche Untersuchungen.....	201
Teil III: Compliance-Rechtsgebiete mit hohen Risiken	221
Kapitel 12: Korruptionsdelikte und Prävention	223
Kapitel 13: Kartellrecht	255
Kapitel 14: Exportkontrolle und Sanktionslistenprüfung.....	279
Kapitel 15: Geldwäscheprävention und Vermeidung von Terrorismusfinanzierung.....	303
Kapitel 16: Datenschutzrecht.....	331
Kapitel 17: Lieferkettensorgfaltspflichtengesetz	361
Teil IV: Der Top-Ten-Teil	387
Kapitel 18: Zehn falsche Thesen über Compliance.....	389
Kapitel 19: Notfallmanagement – wenn es eng wird	393
Kapitel 20: Zehn Websites rund um das Thema Compliance und Integrität.....	397
Stichwortverzeichnis	401

Inhaltsverzeichnis

Über die Autoren	7
Einführung	21
Über dieses Buch	21
Was dieses Buch nicht will	22
Konventionen in diesem Buch	23
Törichte Annahmen über den Leser	23
Wie dieses Buch aufgebaut ist	24
Teil I: Willkommen in der Welt von Compliance	24
Teil II: Anforderungen an eine funktionierende Compliance	24
Teil III: Compliance-Rechtsgebiete mit hohen Risiken	24
Teil IV: Der Top-Ten-Teil	24
Symbole, die in diesem Buch verwendet werden	25
Wie es weitergeht	25
TEIL I	
WILLKOMMEN IN DER WELT VON COMPLIANCE	27
Kapitel 1	
Was Sie schon immer über Compliance wissen wollten	29
Back to the roots	29
Warum Menschen Wirtschaftsstraftaten begehen	30
Gelegenheit macht Diebe!	31
Motivation aus unterschiedlichen Beweggründen	31
Rechtfertigung – der klassische Selbstbetrug!	31
Das Modell: eine ganz einfache »Betrugsmathematik«	32
Was die Gesetze zu Compliance sagen	33
Gesellschaftsrechtliche Vorschriften	34
Das Ordnungswidrigkeitengesetz (OWiG)	40
Internationale Gesetze einhalten	42
Die Bedeutung von Corporate Social Responsibility (CSR) und Environmental, Social and Governance (ESG): Konzepte für eine nachhaltige Zukunft	52
Und was ist nun die Quintessenz?	64
TEIL II	
ANFORDERUNGEN AN EINE FUNKTIONIERENDE COMPLIANCE	67
Kapitel 2	
Compliance-Organisation	69
Compliance-Verantwortung obliegt der Leitung!	70
Die horizontale Delegation	71
Die vertikale Delegation	71
Wesentliche Anforderungen an eine wirksame Delegation	75

12 Inhaltsverzeichnis

Der (Chief) Compliance Officer (CCO oder CO)	76
Typische Aufgaben des Compliance Officers	76
Anforderungen an einen Compliance Officer	77
Informationsversorgung und Berichtswesen	78
Die Rolle des Aufsichtsrats	79
Organisatorische Besonderheiten für Unternehmen von »öffentlichem Interesse«	81

Kapitel 3 Gefahren im Blick behalten: Die Risikoanalyse

Typische Compliance-Risiken	83
Der Risikomanagementprozess	84
Risikoidentifikation	85
Eine Risikobewertung durchführen	88
Strategien zur Risikosteuerung	89
Risikoüberwachung bringt mehr Sicherheit	91
Risikoberichtswesen und Dokumentation	92

