

# Inhalt

Vorwort	— V
Abkürzungsverzeichnis	— XXXI
Literaturverzeichnis	— XLIII
Bearbeiterverzeichnis	— LIII
Rechtsprechungsübersicht	— LIX

## Kapitel 1

<b>Unternehmensorganisation, Risikomanagement, Compliance-Management</b>	<b>— 1</b>
--------------------------------------------------------------------------	------------

## Kapitel 2

<b>Implementierung eines Compliance-Management-Systems</b>	<b>— 9</b>
------------------------------------------------------------	------------

A.	Einleitung	— 9
B.	Definition des Compliance-Management-System-Begriffs und Bedeutung für den Mittelstand	— 10
C.	Motive für die Implementierung eines Compliance-Management-Systems	— 13
I.	Selbstverständnis und Compliance-Kultur	— 13
II.	Auftragserlangung und Anforderungen von Dritten	— 14
III.	Haftungsvermeidung und Reputationssicherung	— 15
D.	Herausforderungen bei der Umsetzung	— 16
E.	Unternehmerische Verantwortung	— 16
F.	Compliance-Kompaktanalyse	— 17
G.	Compliance und Risikomanagement	— 18
I.	Compliance-Risiken	— 18
1.	Gefährdungsanalyse	— 18
2.	Risikomatrix	— 19
II.	Definition relevanter Leitsätze und Compliance-Ziele	— 20
1.	SMARTe Leitsätze	— 20
2.	Definition einer Vision	— 22
3.	Mission und Unternehmensumfeld	— 22
4.	Unternehmensleitbild	— 23
III.	Unternehmensprozesse und -organisation	— 23
1.	Aufbauorganisation	— 23
2.	Ablauforganisation	— 24
H.	Compliance-Abteilung und Compliance-Manager	— 25
I.	Compliance-Abteilung bzw. zuständige Abteilungen	— 25
II.	Funktion eines Compliance-Managers	— 26
1.	Allgemeine Funktionen	— 26
2.	Anforderungen an Compliance-Manager	— 27

- I. Mechanismen zur Sicherstellung der Einhaltung der Regeln – IT-gestütztes Feedbacksystem — **28**
- J. Notfallplan — **29**
- K. Checkliste — **29**

### **Kapitel 3**

#### **Risikomanagement in kleinen und mittleren Unternehmen — 31**

- A. Überblick — **31**
  - I. Jedermann ist Risikomanager — **31**
  - II. Ökonomische Vorteile des Risikomanagements — **31**
  - III. Gesetzliche Pflichten zum Umgang mit Risiken — **32**
- B. Risikoarten — **34**
- C. Risikomanagement — **39**
- D. Risikomanagementprozess — **41**
  - I. Strategisches Risikomanagement — **42**
  - II. Systematische Risikoidentifikation und Risikokommunikation — **43**
    - 1. Grundsätze der Risikoidentifikation — **43**
    - 2. Umsetzungshilfen der Risikoidentifikation — **45**
    - 3. Grundsätze und Umsetzungshilfen der Risikokommunikation — **49**
  - III. Risikobewertung und Risikoaggregation — **50**
    - 1. Bewertung der einzelnen Risiken — **50**
      - a) Qualitative Methoden der Risikobewertung — **50**
        - aa) Klassifizierung der Risiken anhand einer ABC-Analyse — **50**
        - bb) Qualitative Risk-Map — **51**
      - b) Quantitative Methoden der Risikobewertung — **52**
        - aa) Erwartungswerte verschiedener Szenarien und Sensitivitätsanalyse — **52**
        - bb) Quantitative Risk-Map — **54**
      - c) Quantitative Risikomaße — **55**
        - aa) Value-at-Risk und andere „at-Risk-Kennzahlen“ — **55**
        - bb) Risikoorientierte Performancekennzahlen — **58**
      - d) Risikoabhängigkeiten: Aggregation der einzelnen Risiken zum Gesamtrisiko — **60**
  - IV. Risikosteuerung und Risikokontrolle — **62**
    - 1. Risikosteuerung — **62**
    - 2. Zu tragendes Restrisiko und Risikokapital — **62**
      - a) Risikosteuerungsmaßnahmen — **63**
      - b) Risikoüberwachung — **65**
      - c) Risikodokumentation — **66**
- E. Prüfung von Risikomanagementsystemen — **66**

**Kapitel 4****Compliance – Begriff, Entwicklung, Funktion — 69**

- A. Einleitung — **69**
- B. Der Begriff Compliance — **71**
  - I. Die wörtliche Übersetzung als Anhaltspunkt — **71**
  - II. Compliance in der Medizin — **71**
  - III. Enges Verständnis von Compliance — **72**
  - IV. Weites Verständnis von Compliance — **74**
  - V. Compliance als Managementfunktion — **77**
- C. Die historische Entwicklung von Compliance — **78**
  - I. Die Entwicklung in den USA — **79**
  - II. Ausstrahlung auf Europa — **80**
  - III. Compliance: In Europa nichts Neues! — **83**
- D. Rechtliche Verpflichtung zur Errichtung einer Compliance-Funktion — **85**
  - I. Ausdrückliche gesetzliche Vorgabe nur in Einzelfällen — **85**
  - II. Allgemeine Verpflichtung zur Einrichtung einer Compliance-Funktion? — **86**
    - 1. Generelle Verpflichtung zur Einrichtung einer Compliance-Funktion? — **87**
    - 2. Keine Verpflichtung zur Einrichtung einer Compliance-Funktion? — **88**
    - 3. Einzelfallabhängige Pflicht zur Einrichtung einer Compliance-Funktion? — **89**
  - III. Zwischenfazit — **90**
- E. Funktion von Compliance — **98**
  - I. Schutzfunktion von Compliance — **99**
  - II. Image- bzw. Reputationsfunktion von Compliance — **104**

**Kapitel 5****Kernelemente eines Compliance-Management-Systems — 107**

- A. Einleitung — **107**
- B. Compliance-Kultur — **112**
- C. Organisatorische Ausgestaltung — **113**
  - I. Verantwortlichkeitszuordnung — **113**
  - II. Organisatorische Lösungen — **115**
  - III. Aufgaben, Qualifikationen und Rechtsstellung des Compliance-Verantwortlichen — **123**
    - 1. Aufgaben — **124**
      - a) Beratung/Beratungspflicht — **124**

