Ines Zenke, Ralf Schäfer, Holger Brocke (Hrsg.)
Corporate Governance
De Gruyter Praxishandbuch

Corporate Governance

Risikomanagement, Organisation, Compliance
für Unternehmer

Herausgegeben von
Ines Zenke, Ralf Schäfer, Holger Brocke

Bearbeitet von
Philipp Bacher, Sebastian Blumenthal-Barby, Wolfram von Blumenthal,
Holger Brocke, Matthias Brugger, Kai Buchholz-Stepputtis, Christian Dessau,
Jost Eder, Kirsten Erhard, Claudia Fischer, Jürgen Gold, Bernd Günter,
Tigran Heymann, Sebastian Holzinger, Michael Koch, Rebecca Julia Koch,
Lucian Krawczyk, Niko Liebheit, Christian Pisani, Ralf Schäfer,
Tobias Sengenberger, Thomas Straßer, Jörg B. Soetebeer, Meike Weichel,
Joachim Weide, Ingmar Weitemeier, Ines Zenke

DE GRUYTER

Zitiervorschlag: Zenke/Schäfer/Brocke/*Bearbeiter*, 2. Auflage, Kap. 1 Rn 10

Hinweis:
Alle Angaben in diesem Werk sind nach bestem Wissen unter Anwendung aller gebotenen Sorgfalt erstellt worden. Trotzdem kann von dem Verlag und den Autoren keine Haftung für etwaige Fehler übernommen werden.

ISBN 978-3-11-066779-0
e-ISBN (PDF) 978-3-11-067049-3
e-ISBN (EPUB) 978-3-11-066787-5

Library of Congress Control Number: 2020939765

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar.

© 2020 Walter de Gruyter GmbH, Berlin/Boston
Satz: jürgen ullrich typosatz, Nördlingen
Druck und Bindung: CPI books GmbH, Leck

www.degruyter.com

Inhalt

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

Kapitel 1
Unternehmensorganisation, Risikomanagement, Compliance-Management —— 1

Kapitel 2
Implementierung eines Compliance-Management-Systems —— 9

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 Beschlagnahmebefugnisse — 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. Revisionssicheres 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

Bearbeiterverzeichnis

Dr. Philipp Bacher ist Rechtsanwalt, Fachanwalt für Steuerrecht und Partner Counsel der auf Infrastrukturrecht spezialisierten Partnerschaft Becker Büttner Held. Herr Dr. Bacher berät Bund, Länder und Kommunen sowie kommunale und privatwirtschaftliche Unternehmen in allen Bereichen des Gesellschafts- und Wirtschaftsrechtes. Aktuell befasst sich Herr Dr. Bacher mit diversen umwandlungsrechtlichen Vorgängen (Spaltungen, Ausgliederungen und Verschmelzungen) zur Herstellung geeigneter Unternehmensstrukturen im Bereich der Rekommunalisierung, des Vergaberechtes (insb. ÖPNV), dem Erwerb von Beteiligungen an Erzeugungskapazitäten sowie der Errichtung von Bürgerenergiegesellschaften unter Berücksichtigung der Vorgaben des neuen EEG. Daneben ist er als interner und externer Referent für Vorträge über Rechte, Pflichten und Haftungsfragen von (kommunalen) Aufsichtsratsmitgliedern und Verwaltungsräten tätig.

Sebastian Blumenthal-Barby, LL.M., ist Rechtsanwalt und Partner Counsel der auf Infrastrukturrecht spezialisierten Partnerschaft Becker Büttner Held mit den Beratungsschwerpunkten Energie- und Energiewirtschaftsrecht, Regulierungsrecht und Gesellschaftsrecht. Er befasst sich projektleitend mit der Begleitung von Konzessionierungsverfahren für Kommunen und Energieversorger sowie mit der vertraglichen Umsetzung gesellschaftsrechtlicher Transaktionen (Umstrukturierungen, Entflechtung, Netzübernahmen). Er ist Verfasser zahlreicher Fachpublikationen.