Kapitel 4 Compliance- und Verhaltensrichtlinien

Unwissenheit schützt vor Strafe nicht: den richtigen Pfad abstecken	94
Der Verhaltenskodex (Code of Conduct)	95
Kür oder Pflicht? Wozu ein Verhaltenskodex?	96
Verhaltenskodex ... ja klar, aber wie?	96
Ziehen Sie Ihre Mitarbeiter mit ins Boot!	98
Wann Compliance- und Verhaltensrichtlinien spezifisch definiert sein müssen	98
Welche Themen für Sie wichtig sind	98
Für wen der Kodex gelten muss und für wen nicht	99
Erforderlichkeit von Ergänzungen	100
Typischer Aufbau von Compliance- und Verhaltensrichtlinien	102
Die Einleitung	102
Der Zweck der Richtlinie	102
Anwendungsbereich	102
Begriffsdefinitionen	103
Allgemeine Grundsätze	103
Praxisbeispiele	103
Verweis auf weitere Richtlinien, Leitfäden oder Praxishilfen	103
Benennung von Ansprechpartnern	104
Wichtige Punkte zu Compliance- und Verhaltensrichtlinien	104
Bestandsaufnahme	104
Einfache und klare Sprache	105
Handlungsspielraum festlegen	105
Bekanntmachung von Compliance- und Verhaltensrichtlinien	106
Verhaltens- und Compliance-Richtlinien in ausländischen Tochterunternehmen	107
Beachtung lokaler Gesetze	107
Die richtige Sprache wählen	108

Anpassung von Richtlinien und Dokumentation	108
Der Richtlinienverantwortliche	108
Gültigkeitsdauer	109
Dokumentation	109
Compliance-Richtlinien und der Betriebsrat	110
Mitbestimmungsrechte des Betriebsrats	110
Rechtsfolgen bei Verletzung der Mitbestimmungsrechte	111

Kapitel 5

Kennen Sie Ihren Geschäftspartner? 113

Prüfe, wer sich bindet – die Geschäftspartnerprüfung	113
Ziel einer Geschäftspartnerprüfung	115
Geschäftspartnerprüfung in der Praxis	115
Einordnung in Risikoklassen	115
Wie intensiv Sie prüfen sollten	117
Zeitpunkt und Wiederholung der Überprüfung	120
Wer die Prüfung machen sollte	121
Freigabe- und Entscheidungsprozesse sinnvoll festlegen	121
Compliance-Risiken mit Geschäftspartnern minimieren	122

Kapitel 6

Compliance im Personalwesen 125

Sorgfältige Personalauswahl	125
Umfang und Tiefe der Prüfungsmaßnahmen (Pre-Employment-Screening)	126
Neueinstellung von externen Bewerbern	126
Interne Stellenbesetzungen	129
Personaleinstellung und Einarbeitungsprozess	129
Personal- und Führungskräfteentwicklung	130
Vergütung und finanzielle Anreizsysteme	130
Personal- oder Aufgabenrotation	131
Die Sanktionierung von Fehlverhalten	132
Mögliche Warnsignale für Fehlverhalten	132
Null-Toleranz-Prinzip (Zero Tolerance)	133
Das hat Konsequenzen – Reaktion auf Verstöße	133
»Lessons learned« – der positive Nebeneffekt einer umfassenden Aufklärung	134
Ausscheiden von Mitarbeitern	134
Die Rolle der Personalabteilung	135

Kapitel 7

Whistleblowing – das Hinweisgebersystem 137

Müssen Sie ein Hinweisgebersystem einrichten?	138
Die interne Meldestelle und ihre Aufgaben	140
Aufbau einer internen Meldestelle (§ 14 HinSchG)	141
Anforderungen an die Personen der internen Meldestelle (§ 15 HinSchG) ...	141
Die Aufgaben der internen Meldestelle (§ 13 HinSchG)	142
Dokumentation der Meldungen	149