- b) Entwicklung und Umsetzung interner Regelwerke — **125**
      - c) Schulungen und Informationen — **125**
      - d) Kontrolle und Aufdeckung — **125**
      - e) Berichtspflicht — **126**
    - 2. Qualifikation — **127**
    - 3. Rechtsstellung — **129**
  - IV. Auslagerung — **133**
    - 1. Die Zulässigkeit — **133**
    - 2. Ausgestaltung — **134**
  - V. Schnittstellen mit anderen unternehmensinternen Organisationseinheiten — **136**
  - VI. Compliance-Audit — **139**
- D. Präventionsmaßnahmen — **141**
  - I. Mitarbeiterhandbuch — **141**
  - II. (Mitarbeiter-)Schulungen — **142**
  - III. Beratungsangebote für Mitarbeiter — **145**
  - IV. Sonstige Präventionsmaßnahmen — **146**
- E. Überwachung/Aufdeckung — **151**
  - I. Überwachung — **152**
  - II. Hinweisgebersysteme (Whistleblowing) — **155**
  - III. Selbstanzeige — **160**
- F. Sanktionen — **161**
  - I. Unternehmensinterne Sanktionen — **162**
  - II. Behördliche Sanktionen gem. § 30, 130 OWiG — **165**
    - 1. Überblick — **165**
    - 2. § 130 Abs. 1 OWiG — **167**
      - a) Normadressaten — **167**
      - b) Erforderliche/zumutbare Aufsichtsmaßnahmen — **169**
      - c) Verstoß gegen betriebsbezogene Pflichten — **170**
    - 3. § 30 OWiG — **171**
      - a) Normadressaten — **171**
      - b) Täterkreis der Bezugstat — **172**
      - c) Bezugstat — **172**
        - aa) Betriebsbezogene Pflicht — **172**
        - bb) Bereicherung — **173**

## **Kapitel 6**

### **Maßnahmen und Regelwerke — 175**

- A. Überblick — **175**
- B. Ethikregeln (Code of Conduct) — **177**

- I. Zielsetzung/Funktion — 177
- II. Wesentliche Regelungsinhalte — 178
- C. Verhalten bei behördlichen Durchsuchungen — 179
  - I. Zielsetzung/Funktion — 179
  - II. Wesentliche Regelungsinhalte — 180
    - 1. Ankunft der Durchsuchungspersonen im Unternehmen — 181
    - 2. Vorbereitung der Durchsuchungsmaßnahmen — 181
    - 3. Durchsuchung von Räumen/Befragung von Personen — 182
    - 4. Versiegelung von Räumlichkeiten — 183
    - 5. Nachbereitung der Durchsuchung im Unternehmen — 183
- D. Beauftragung von externen Dienstleistern und Lieferanten — 184
  - I. Zielsetzung/Funktion — 184
  - II. Wesentliche Regelungsinhalte — 184
    - 1. Anwendungsbereich — 184
    - 2. Schwellenwerte — 185
    - 3. Angebotseinholung — 185
    - 4. Checkliste — 185
    - 5. Überprüfung — 186
    - 6. Dokumentation von Vertragsverhandlungen/Vergabeentscheidung/Beauftragung — 186
    - 7. Verwendung von Musterverträgen — 187
    - 8. Vertragsarchivierung/Vertragscontrolling — 188
- E. Umgang mit Einladungen, Geschenken und sonstigen Vorteilen (sog. Incentive-Richtlinien) — 188
  - I. Zielsetzung/Funktion — 188
  - II. Wesentliche Regelungsinhalte — 190
    - 1. Anwendungsbereich — 190
    - 2. Schwellenwerte — 190
    - 3. Zuwendungsberechtigte — 191
    - 4. Zuwendungsverfahren — 191
    - 5. Registrierung von Zuwendungen/Berichterstattung — 193
    - 6. Verwendung von Sachzuwendungen — 193
    - 7. Checkliste — 193
- F. Umgang mit der Öffentlichkeit — 194
  - I. Zielsetzung/Funktion — 194
  - II. Wesentliche Regelungsinhalte — 194
    - 1. Anwendungsbereich — 194
    - 2. Verantwortlichkeiten — 195
    - 3. Delegation — 195
  - III. Ergänzende Maßnahmen im Krisenfall — 196
  - IV. Litigation-PR — 196

- G. Sonstige praxisrelevante Regelwerke (Übersicht) — 198**
  - I. Unterschriften-/Zeichnungsrichtlinien — 198**
  - II. Telekommunikations-/IT-Richtlinien — 198**
  - III. Richtlinien zum Umgang mit Dokumenten (sog. Clean Desk Policy) — 199**
  - IV. Verhaltensregeln für einzelne operative Einheiten — 199**
  - V. Grundsätze zur Wahrnehmung von Nebentätigkeiten — 200**
  - VI. Spenden-/Sponsoring-Richtlinie — 200**
  - VII. Richtlinie zur Durchführung interner Ermittlungen — 201**
  - VIII. Richtlinie zur Geldwäscheprävention — 202**

## **Kapitel 7**

### **Compliance in der Abschlussprüfung — 205**

- A. Überblick — 205**
- B. Auswirkungen des Deutschen Corporate Governance Kodex auf die Pflichten des Abschlussprüfers — 206**
- C. Pflichten des Abschlussprüfers im Zusammenhang mit der abzugebenden Entsprechenserklärung — 207**
  - I. Rechtliche Grundlagen der Abgabe und Veröffentlichung der Entsprechenserklärung — 207**
  - II. Bindungswirkung des DCGK — 208**
  - III. Prüfungsgegenstand — 209**
  - IV. Prüfungsdurchführung und Prüfungshandlungen — 210**
  - V. Berichterstattung — 211**
    - 1. Bestätigungsvermerk — 211**
    - 2. Prüfungsbericht — 212**
- D. Abgabe der Unabhängigkeitserklärung nach Nr. 7.2.1 DCGK — 213**
  - I. Inhalt der Erklärung — 214**
    - 1. Angaben zu geschäftlichen, finanziellen, persönlichen und sonstigen Beziehungen — 214**
    - 2. Honorarangaben — 215**
  - II. Sonstige Erklärungen — 216**
- E. Auftragsgemäße Erweiterung der Berichtspflichten des Abschlussprüfers nach Nr. 7.2.3 DCGK — 216**
- F. Prüfung von Compliance-Management-Systemen — 216**