Wolfram von Blumenthal ist Rechtsanwalt, Fachanwalt für Handels- und Gesellschaftsrecht und Partner der auf Infrastrukturrecht spezialisierten Partnerschaft Becker Büttner Held mit den Tätigkeitsschwerpunkten Gesellschaftsrecht, Mergers & Acquisitions (M&A) und allgemeines Zivilrecht. Er berät deutsche und ausländische Unternehmen in den Bereichen Gesellschaftsrecht und M&A. Er befasst sich mit Unternehmenskäufen und -verkäufen, Joint Ventures, Restrukturierungen, Unternehmenszusammenschlüssen und Umwandlungen, auch im Rahmen strukturierter Bieterverfahren. Daneben betreut Wolfram von Blumenthal Projekte zur Schaffung neuer Stromerzeugungskapazitäten auf der Basis Erneuerbarer Energien.

Dr. Holger Brocke, LL.M., ist seit 2005 als Staatsanwalt bei der Staatsanwaltschaft Berlin tätig. Er hat zum Thema der europäischen Staatshaftung promoviert und einen Master-Abschluss mit Schwerpunkt im Europarecht an der University of Edinburgh gemacht. Vor seinem Wechsel in den öffentlichen Dienst hat er fast zwei Jahre als Rechtsanwalt in Berlin gearbeitet. Holger Brocke ist Verfasser mehrerer Fachpublikationen und Mitautor des Münchener Kommentars zur StPO.

Matthias Brugger ist Rechtsanwalt und Partner Counsel bei der auf Infrastrukturrecht spezialisierten Partnerschaft Becker Büttner Held mit den Beratungsschwerpunkten Energie- und Energiewirtschaftsrecht, Gesellschaftsrecht und öffentliches Wirtschaftsrecht. Er befasst sich projektleitend mit der Begleitung von Konzessionierungsverfahren für Kommunen und Energieversorger sowie mit der vertraglichen Umsetzung gesellschaftsrechtlicher und insbesondere landesübergreifender kommunalrechtlicher Transaktionen.

Dr. Kai Buchholz-Stepputtis ist Security Consultant beim gemeinnützigen Verein G4C (German Competence against Center Cybercrime e.V.). Vereinszweck des G4C ist die Kriminalprävention im Bereich Cybercrime, Schwerpunkt seiner Tätigkeit ist dabei u.a. die Förderung des Erfahrungsaustauschs zwischen Wirtschaftsunternehmen und den G4C-Kooperationspartnern BSI und BKA sowie Awareness-Schaffung bei Unternehmen und Institutionen für die Risiken des Cybercrime. Vorher war Dr. Kai Buchholz-Stepputtis seit 1996 bei der Commerzbank AG beschäftigt und war dort 2002 Begründer und bis Ende 2018 Leiter des internen Information Security Consulting & Research.

https://doi.org/10.1515/9783110670493-206

Dr. Christian Dessau ist Rechtsanwalt und Partner Counsel der auf Infrastrukturrecht spezialisierten Partnerschaft Becker Büttner Held. Er hat mit einem rechtstheoretischen Thema promoviert (Ernst-Moritz-Arndt-Universität zu Greifswald) und beschäftigt sich heute insbesondere mit dem Commodityhandels-, Regulierungs-, Bankaufsichtsrecht und dem Thema Compliance. Christian Dessau ist u.a. Mitautor der Werke Schneider/Theobald, „Recht der Energiewirtschaft", Zenke/Schäfer, „Energiehandel in Europa" und des energierechtlichen Kommentarbandes von Theobald/Kühling, „Energierecht" (Loseblattsammlung) (alle im Verlag C.H.BECK).

Dr. Jost Eder ist Rechtsanwalt und Partner bei der auf Infrastrukturrecht spezialisierten Partnerschaft Becker Büttner Held mit den Beratungsschwerpunkten Datenschutz, Netzzugangs- und Energielieferverträge, Entflechtung (Unbundling), Zähler- und Messwesen, Regulierung sowie Arbeitsrecht. Er ist Herausgeber und Autor zahlreicher Fachpublikationen, u.a. Mitherausgeber von de Wyl/Eder/Hartmann, „Praxis-Kommentar Netzanschluss- und Grundversorgungsverordnungen", VWEW Energieverlag, 2008; Mitautor von Theobald/de Wyl/Eder, „Der Wechsel der Stromlieferanten", Beck-Rechtsberater im dtv, 2004, sowie Mitautor des energierechtlichen Kommentarbandes Theobald/Kühling, „Energierecht", Verlag C.H.BECK (Loseblattsammlung).