14 Inhaltsverzeichnis

Die externen Meldestellen	150
Die Aufgaben der externen Meldestellen	151
Welche externen Meldestellen gibt es?	151
Welche Art von Hinweisen fällt eigentlich in den Schutzbereich des HinSchG?	152
Auf welche Personen erstreckt sich der Hinweisgeberschutz?	153
Umfang des Hinweisgeberschutzes	154
Das Vertraulichkeitsgebot	154
Verbot von Repressalien	155
Wenn Unternehmen die Vorgaben des HinSchG nicht erfüllen	156
Da hat der Hinweisgeberschutz seine Grenzen	156
Hier haben Sicherheitsinteressen sowie Verschwiegenheits- und Geheimhaltungspflichten absoluten Vorrang	156
Sonstige Verschwiegenheits- und Geheimhaltungspflichten	157
Der Schritt in die Öffentlichkeit – die Offenlegung von Informationen	157
Hier gibt es keinen Hinweisgeberschutz – die bewusste Falschmeldung	158
Auch diese Personen werden geschützt	159
Meldepflicht für Mitarbeiter	159
Datenschutz und Datensicherheit	161
Herausforderungen an (internationale) Konzerne	162
Ist ein zentrales Hinweisgebersystem in Konzernen zulässig?	162
Sonstige Aspekte in Bezug auf ein wirksames zentrales Hinweisgebersystem	164
Amnestie im Unternehmen	165
Das Ziel eines Amnestieprogramms	166
Grundsätzliche Erwägungen, wie Amnestieprogramme gestaltet sein sollten	166

Kapitel 8	
Compliance-Kommunikation, Schulung und	
Unternehmenskultur	169
Training und Schulung	170
Mögliche Trainings- und Schulungsmaßnahmen	170
Adressatengerechtes Training	171
Fortlaufende Schulungsmaßnahmen	173
Durchführung der Schulungsmaßnahmen	173
Die saubere Dokumentation	174
Interne Compliance-Kommunikation	174
Vorbildfunktion der Unternehmensleitung – der gute Ton von oben (Tone from the Top)	174
Die Rolle des mittleren Managements (Tone from the Middle)	175
Weitere interne Kommunikationsmöglichkeiten	175
Gestaltung der Schulungsinhalte und Kommunikationsmaßnahmen	177
Der Praxisbezug	177
Kreativität ist gefragt!	178
Welche Sprache soll's denn sein?	178

Externe Compliance-Kommunikation.....	178
Gegenüber Geschäftspartnern	178
Gegenüber der Öffentlichkeit.....	179
Kommunikation bei Neueinführung von Compliance	180
Unternehmenskultur – nicht Wasser predigen und Wein trinken	181

Kapitel 9

Überwachung und Kontrolle 183

Fehlverhalten vermeiden und aufdecken	183
Prozessintegrierte Kontrollprinzipien	184
Prozessunabhängige Kontrollmaßnahmen	185
Delegation von Überwachungs- und Kontrollpflichten	186
Umfang und Häufigkeit von Kontrollen – das richtige Maß.....	187
Den Datenschutz nicht aus den Augen lassen!	188
Wie gut funktioniert Ihr CMS?	190
Die Beurteilung der Funktionsfähigkeit	190
Zertifizierungen von Compliance-Management-Systemen	191
Der amerikanische Monitor – was Sie sicher nicht wünschen!	193

Kapitel 10

Compliance-Programm 195

Die richtigen »Zutaten« für Ihr Unternehmen.....	195
Unternehmensspezifische Compliance-Maßnahmen definieren.....	196
»Safran macht den Kuchen gelb!«: das Compliance-Programm.....	198
Compliance bedeutet kontinuierliche Arbeit!	199