**Kapitel 8****Zertifizierung von Compliance-Management-Systemen (IDW PS 980) — 219**

- A. Einführung in die Prüfung eines Compliance-Management-Systems — 219
- B. Die Arten der Prüfung eines CMS — 220
  - I. Konzeptionsprüfung — 221
  - II. Angemessenheitsprüfung — 222
  - III. Wirksamkeitsprüfung — 222
- C. Die Grundlagen eines CMS nach dem IDW PS 980 — 223
- D. Der Sinn und Zweck eines CMS aus Sicht der Wirtschaftsprüfung — 226
  - I. Prüfungsanlässe — 228
    - 1. Hilfestellung bei der Konzeption und Implementierung eines CMS — 228
    - 2. Laufende Qualitätssicherung — 229
    - 3. Objektiver Nachweis der Wirksamkeit eines CMS — 229
    - 4. CMS-Prüfung bei Unternehmenstransaktionen — 230
- E. Kritische Beurteilung der Prüfung des CMS — 230

**Kapitel 9****Absicherung durch Versicherungslösungen — 233**

- A. Überblick — 233
- B. D&O-Versicherung — 234
  - I. Allgemeines — 234
  - II. Gegenstand der Deckung — 235
  - III. Versicherungsnehmer und versicherter Personenkreis — 236
  - IV. Versicherte Haftungstatbestände — 238
    - 1. Innenansprüche — 239
    - 2. Außenansprüche — 241
      - a) Kartellrecht — 241
      - b) Umweltrecht — 242
      - c) Patentverletzung — 244
    - 3. Claims-Made-Prinzip — 245
  - V. Abgrenzung zu sonstigen Versicherungen (sog. Subsidiaritätsklauseln) — 246
  - VI. Ausschlüsse — 247
    - 1. Vorsatzausschluss — 247
    - 2. Keine Deckung im Zusammenhang mit Bestechung, Schenkungen, Spenden oder ähnlichen Zuwendungen — 249
  - VII. Selbstbeteiligung des Leitungsorgans — 250
    - 1. VorstAG — 250

- a) Anwendungsbereich — **250**
- b) Intention des Gesetzgebers — **251**
- c) Verstoß gegen § 93 Abs. 2 S. 3 AktG — **252**
- 2. Die Auswirkungen des VorstAG auf einzelne Vorstandsmitglieder — **253**
  - a) Regelung im Anstellungsvertrag — **253**
  - b) Auslegung von Unklarheiten — **254**
    - aa) Zeitliche Geltung des § 93 Abs. 2 S. 3 AktG — **254**
    - bb) Höhe der Selbstbeteiligung — **254**
    - cc) Mehrfachverstöße — **255**
    - dd) Keine Vergütung in der Tochteraktiengesellschaft — **255**
    - ee) Selbstbeteiligung für Innenansprüche und Kompensation des Schadens — **256**
- VIII. Die Selbstbehaltsversicherung — **257**
  - 1. Anrechnungsmodelle — **258**
  - 2. Selbstbehaltsversicherung ohne Anrechnung (Zusatzsummen-Modell) — **258**
  - 3. Personal-D&O — **259**
  - 4. Empfehlung — **260**
  - 5. Zusammenfassung — **261**
- IX. Versicherungssummen — **261**
- X. Bewertung — **263**
- C. Die Rechtsschutzversicherung — **263**
  - I. Die unternehmensfinanzierte Straf-Rechtsschutzversicherung — **263**
    - 1. Versicherungsgegenstand — **264**
    - 2. Versicherte Kosten — **264**
    - 3. Widerspruchsrecht der Versicherungsnehmerin — **265**
  - II. Die private Straf-Rechtsschutzversicherung — **265**
  - III. Die private Anstellungsvertrags-Rechtsschutzversicherung — **265**
  - IV. Bewertung — **266**

## **Kapitel 10**

### **Arbeitsrecht — 267**

- A. Überblick — **267**
- B. Rechtsgrundlagen für Compliance-Strukturen — **268**
  - I. Arbeitsschutz und Arbeitssicherheit — **268**
    - 1. Allgemeine Fürsorgepflichten — **268**
    - 2. Sicherheit und Gesundheitsschutz — **269**
      - a) Arbeitsschutz — **269**
      - b) Beschäftigungsverbote — **271**



- c) Arbeitssicherheit — **271**
    - d) Weitere Arbeitsschutz- und Unfallverhütungsvorschriften — **272**
  - 3. Gesetzliche Arbeitszeitbeschränkungen — **272**
- II. Sozialversicherung — **273**
  - 1. Abführung der Sozialversicherungsbeiträge — **273**
  - 2. Risikofall Scheinselbstständigkeit — **274**
  - 3. Risiko Phantomlohn — **276**
    - a) Typische Gefahrenquellen für die Entstehung eines Phantomlohnes — **276**
    - b) Rechtsfolgen des Phantomlohns — **278**
- III. Arbeitnehmerüberlassung — **279**
  - 1. Das Transparenzgebot – Vorsicht beim Abschluss von Dienst- und Werkverträgen — **279**
  - 2. Einführung einer Höchstüberlassungsdauer – nicht länger als 18 Monate — **280**
  - 3. Der „equal-pay“-Grundsatz – Zahlung des gleichen Arbeitsentgeltes nach 9 Monaten — **282**
- IV. Betriebsverfassungsrecht — **283**
  - 1. Unmittelbare Relevanz für Compliance — **283**
  - 2. Risikofall Betriebsratsvergütung — **283**
  - 3. Mitbestimmung bei Compliance-Maßnahmen — **285**
- V. Allgemeines Gleichbehandlungsgesetz (AGG) — **286**
  - 1. Schutzzweck des AGG und Relevanz für Compliance — **286**
  - 2. Persönlicher Anwendungsbereich des AGG — **287**
    - a) Geschützte Personen — **287**
    - b) Mögliche Täter und Verantwortliche nach dem AGG — **288**
  - 3. Sachlicher Anwendungsbereich des AGG — **288**
  - 4. Formen der Benachteiligung — **289**
  - 5. Ausnahmen vom Verbot der Benachteiligung — **290**
  - 6. Rechtsfolgen bei Verstößen gegen das Verbot der Benachteiligung durch den Arbeitgeber — **291**
    - a) Beschwerderecht — **291**
    - b) Leistungsverweigerungsrecht — **291**
    - c) Entschädigung und Schadenersatz — **292**
    - d) Unterlassungs- und Beseitigungsanspruch — **294**
    - e) Maßregelungsverbot — **295**
    - f) Information an Betriebsrat und die Antidiskriminierungsstelle des Bundes — **295**
    - g) Unwirksamkeit von Vereinbarungen — **295**
  - 7. Organisationspflichten des Arbeitgebers — **295**
    - a) Stellenausschreibungen — **295**
    - b) Schutzmaßnahmen — **296**