Kirsten Erhard ist M.Sc. in Financial Management, M.A. in International Business und Junior Consultant im Bereich Corporate Finance bei der auf das Infrastrukturrecht spezialisierten Partnerschaft Becker Büttner Held mit den Beratungsschwerpunkten Bewertung von Unternehmen, Energieversorgungsnetzen sowie Erzeugungsanlagen. Ferner führt sie Prozessoptimierungen in den rechnungslegungsnahen Bereichen von Unternehmen sowie die Einführung von steuer- und rechnungslegungsbezogenen Risiko- und Compliance-Management-Systemen durch. Zudem ist sie in vielen weiteren Fragen der steuerlichen und betriebswirtschaftlichen Beratung tätig.

Dr. Claudia Fischer ist Hauptabteilungsleiterin des Bereiches Recht/Beteiligungen/Compliance und Compliance-Beauftragte bei der Neubrandenburger Stadtwerke GmbH. Zuvor war sie seit 2010 Rechtsanwältin in der auf Energie- und Infrastrukturrecht spezialisierten Partnerschaft Becker Büttner Held und beschäftigte sich dort mit dem Energiehandels-, Emissionshandels- und Bankaufsichtsrecht. Sie hat mit einem naturschutzrechtlichen Thema promoviert (Universität Rostock). Claudia Fischer ist u.a. Mitautorin des Werkes Zenke/Schäfer, „Energiehandel in Europa" (Verlag C.H.BECK).

Jürgen Gold ist Wirtschaftsprüfer, Steuerberater und Partner der auf Infrastrukturrecht spezialisierten Partnerschaft Becker Büttner Held mit den Beratungsschwerpunkten Prüfung von Jahres- und Konzernabschlüssen und Umsetzung der Anforderungen des EnWG in EVU. Besondere Schwerpunkte bilden hierbei die buchhalterische Entflechtung sowie die Netzentgeltregulierung. Er ist Verfasser zahlreicher Fachpublikationen, u.a. steuerrechtliche und bilanzielle Implikationen des Emissionshandels als Mitautor zus. mit Guido Sydow des Buches Zenke/Fuhr/Bornkamm, „CO_2-Handel aktuell", EW Medien und Kongresse GmbH (vormals VWEW Energieverlag), 2009, sowie als Mitautor des Buches BBH/AGFW, „Neuer Gesetzesrahmen für die Kraft-Wärme-Kopplung und Erneuerbare Energien", 2009, und BBH/AGFW, „Fristen für Mitteilungen, Veröffentlichungen und Wirtschaftsprüfertestate nach EEG 2009 und KWKModG 2009".

Bernd Günter ist Rechtsanwalt, Fachanwalt für Arbeitsrecht und Partner Counsel der auf das Infrastrukturrecht spezialisierten Partnerschaft Becker Büttner Held. Er berät und vertritt Versorgungsunternehmen sowie andere Arbeitgeber auf allen Gebieten des Individual- und Kollektivarbeitsrechts. Den Beratungsschwerpunkt bildet die arbeitsrechtliche Begleitung von M&A-Projekten und Umstrukturierungen sowie Fragen der arbeits- und sozialversicherungsrechtlichen Compliance.

Zudem berät und vertritt er im Bereich der Anstellungsverhältnisse von Vorständen und Geschäftsführern. Daneben ist Bernd Günter seit Jahren ehrenamtlich als Mitglied des Fachausschusses Arbeitsrecht für die Rechtsanwaltskammer München tätig.

Dr. Tigran Heymann ist Rechtsanwalt und Partner der auf Infrastrukturrecht spezialisierten Partnerschaft Becker Büttner Held mit den Beratungsschwerpunkten Kartell- und Regulierungsrecht (insb. Fusionskontrolle und Missbrauchsaufsicht) und dem Umweltrecht (u.a. Emissionshandels-, Immissionsschutz- und Abfallrecht). Er hat sich in diesen Bereichen v.a. auf die Beratung von Energieversorgern und Industriekunden spezialisiert und berät Mandanten hierbei in gesetzgeberischen, behördlichen und (schieds-)gerichtlichen Angelegenheiten ebenso wie bei außergerichtlichen Fragestellungen. Als (Mit-)Autor hat er an zahlreichen einschlägigen Online- und Printpublikationen mitgewirkt.