Kapitel 11

Interne und behördliche Untersuchungen 201

Interne Untersuchungen	201
Gute Gründe für eine gründliche Sachverhaltsaufklärung	202
Untersuchungsauftrag und Untersuchungseinheit – was macht wer? ...	203
Wie Sie interne Untersuchungen durchführen	204
Datenschutzrechtliche Aspekte – Vorsicht ist geboten!	209
Beteiligung des Betriebsrats.....	214
Zehn goldene Regeln bei behördlichen Durchsuchungen	215
Wenn der Staatsanwalt zweimal klingelt ... sich richtig verhalten	215
Um die Dienstausschüsse bitten	216
Durchsuchungs- und Beschlagnahmebeschluss einsehen und prüfen... ..	216
Die Mitarbeiter informieren	217
Ermittlungsbeamte immer begleiten!	218
Wichtige Geschäftsunterlagen und Datenträger kopieren	218
Die IT-Abteilung informieren	219
Notizen anfertigen – unbedingt erforderlich!	219
Widerspruch gegen die Beschlagnahme von Unterlagen und Dateien einlegen	219
Der Abschluss der Durchsuchung	220

TEIL III COMPLIANCE-RECHTSGEBIETE MIT HOHEN RISIKEN..... 221

Kapitel 12 Korruptionsdelikte und Prävention 223

Eine Hand wäscht die andere?	224
Amtsträgerbestechung	224
Die Bestechungshandlung	225
Die Unrechtsvereinbarung	228
Abgeordnetenbestechung	229
Bestechung und Bestechlichkeit im geschäftlichen Verkehr	230
Unlautere Bevorzugung im Wettbewerb	230
Das Geschäftsherrenmodell	231
Bestechung und Bestechlichkeit im Gesundheitswesen	232
Wo ist die Grenze zwischen Höflichkeit und Korruption?	234
Die Korruption kommt selten allein	236
Untreue – nicht nur in romantischer Beziehung	236
Der Betrug	237
... und in der Regel immer Steuerhinterziehung	237
Korruptionstypologien und »Red Flags«	237
Kick-Back-Zahlungen	238
Schwarze Kassen	238
Red Flags – besser mal genauer hinsehen	240
Korruption im internationalen Kontext	242
Die verschiedenen Amtsträgerbegriffe	242
Die Gefahr bei Beschleunigungszahlungen (Teil II)	244
Bestechung durch Mitarbeiter von ausländischen Tochterfirmen an Nicht-Amtsträger	245
Niemals Korruption – außer im absoluten Notfall	246
Spenden und Sponsoring	247
Korruptionsprävention im Unternehmen	248
Sanktionen	252
Ein kleiner Denkanstoß zum Schluss	253

Kapitel 13 Kartellrecht 255

Kartellrecht – was ist das?	256
Das Kartellverbot	257
Was unter Vereinbarungen und abgestimmte Verhaltensweisen fällt ...	257
Nur was »spürbar« ist, wird vom Kartellverbot erfasst	258
Effizienzgewinne – die Ausnahme vom Kartellverbot	259
Absolute Tabuzone – Hardcore-Verstöße	261
Und auch das ist ein »No-Go«!	262
Hier ist Vorsicht geboten!	263
Der erlaubte und der kritische Informationsaustausch	267
Kartellrechtlich kritisch: Unternehmen kaufen oder verkaufen	269
Missbrauch einer marktbeherrschenden Stellung	271
Wann beherrscht ein Unternehmen den Markt?	272
Was ein marktbeherrschendes Unternehmen nicht tun darf	273

Sanktionen, Bußgelder und sonstige Konsequenzen.	274
Bußgeld – es muss weh tun, bevor Umdenken einsetzt	274
Heute ist Zahhtag – Schadensersatzklagen von Geschädigten	276
Was sonst noch drohen kann	277
Das Kind ist im Brunnen – was tun bei Verstößen?	277