- c) Schulungen — **296**
- d) Beschwerdestelle — **297**
- e) Bekanntmachungspflichten — **297**
- VI. Persönlichkeitsrecht und Datenschutz — **297**
  - 1. Verhaltens- bzw. Ethikrichtlinien — **297**
  - 2. Arbeitnehmerdatenschutz und E-Mail-Überwachung — **298**
- VII. Mindestlohn nach Mindestlohngesetz (MiLoG) — **299**
  - 1. Haftung des Generalunternehmers für Drittunternehmer — **300**
  - 2. Unterschreitung des Mindestlohns stellt Ordnungswidrigkeit dar — **301**
  - 3. Strafbarkeit nach § 266a StGB — **302**
- VIII. Die Arbeitnehmerentsendung nach dem Arbeitnehmerentsendegesetz (AEntG) — **303**
- C. Einführung und Durchsetzung von Compliance-Vorgaben im Unternehmen — **303**
  - I. Einführung durch Direktionsrecht — **304**
  - II. Einführung durch Individualvereinbarung — **305**
  - III. Einführung durch Betriebsvereinbarung — **307**

## **Kapitel 11**

### **Datenschutzrechtliche Compliance — 309**

- A. Einleitung — **309**
- B. Allgemeines zur DS-GVO — **311**
  - I. Zentrale Anforderungen an den Verantwortlichen — **311**
  - II. Zentrale Datenschutzprozesse — **311**
  - III. Zentrale Datenschutzstrukturen — **312**
- C. Umsetzung der Datenschutz-Compliance — **312**
  - I. Datenschutzprozesse — **312**
    - 1. Rechtskonforme Datenverarbeitung — **312**
      - a) Einhaltung der Datenschutzgrundsätze — **313**
      - b) Rechtmäßigkeit der Verarbeitung auf einer Rechtsgrundlage — **317**
        - aa) Datenverarbeitung aufgrund einer Einwilligung — **318**
        - bb) Einwilligung bei Cookies, Analytics und Tracking — **319**
      - c) Transparenz bei Datenerhebung durch Information der betroffenen Person — **322**
        - aa) Inhalt der Informationspflicht gemäß Art. 13 und 14 DS-GVO — **322**
        - bb) Zeitpunkt der Informationspflicht gemäß Art. 13 und 14 DS-GVO — **324**

- cc) Form der Informationspflichten gemäß Art. 13 und 14 DS-GVO — **327**
    - d) Sicherheit der Verarbeitung durch Umsetzung geeigneter technischer und organisatorischer Maßnahmen — **330**
      - aa) Vorgaben in Art. 24 und 32 DS-GVO — **330**
      - bb) Datenschutz-Folgenabschätzung — **331**
    - e) Datenschutzkonforme Auftragsverarbeitung — **333**
    - f) Schutzniveau bei Übermittlung in Drittländer — **334**
    - g) Dokumentation der Verarbeitungstätigkeiten — **334**
  - 2. Sicherstellung der Rechte betroffener Personen — **335**
    - a) Rechte betroffener Personen im Überblick — **335**
    - b) Umsetzung der Rechte betroffener Personen — **336**
      - aa) Auskunft — **336**
      - bb) Löschung — **336**
      - cc) Datenübertragbarkeit — **337**
      - dd) Widerspruch — **338**
      - ee) Sonstige Rechte — **340**
  - 3. Umgang mit Datenschutzverstößen — **340**
- II. Datenschutzstrukturen — **341**
  - 1. Adressaten des Datenschutzrechts — **341**
  - 2. Datenschutzziele — **342**
  - 3. Datenschutz-Governance-Struktur — **343**
  - 4. Datenschutzleitlinie — **344**
- D. Datenschutzdokumentation — **345**
- I. Dokumentation der Datenverarbeitung — **345**
  - II. Dokumentation der Sicherstellung der Rechte betroffener Personen — **346**
  - III. Dokumentation des Umgangs mit Datenschutzverstößen — **347**
  - IV. Nachweiserbringung durch Verhaltensregeln und Zertifizierungsverfahren — **347**
  - V. Verzeichnis von Verarbeitungstätigkeiten als Dokumentationsgrundlage — **348**
- E. Datenschutzbewusstsein und Schulungen — **348**
- I. Schulungen als organisatorische Maßnahme — **348**
  - II. Datenschutzbewusstsein — **349**
  - III. Konkrete Maßnahmen — **349**
- F. Überwachung des Datenschutzes und Rechtsfolgen bei Verstößen — **350**
- I. Aufgaben der Aufsichtsbehörde — **350**
  - II. Befugnisse der Aufsichtsbehörde — **351**
  - III. Anspruch auf Schadenersatz — **352**