Sebastian Holzinger ist Rechtsanwalt und arbeitet als Jurist bei der NATURSTROM AG mit Hauptsitz in Düsseldorf. Dort ist er u.a. zuständig für das Energiehandelsrecht sowie das Recht der Erneuerbaren Energien. Zuvor war er Leiter Marktüberwachung und Risikomanagement bei einer kommunalen Beratungssozietät in Berlin und von 2012 bis 2015 Dozent für Energierecht am WIT der TH Wildau.

Michael Koch ist Wirtschaftsprüfer und Steuerberater in der auf Infrastrukturrecht spezialisierten Partnerschaft Becker Büttner Held. Er beschäftigt sich vorwiegend mit der Prüfung von Jahres- und Konzernabschlüssen, Risikomanagementberatung, der Prüfung von Compliance-Management-Systemen sowie steuerlicher und betriebswirtschaftlicher Beratung und Sonderprüfungen. Er schloss sein Studium der Betriebswirtschaftslehre an der Universität zu Köln und der University of Calgary im Jahr 2006 mit einer Diplomarbeit zum kanadischen und europäischen Versicherungsaufsichtsmodell ab. Nebenberuflich engagiert er sich als Finanzvorstand des Fördervereins der Schulte-Schmelter-Stiftung „Kinder verstehen – Zukunft eröffnen e.V.“.

Dr. Rebecca Julia Koch studierte Rechtswissenschaften an den Universitäten Münster und Jena und wurde mit einer Arbeit über Produktrückruf-Versicherungen promoviert. Seit 2001 arbeitet sie im D&O-Versicherungsmarkt – in unterschiedlichen Funktionen (Spezialmakler, internationaler Konzern, Versicherung). Seit 2010 ist sie Geschäftsführerin der Kleist Versicherungsmakler GmbH. Hier ist sie spezialisiert auf D&O- und Cyber-Versicherungen. Als Lehrbeauftragte im Postgraduiertenstudiengang zum Versicherungsrecht an der Universität Münster und im Rahmen von Ausbildungsgängen der DVA (Deutsche Versicherungsakademie) unterrichtet sie zur D&O- und Cyber-Versicherung.

Prof. Dr. Lucian Krawczyk arbeitete nach seiner juristischen Ausbildung und akademischen Tätigkeit am Lehrstuhl für Straf- und Strafprozessrecht von Prof. Dr. Stephan Barton (Universität Bielefeld) zunächst als wissenschaftlicher Mitarbeiter in der renommierten wirtschaftsstrafrechtlichen Kanzlei Wessing & Partner in Düsseldorf. Ab 2011 ist Dr. Lucian Krawczyk als Rechtsanwalt in Berlin mit der Spezialisierung auf strafrechtliche Beratung und Strafverteidigung tätig gewesen. Seit 2016 ist er Professor für Strafrecht an der Hochschule für Wirtschaft und Recht Berlin. Er verfügt über Erfahrungen in umfangreichen Wirtschafts-, Korruptions- und Steuerstrafverfahren und ist Autor von Fachpublikationen zum Straf- und Strafprozessrecht.

Niko Liebheit, LL.M., ist Rechtsanwalt und Partner in der auf Infrastrukturrecht spezialisierten Partnerschaft Becker Büttner Held. Er befasst sich besonders mit deutschem und europäischem Stromsteuer- und Energiesteuerrecht sowohl aus Sicht der Energieversorger wie auch der Energie-

verbraucher. Daneben sind Fragestellungen zum Energiemanagement, zu weiteren Abgaben (EEG, KWKG etc.), zur dezentralen Erzeugung und zur Vertragsgestaltung weitere Schwerpunkte. Als (Mit-) Autor hat er an zahlreichen einschlägigen Online- und Printpublikationen mitgewirkt, u.a. als Mitautor des energierechtlichen Kommentarbandes Theobald/Kühling „Energierecht", Verlag C.H.BECK (Loseblattsammlung).