Kapitel 14

Exportkontrolle und Sanktionslistenprüfung 279

Die Ziele der Exportkontrolle.	280
Exportkontrolle – Basiswissen für Sie als Unternehmer!	280
Was darf ich ausführen oder verbringen, was nicht?	281
Rüstungsgüter	281
Güter mit »doppeltem Verwendungszweck« (Dual-Use)	282
Der Genehmigungsantrag	287
Organisatorische Anforderungen an die Exportkontrolle.	289
Organisation ist alles	290
Das richtige Personal bestellen	290
Schulung, Schulung und nochmals Schulung	291
Überwachung und Kontrolle	291
Kurze Randnotiz – der »Ermächtigte Ausführer«.	292
Embargos und Anti-Terror-Verordnungen der EU	292
Verschiedene Arten von Embargos	293
Anti-Terror-Verordnungen der EU oder Sanktionslisten	294
Exportkontrolle und Terrorlisten der USA.	297
Wann liegt ein US-Gut vor?	297
Die Commerce Control List (CCL) der USA	298
Die Export Control Classification Number (ECCN) der USA	298
Die Bedeutung von Embargos und Sanktionslisten nach US-Recht	299
Verstöße gegen Exportkontrollvorschriften und Sanktionslisten.	302

Kapitel 15

Geldwäscheprävention und Vermeidung von

Terrorismusfinanzierung 303

Die drei Waschvorgänge für illegale Einnahmen	304
Platzierungsphase (Placement)	305
Umschichtungsphase (Layering)	306
Integrationsphase (Integration)	307
Geldwäschebekämpfung und Vermeidung der Terrorismusfinanzierung – das Geldwäschegesetz (GwG)	307
Wer muss und wer nicht? – Die glorreichen 16 »Verpflichteten«.	308
Allgemeines Risikomanagement	309
Die Risikoanalyse (§ 5 GwG)	310
Erkenntnisse der Risikoanalyse – interne Sicherungsmaßnahmen	312
Allgemeine Sorgfaltspflichten	313
Die Identifizierung – wen, wie und wann?	314
Der Einfluss von Macht – politisch exponierte Personen.	319
Wo es Allgemeines gibt, existiert auch das Besondere	320
Vereinfachte Sorgfaltspflichten	320
Verstärkte Sorgfaltspflichten	321

Dokumentation nicht vergessen!	322
Des einen Freud, des andren Leid – das Transparenzregister	322
Das ist doch faul – Meldepflicht bei Verdachtsfällen	325
Verstöße gegen das GwG – immer ein teurer Spaß	327
Hohe Sanktionen	328
Den Übeltäter bloßstellen – die »Prangervorschrift«	328
Ein gut gemeinter Rat zum Schluss	328

Kapitel 16

Datenschutzrecht 331

Das Datenschutzgesetz	332
Das Marktortprinzip	332
Verantwortliche und betroffene Personen nach dem Datenschutzrecht	332
Personenbezogene Daten	332
Die Verarbeitung	333
Unter welchen Voraussetzungen dürfen Sie Daten verarbeiten?	334
Die Erlaubnistatbestände der DSGVO	334
Ergänzungen durch das BDSG: was geht, was geht nicht?	336
Transparenz- und Informationspflichten	337
Welche Informationen müssen Sie den betroffenen Personen liefern?	338
Wie und wann müssen Sie die Informationen bereitstellen?	342
Ausnahmen von der Informationspflicht	342
Die »Datenschutz-Folgenabschätzung«	345
Wann genau besteht ein hohes Risiko?	345
Worin besteht eine DSFA?	346
Der Datenschutzbeauftragte	346
Die Aufgaben des Datenschutzbeauftragten	347
Wen kann ich als DSB bestellen?	348
Die besondere Stellung des DSB im Unternehmen	348
Besondere Rechte der betroffenen Personen	349
Auftragsdatenverarbeitung	353
Der Auftragsverarbeiter	353
Gemeinsame Verantwortliche – Joint Controller	355
TOM ist gefragt	355
Verzeichnis von Verarbeitungstätigkeiten	357
Inhalt des Verzeichnisses	357
Rechtsfolgen bei Nichtführung eines Verzeichnisses	358
Datenpannen-Meldepflicht	358
Bußgelder und Sanktionen	358
Die Herausforderung an Compliance	359
Datenübermittlung in Drittländer	360