**Kapitel 12  
Cyberkriminalität und Cybersicherheit — 355**

- A. Vormerkungen — **355**
- B. Cyberkriminalität im engeren Sinne — **356**
- C. Das Lagebild Cyberkriminalität — **357**
  - I. Das Lagebild des Bundeskriminalamtes — **357**
  - II. Beurteilung der Lage durch Erhebungen von G4C — **358**
- D. Häufig anzutreffende Angriffsarten — **360**
  - I. Schadsoftware „Emotet“ — **360**
  - II. Ransomware — **361**
- E. Status der Sicherheit in Unternehmen und zunehmende Digitalisierung — **364**
- F. Cyber-Abwehr beginnt mit Schulung — **366**
- G. Bedrohungsszenarien — **367**
  - I. Erscheinungsformen — **367**
  - II. Verantwortlichkeiten und Grenzen der Unternehmen — **367**
  - III. Sicherheit: aktive und passive Maßnahmen — **368**
- H. Ransomware: Unternehmen und Institutionen als Zielscheibe — **369**
  - I. Wie gelangt Ransomware in die Unternehmen? — **369**
  - II. Fatale Folgen — **369**
  - III. Neue Gefahren durch gezielte Angriffe — **370**
  - IV. Wie gehen die Täter vor? — **370**
  - V. Varianten der Vollverschlüsselung einschließlich Backups — **370**
  - VI. Welche Maßnahmen schützen effektiv vor Infektionen mit Ransomware? — **371**
  - VII. Welche Maßnahmen können einer gezielten Datenvernichtung vorbeugen? — **373**
  - VIII. Aufbau eines Systems zur Notfallplanung und Krisenvorsorge — **374**
  - IX. Wie können Unternehmen für eine Früherkennung sorgen? — **376**
  - X. Wie ist zu handeln, wenn der Ernstfall eintritt? — **376**
  - XI. Lösegeld: Wie sollten Unternehmen sich verhalten? — **378**
- I. Schlussbemerkungen — **379**

**Kapitel 13  
Kartellrecht — 381**

- A. Überblick — **381**
- B. Bedeutung des Kartellrechts am Beispiel der Energiewirtschaft — **381**
- C. Die Motivation kartellrechtlicher Compliance — **386**
- D. Ziele kartellrechtlicher Compliance — **387**

- E. Grundzüge: Was ist Kartellrecht? Wozu dient es? Was verbietet es?  
Wen betrifft es? — **388**
  - I. Allgemeines — **388**
  - II. Das Kartellverbot — **390**
  - III. Die Missbrauchsverbote — **393**
  - IV. Die Fusionskontrolle — **395**
  - V. Praxisrelevante Fälle von Kartellverstößen — **399**
    - 1. Klassische Kartellabsprachen im Sinne des § 1 GWB — **399**
    - 2. Informationsaustausch — **400**
    - 3. Gestaltung von Verträgen, z.B. langfristige Bezugsbindungen — **402**
    - 4. Verstöße gegen kartellrechtliche Missbrauchsverbote — **404**
    - 5. Verstöße gegen Fusionskontrollvorschriften — **406**
  - VI. Welche Unternehmensbereiche/Personen sind betroffen/gefährdet? — **407**
    - 1. Unternehmensleitung — **407**
    - 2. Handel/Vertrieb — **407**
    - 3. Vertragsmanagement — **408**
- F. Zu den Folgen von Kartellverstößen: Was passiert bei Verstößen gegen das Kartellrecht? — **408**
  - I. Ermittlungs-, Auskunfts- und Beschlagnahmefugnisse — **409**
  - II. Abstellungsverfügungen und einstweilige Maßnahmen — **411**
  - III. Verhängung von Bußgeldern — **413**
    - 1. Bußgelder gegen Unternehmen — **413**
      - a) Bußgeldbemessung — **414**
      - b) Steuerliche Behandlung von Bußgeldern — **415**
    - 2. Bußgelder gegen natürliche Personen — **415**
      - a) Bußgeldbemessung — **416**
      - b) Versicherungsrechtliche Behandlung von Bußgeldern — **416**
  - IV. Vorteilsabschöpfung durch die Kartellbehörden oder durch Verbände — **416**
  - V. Schadenersatz- und Unterlassungsansprüche der Betroffenen nach dem GWB — **417**
    - 1. Private Kartellverfolgung — **417**
    - 2. Bindungswirkung kartellbehördlicher Entscheidungen — **418**
    - 3. Verweis auf Möglichkeiten der Schadensabwälzung im Rahmen der Schadenermittlung (Passing-on-Defense) und Ansprüche indirekter Abnehmer — **419**
    - 4. Kausalität in sog. Umbrella-Pricing-Fällen — **421**
    - 5. Die Verjährung kartellrechtlicher Schadenersatzansprüche — **422**
    - 6. Persönliche Haftung von Geschäftsführern bzw. Unternehmensverantwortlichen — **423**

- VI. Weitere Konsequenzen — **424**
  - 1. Zivilrechtliche Unwirksamkeit kartellrechtswidriger Rechtsgeschäfte — **424**
  - 2. Gesellschafts- und arbeitsrechtliche Konsequenzen — **425**
- G. Hinweise zur kartellrechtlichen Compliance — **426**
  - I. Ausgangspunkt: Bestandsaufnahme und Risikobewertung — **426**
    - 1. Reaktionsmöglichkeiten bei festgestellten Zuwiderhandlungen — **427**
      - a) Der Kartellverstoß wird bislang kartellbehördlich nicht verfolgt — **427**
      - b) Der Kartellverstoß wird bereits kartellbehördlich verfolgt — **428**
    - 2. Bestimmung des relevanten Personenkreises und der wesentlichen Inhalte einer Kartellrechts-Compliance — **429**
  - II. Kartellrechts-Compliance als Aufgabe der Leitungsebene — **429**
  - III. Information und Schulung von Mitarbeitern — **430**
  - IV. Erstellung von Richtlinien bzw. Checklisten — **430**
  - V. Organisatorische Vorkehrungen zur Überwachung — **431**
  - VI. Dokumentation — **432**
  - VII. Umgang mit kartellrechtlich sensiblen Unterlagen — **433**
    - 1. Korrespondenz mit einem externen Anwalt — **433**
    - 2. Korrespondenz mit Syndikusanwälten — **434**

## **Kapitel 14**

### **Energiewirtschaftsrecht und Entflechtungsvorgaben — 437**

- A. Entflechtungsvorgaben des EnWG — **437**
  - I. Überblick — **437**
    - 1. Europarechtliche Grundlagen und die Umsetzung im EnWG — **437**
    - 2. Gesetzliche Ziele der Entflechtungsvorgaben — **438**
    - 3. Stufenfolge der und Ausnahmen von den Entflechtungsvorgaben — **438**
    - 4. Auslegung und Konkretisierung der Entflechtungsvorgaben — **440**
    - 5. Weiterentwicklung der Entflechtungsvorgaben auf europäischer Ebene — **441**
  - II. Vertraulichkeitsvorgaben — **442**
    - 1. Ziele des § 6a EnWG — **442**
    - 2. Vertraulichkeitsgebot, § 6a Abs. 1 EnWG — **443**
      - a) Welche Unternehmen sind verpflichtet? — **443**
      - b) Umfang der Verpflichtung — **444**
      - c) Sicherstellung der Vertraulichkeit im Unternehmen — **445**

3. Verpflichtung zur nichtdiskriminierenden Offenlegung, § 6a Abs. 2 EnWG — **447**
  - a) Welche Unternehmen sind verpflichtet? — **447**
  - b) Umfang der Verpflichtung — **447**
  - c) Sicherstellung der nichtdiskriminierenden Offenlegung — **448**
4. Festlegungen der BNetzA (GPKE, GeLi Gas) — **449**
5. Dokumentation der Geschäftsprozesse — **450**
- III. Buchhalterische Entflechtung — **451**
  1. Ziele des § 6b EnWG — **451**
  2. Umfang der Verpflichtung — **452**
- IV. Rechtliche und operationelle Entflechtung — **454**
  1. Rechtliche Entflechtung — **454**
    - a) Inhalt der Verpflichtung — **454**
    - b) Energierechtliche Umsetzung — **455**
    - c) Arbeitsrechtliche Umsetzung — **458**
  2. Operationelle Entflechtung — **458**
    - a) Bestimmungen zur „personellen Entflechtung“ — **459**
    - b) Auslegungsverständnis der Regulierungsbehörden — **462**
    - c) Kommunikationsverhalten und Markenpolitik — **463**
    - d) Gleichbehandlungsmanagement — **464**
  3. Ausnahmeregelung: De-minimis-Unternehmen — **466**
- B. Zusätzliche grundlegende Verpflichtungen des Energiewirtschaftsrechts — **467**
- C. Checkliste — **469**
  - I. Entflechtungsvorgaben — **469**
    1. Vertraulichkeit, § 6a EnWG — **469**
    2. Buchhalterische Entflechtung, § 6b EnWG — **469**
    3. Rechtliche Entflechtung, § 7 EnWG — **470**
    4. Operationelle Entflechtung, § 7a EnWG — **470**
  - II. Energiewirtschaftsrecht — **470**

## Kapitel 15

### Tax-Compliance-Management-System — 473

- A. Einleitung — **473**
- B. Rechtsrahmen für die Ausgestaltung eines Tax CMS — **474**
  - I. § 153 AO — **474**
  - II. Schreiben des BMF vom 23.5.2016 — **474**
  - III. IDW Praxishinweis vom 31.5.2017 — **476**
  - IV. Rechtsprechung des BGH — **477**
  - V. Start für die Herausbildung einer Best Practice — **478**

- C. Grundüberlegungen — **478**
  - I. Steuerliche Pflichten — **479**
  - II. Management-System — **480**
    - 1. Verantwortung und Zuweisung von Rollen — **480**
    - 2. Umfang — **481**
    - 3. Berichterstattung — **482**
    - 4. Inhalt der Berichterstattung — **482**
    - 5. Risiko-Kontrollmatrix — **483**
    - 6. Überwachung und Verbesserung — **483**
    - 7. Revisions-sicheres System — **483**
  - III. Status quo bei der Umsetzung von Tax CMS — **483**
- D. Zusammenfassung — **486**

## **Kapitel 16**

### **Strom- und energiesteuerrechtliche Compliance — 487**

- A. Einführung — **487**
- B. Steuerliche Pflichten, Überwachung und Sanktionen — **487**
- C. Systematischer Überblick — **490**
- D. Stromsteuerrecht — **491**
  - I. Übersicht zum StromStG — **493**
  - II. Besteuerung des Stroms — **493**
    - 1. Steuerentstehung — **493**
    - 2. Steuerschuldner — **494**
    - 3. Versorgererlaubnis — **495**
    - 4. Pflichten des Versorgers — **496**
    - 5. Stromsteueranmeldung — **497**
  - III. Entnahme steuerbefreiten oder steuerbegünstigten Stroms und Steuerentlastung — **498**
    - 1. Entnahme steuerbefreiten oder steuerbegünstigten Stroms — **499**
      - a) Beantragung und Erteilung der Erlaubnis — **499**
      - b) Pflichten des Erlaubnisinhabers — **500**
    - 2. Stromsteuerbefreiungen — **500**
      - a) Strom aus erneuerbaren Energieträgern — **500**
      - b) Strom zur Stromerzeugung — **502**
      - c) Dezentrale Stromerzeugung und -versorgung — **503**
    - 3. Steuerentlastung für Unternehmen des Produzierenden Gewerbes — **504**
      - a) Unternehmen des Produzierenden Gewerbes — **504**
      - b) Stromentnahme zu betrieblichen Zwecken — **506**