Kapitel 17

Lieferkettensorgfaltspflichtengesetz 361

Was ist das LkSG und warum brauchen wir es?	361
Diese Unternehmen müssen handeln – der Anwendungsbereich des LkSG	362
Bestimmung der Beschäftigtenzahl – eine einfache Rechenmethode	362
Mitarbeiter von Tochtergesellschaften	363

Die geschützten Menschenrechte und Umweltbelange	364
Menschenrechtliche Risiken	365
Umweltbezogene Belange	365
Hätte, hätte, Lieferkette – was ist eigentlich die »Lieferkette«?	366
Das gehört zum »eigenen Geschäftsbereich«	367
Die »unmittelbaren Zulieferer«	367
Die »mittelbaren Zulieferer«	368
Die neun Gebote des LkSG – Sorgfaltspflichten von Unternehmen	368
Ermittlung und Bewertung von Gefahren – das Risikomanagement und regelmäßige Risikoanalysen	369
Ergebnisse der Risikoanalyse an wichtige Stellen weitergeben	372
Bestimmung, wer im Haus was macht – die betriebsinterne Zuständigkeit.	372
Grundsatzerklärung – klare Ansage von oben	373
Präventionsmaßnahmen verankern.	374
Präventionsmaßnahmen im eigenen Geschäftsbereich	374
Präventionsmaßnahmen gegenüber unmittelbaren Zulieferern	376
Hier müssen Sie einschreiten – Abhilfemaßnahmen ergreifen.	378
Es ist ein Beschwerdeverfahren einzurichten	380
Umsetzung von Sorgfaltspflichten in Bezug auf Risiken bei mittelbaren Zulieferern.	382
Dokumentations- und Berichtspflichten.	383
Jährlich und ad hoc »grüßt das Murmeltier« – regelmäßige und anlassbezogene Überprüfung der Wirksamkeit von Sorgfaltspflichten ...	384
Wer nicht folgt, muss mit Folgen rechnen – Konsequenzen bei LkSG-Verstößen	384
Die Rolle des BAFA.	384

TEIL IV DER TOP-TEN-TEIL..... 387

Kapitel 18 Zehn falsche Thesen über Compliance..... 389

Compliance ist doch nur etwas für Großkonzerne!	389
Wir brauchen keine Compliance, unsere Mitarbeiter begehen keine Verstöße! ...	390
Compliance bringt keinen Mehrwert und kostet nur unnötig Geld!	390
Meinen Verstoß bekommen die Behörden doch gar nicht mit!	390
Ein Verstoß wird schon nicht so teuer werden	390
Uns kann nichts passieren, wir haben uns ja rausgehalten!	391
Compliance ist doch nur ein Geschäftsverhinderer!	391
Ein Hinweisgebersystem (Whistleblowing System) fördert nur das Denunziantentum!	392
Ein funktionierendes Compliance-Management-System verhindert alle Verstöße.	392
Wegen Compliance müssen wir die Finger von Risikogeschäften lassen.	392

Kapitel 19 Notfallmanagement – wenn es eng wird..... 393

Notfall – ja, aber welcher?	394
In der Kürze liegt die Würze.	394

20 Inhaltsverzeichnis

Tatütata – das Notfallteam ist da	394
Auch Notfallteams haben Urlaub – die Stellvertretung	395
Informations- und Meldepflichten	395
Unterlagen sind gefragt	395
Kommunikationsregeln	395
Schulung des Notfallteams	396
Aktualisieren Sie den Notfallplan	396
Übung macht den Meister	396

Kapitel 20

Zehn Websites rund um das Thema Compliance

und Integrität..... 397

Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA).....	397
Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)	398
Bundeskartellamt	398
Berufsverband der Compliance-Manager (BCM)	398
Deutsches Institut für Compliance e.V.	398
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI).....	399
Forum Compliance & Integrity.....	399
Konstanz Institut für Corporate Governance (KICG).....	399
Transparency International Deutschland e.V.....	400
UN Global Compact.....	400

Stichwortverzeichnis..... 401