- c) Nutzenergie-Lieferung — **506**
    - d) Allgemeine Entlastung — **507**
  - 4. Spitzenausgleich — **507**
- IV. Übersicht der wichtigsten Fristen aus dem Stromsteuerrecht — **508**
- E. Energiesteuerrecht — **509**
  - I. Besteuerung von Erdgas — **509**
    - 1. Steuertarife — **510**
    - 2. Steuerentstehung („Entnahme zum Verbrauch“) — **510**
    - 3. Keine Steuerentstehung bei anschließender steuerfreier Verwendung — **512**
    - 4. Steuerschuldner — **512**
    - 5. Anmeldung als Lieferer — **512**
    - 6. Pflichten des Lieferers — **514**
    - 7. Erdgassteueranmeldung — **514**
  - II. Steuerentlastungen — **515**
    - 1. Formelle Voraussetzungen der Steuerentlastungen — **515**
    - 2. Energiesteuerentlastungen im Einzelnen — **516**
      - a) Keine Verwendung als Kraft- oder Heizstoff — **516**
      - b) Begünstigte Prozesse und Verfahren — **517**
        - aa) Allgemeine Voraussetzungen — **517**
        - bb) Mineralogische Verfahren — **517**
        - cc) Verfahren der Metallerzeugung und -bearbeitung — **518**
        - dd) Chemisches Reduktionsverfahren — **518**
        - ee) Zweierlei Verwendungszweck (Dual Use) — **519**
      - c) Thermische Abfall- und Abluftbehandlung — **519**
      - d) Stromerzeugung und Kraft-Wärme-Kopplung — **520**
      - e) Energieeinsatz in (hocheffizienten) KWK-Anlagen — **521**
      - f) Begünstigung von Unternehmen des Produzierenden Gewerbes — **523**
        - aa) Allgemeine Steuerentlastung — **523**
        - bb) Spitzenausgleich — **524**
  - III. Exkurs: Biogas — **525**
    - 1. Steuerentstehung — **525**
    - 2. Steuerbegünstigung von Biogas — **526**
  - IV. Übersicht der wichtigsten Fristen aus dem Energiesteuerrecht — **526**
- F. Beihilfenrechtliche Pflichten — **527**
  - I. Energiesteuer- und Stromsteuer-Transparenzverordnung (EnSTransV) — **527**
  - II. Selbsterklärung zu staatlichen Beihilfen (Formular 1139) — **528**

## Kapitel 17

### Gesellschaftsrechtliche Compliance — 529

- A. Systematischer Überblick — 529
- B. Pflichten der Unternehmensleitung — 530
  - I. Organisationspflichten — 531
    - 1. Beachtung des Unternehmensgegenstandes — 531
    - 2. Wahrung der Kompetenzordnung — 532
    - 3. Organisationsverantwortung — 534
    - 4. Besondere Legalitätspflichten — 535
  - II. Informations- und Berichtspflichten — 536
    - 1. Berichtspflichten gegenüber dem Aufsichtsrat — 536
    - 2. Berichtspflichten gegenüber den Anteilseignern — 537
    - 3. Offenlegungspflichten gegenüber der Allgemeinheit — 538
  - III. Unternehmensstrategie – unternehmerisches Ermessen — 539
  - IV. Planung und Finanzierung — 541
    - 1. Planungs- und Finanzverantwortung — 541
    - 2. Insolvenzantragspflicht — 542
  - V. Treuepflichten — 543
    - 1. Begriff und Fallgruppen — 543
    - 2. Insbesondere: Wettbewerbsverbote — 544
    - 3. Pflicht zur Verschwiegenheit — 545
  - VI. Besonderheiten für den GmbH-Geschäftsführer — 548
  - VII. Verbundene Unternehmen — 549
- C. Pflichten des Aufsichtsorgans — 551
  - I. Bildung eines Aufsichtsorgans – Arten — 551
  - II. Persönliche Eignung — 552
  - III. Überwachungspflicht — 552
    - 1. Aufgabendelegation und Organverantwortung — 553
    - 2. Insbesondere: Prüfungsausschuss — 555
    - 3. Gegenstand der Überwachung und Informationspflicht — 555
    - 4. Überwachungsmittel — 556
    - 5. Erfüllung der Überwachungsaufgabe — 557
  - IV. Weitere Pflichten des Aufsichtsrates — 559
    - 1. Einberufung der Hauptversammlung (§ 111 Abs. 3 AktG) — 559
    - 2. Berichts-, Prüfungs- und Mitwirkungspflichten — 560
    - 3. Zustimmungsvorbehalte nach § 111 Abs. 4 AktG — 560
  - V. Treue- und Verschwiegenheitspflicht — 563
    - 1. Loyalität und Bindung an das Unternehmensinteresse — 563
    - 2. Inhalt der Verschwiegenheitspflichten — 564
  - VI. Fakultativer Aufsichtsrat in der GmbH — 566
  - VII. Besonderheiten bei kommunalen Gesellschaften — 567

## **Kapitel 18**

### **Marktmissbrauchsrecht und Compliance — 569**

- A. Überblick — **569**
  - I. Kapitalmarktrechtliches Marktmissbrauchsrecht — **569**
  - II. Das Analogon im Energierecht: die REMIT — **571**
    - 1. Überblick — **571**
    - 2. REMIT-Betroffenheit — **572**
- B. Insiderrecht — **573**
  - I. Überblick — **573**
  - II. Insiderinformation — **573**
    - 1. Konkrete Information — **574**
    - 2. Nicht öffentlich bekannte Information — **574**
    - 3. Emittenten- oder Insiderpapier-Bezug — **576**
    - 4. Eignung zur erheblichen Kursbeeinflussung — **576**
    - 5. Beispiele — **577**
    - 6. Exkurs — **579**
  - III. Insiderpapiere — **579**
    - 1. Finanzinstrumente — **579**
    - 2. Derivate — **580**
  - IV. Insiderhandelsverbot — **581**
    - 1. Tathandlungen — **581**
    - 2. Handelsverbot (Nr. 1) — **581**
    - 3. Weitergabeverbot (Nr. 3) — **582**
    - 4. Empfehlungs- bzw. Verleitungsverbot (Nr. 2) — **583**
  - V. Insiderrecht im Bereich der Energiegroßhandelsprodukte — **584**
    - 1. Überblick und Anwendungsbereich — **584**
    - 2. Insiderinformation und Insiderhandelsverbote — **585**
    - 3. Praktischer Umgang im Unternehmen — **587**
- C. Recht der Marktmanipulation — **587**
  - I. Überblick — **587**
  - II. Informationsgestützte Manipulationen — **588**
    - 1. Tatbestand — **588**
    - 2. Machen unrichtiger oder irreführender Angaben — **589**
    - 3. Verschweigen — **590**
  - III. Handelsgestützte Manipulationen — **591**
    - 1. Tatbestand — **591**
    - 2. Anzeichen nach der MaKonV — **592**
    - 3. Beispiele nach der MaKonV — **593**
  - IV. Sonstige Täuschungshandlungen — **594**
    - 1. Tatbestand — **594**
    - 2. Beispiele nach der MaKonV — **594**

- V. Marktmanipulation im Bereich der Energiegroßhandelsprodukte — **595**
- D. Untersuchung und Sanktionen von Marktmissbrauch — **597**

## **Kapitel 19**

### **Public Corporate Governance Kodex — 601**

- A. Überblick — **601**
- B. Grundlagen und Struktur — **603**
  - I. Quellen — **603**
  - II. Ziele und Regelungstechnik — **604**
  - III. Anwendungsbereich — **606**
- C. Vorgaben für die Geschäftsleitung — **607**
  - I. Leitungsaufgabe — **607**
  - II. Vergütung — **608**
  - III. Interessenkonflikte — **610**
- D. Aufsicht und Zusammenarbeit der Organe — **611**
  - I. Überblick — **611**
  - II. Aufsicht in Unternehmen des Bundes — **612**
  - III. Zusammensetzung und Interessenkonflikte — **613**
- E. Empfehlungen an die Anteilseigner — **613**
- F. Transparenz und Rechnungslegung — **615**
  - I. Jährlicher Bericht — **615**
  - II. Rechnungslegung — **616**
  - III. Abschlussprüfung — **618**
- G. Vergleichbare Regelungen — **618**
  - I. Kodizes auf Landesebene — **619**
  - II. Kodizes auf kommunaler Ebene — **621**
  - III. Entsprechende Regelungen — **622**
- H. Ausblick und aktuelle Entwicklung — **623**

## **Kapitel 20**

### **Strafrecht — 625**

- A. Überblick — **625**
- B. Vorteilsannahme und Vorteilsgewährung gegenüber Amtsträgern — **626**
  - I. Tatbestandsvoraussetzungen — **626**
    - 1. Amtsträger — **627**
    - 2. Vorteil — **630**

- 3. Unrechtsvereinbarung — **632**
    - 4. Vorsatz — **633**
  - II. Handlungsempfehlung — **634**
- C. Bestechlichkeit und Bestechung im geschäftlichen Verkehr — **636**
  - I. Tatbestandsvoraussetzungen — **636**
    - 1. Allgemeines — **637**
    - 2. Unlautere Bevorzugung im Wettbewerb (§ 299 Abs. 1 Nr. 1 und Abs. 2 Nr. 1 StGB) — **639**
    - 3. Pflichtverletzung gegenüber dem Unternehmen (§ 299 Abs. 1 Nr. 2 und Abs. 2 Nr. 2 StGB) — **640**
    - 4. Vorsatz — **640**
  - II. Handlungsempfehlung — **641**
- D. Wettbewerbsbeschränkende Absprache bei Ausschreibungen — **643**
  - I. Tatbestand — **643**
    - 1. Ausschreibung über Waren oder gewerbliche Leistung — **643**
    - 2. Rechtswidrige Absprache — **643**
    - 3. Abgeben eines Angebotes als strafbare Tathandlung — **644**
  - II. Handlungsempfehlung — **646**
- E. Steuerliche Auswirkungen von Zuwendungen — **646**
  - I. Auswirkungen für den Zuwendenden — **646**
  - II. Auswirkungen für den Zuwendungsempfänger — **647**
- F. Untreue — **648**
  - I. Tatbestandsvoraussetzungen — **649**
    - 1. Missbrauch — **649**
    - 2. Treuebruch — **650**
    - 3. Pflichtwidrigkeit — **651**
    - 4. Einverständnis des Vermögensinhabers — **652**
    - 5. Vermögensnachteil — **653**
    - 6. Vorsatz — **655**
  - II. Praxisrelevante Fallgruppen der Untreue — **655**
    - 1. Sponsoring — **655**
    - 2. Schmiergeldzahlungen — **657**
    - 3. Schwarze Kassen — **659**
    - 4. Risikogeschäfte — **660**
    - 5. Untreue im Konzern — **663**
    - 6. Untreue durch Aufsichtsratsmitglieder — **664**
  - III. Handlungsempfehlung — **665**
- G. Strafbarkeit des Compliance-Officers — **666**
- H. Steuerstrafrecht — **668**
  - I. Überblick — **668**
  - II. Materielles Steuerstrafrecht — **670**
    - 1. Der Tatbestand der Steuerhinterziehung — **670**

- a) Steuerhinterziehung durch aktives Tun — **671**
  - aa) Falsche Angaben über Tatsachen (Abs. 1 Nr. 1) — **671**
  - bb) Abgrenzung zu Rechtsauffassungen — **673**
  - cc) Keine Beweislast des Erklärenden — **674**
  - dd) Steuerberater — **674**
- b) Steuerhinterziehung durch Unterlassen — **675**
  - aa) Erklärungspflichtiger — **675**
  - bb) Berichtigungspflicht — **677**
- c) Steuerverkürzung — **678**
  - aa) Allgemeines — **678**
  - bb) Steuerverkürzung auf Zeit — **678**
  - cc) Ungerechtfertigter Steuervorteil — **679**
  - dd) Ermittlung des Steuerschadens — **679**
  - ee) Kompensationsverbot — **680**
- 2. Der subjektive Tatbestand der Steuerhinterziehung — **682**
- 3. Versuchte Steuerhinterziehung — **684**
- 4. Rechtsfolgen der Steuerhinterziehung — **685**
  - a) Kriminalstrafe — **685**
  - b) Verfahrenseinstellung — **687**
  - c) Strafbefehl — **688**
  - d) Bußgeldrechtliche Sanktionen — **689**
  - e) Vermögensabschöpfung — **691**
  - f) Steuerrechtliche Konsequenzen — **692**
- 5. Sonstige Steuerstraftatbestände/Steuerordnungswidrigkeiten — **693**
- 6. Selbstanzeige — **695**
  - a) Positive Voraussetzungen für die Wirksamkeit einer Selbstanzeige — **696**
  - b) Ausschluss der Wirksamkeit einer Selbstanzeige — **697**
- I. Steuerstrafverfahren — **701**
  - I. Allgemeine Hinweise — **701**
  - II. Einzelheiten des Verfahrens — **703**
    - 1. Kein Zwang zur Mitwirkung nach Einleitung eines Strafverfahrens — **704**
    - 2. Strafprozessuale Zwangsmaßnahmen — **705**
    - 3. Verhaltensempfehlungen — **707**

## **Kapitel 21**

**Ausblick** — **711**

**Register** — **713**