Dr. Christian Pisani ist Rechtsanwalt in München sowie Dozent für Versicherungsrecht an der Hagen Law School. Schwerpunkt seiner Tätigkeit bildet die umfassende gerichtliche und außergerichtliche Vertretung und Beratung seiner Mandanten im Haftungs- und Versicherungsrecht. Dr. Christian Pisani begann seine berufliche Laufbahn im Berliner Büro von Becker Büttner Held, bevor er sich der im Versicherungsrecht ausgewiesenen Sozietät Bach Langheid & Dallmayr in München anschloss. Er ist Gründungspartner von Pisani & Partner – Rechtsanwälte in Partnerschaft und Mitautor des Werkes von Schwintowski/Brömmelmeyer, „Praxiskommentars zum Versicherungsvertragsrecht" sowie einer Einführung zum Sachversicherungsrecht und veröffentlicht regelmäßig zu Versicherungs- und Compliance-Themen.

Dr. Ralf Schäfer ist Rechtsanwalt und geschäftsführender Gesellschafter der Rosin Büdenbender Rechtsanwaltsgesellschaft mbH, Essen, mit den Beratungsschwerpunkten Kartell-, Bank- und Börsenrecht sowie im Bereich Compliance. Ralf Schäfer wurde im Kommunalwirtschafts- und Energierecht zu verfassungs- und mitbestimmungsrechtlichen Fragestellungen promoviert. Er ist Verfasser diverser Fachpublikationen, u.a. als Herausgeber und Mitautor des Buches von Zenke/Schäfer, „Energiehandel in Europa", Verlag C.H.BECK, sowie verschiedener Fachaufsätze zum Thema Compliance. Darüber hinaus verfasst er seit rund 20 Jahren die Kolumne zu aktuellen Entwicklungen im Energierecht in der Zeitschrift „Energiewirtschaftliche Tagesfragen". Von 2009 bis 2014 war er Lehrbeauftragter im Bereich Energiewirtschaft an der Fachhochschule Düsseldorf und ist seit 1996 nebenamtlicher Prüfer im 2. juristischen Staatsexamen beim Landesjustizprüfungsamt Nordrhein-Westfalen.

Tobias Sengenberger, LL.M., ist Wirtschaftsprüfer, Steuerberater und Partner der auf das Energie- und Infrastrukturrecht spezialisierten Partnerschaft Becker Büttner Held mit dem Beratungsschwerpunkt Datenschutzcompliance. Ferner führt er Prozessoptimierungen in den rechnungslegungsnahen Bereichen von Unternehmen sowie die Einführung von steuer- und rechnungslegungsbezogenen Risiko- und Compliance-Management-Systemen durch. Zudem ist er in vielen weiteren Fragen der steuerlichen und betriebswirtschaftlichen Beratung tätig.

Thomas Straßer ist Wirtschaftsprüfer, Steuerberater und Partner der auf das Infrastrukturrecht spezialisierten Partnerschaft Becker Büttner Held mit den Beratungsschwerpunkten Bewertung von Unternehmen, Energieversorgungsnetzen und Erzeugungsanlagen. Ferner führt er Sonderprüfungen, Due-Diligence-Prüfungen, Prüfungen von Risikomanagementsystemen, Abwasser- und Wasserentgeltkalkulationen sowie die Prüfung von Jahres- und Konzernabschlüssen durch. Darüber hinaus ist er in vielen weiteren Fragen der steuerlichen und betriebswirtschaftlichen Beratung tätig.

Jörg B. Soetebeer ist selbstständiger Rechtsanwalt in Münster/Westfalen und auf das Energie- und Energiewirtschaftsrecht spezialisiert. Seine Beratungsschwerpunkte umfassen den gesamten Energievertrieb, das Zähler- und Messwesen, die Regulierung, die Wärme- und Wasserversorgung sowie die allgemeine zivilrechtliche Vertragsgestaltung. Er berät ferner umfassend im Bereich des Datenschutzes. Herr Soetebeer begann seine berufliche Laufbahn bei der auf Infrastrukturrecht spezialisierten Kanzlei Becker Becker Büttner Held, für die er zuletzt im Hamburger Büro als Partner Coun-

sel tätig war. Er ist u.a. Mitautor des Werkes Schneider/Theobald, „Recht der Energiewirtschaft", Verlag C.H.BECK.

Meike Weichel, LL.M., ist Rechtsanwältin, Steuerberaterin, Fachanwältin für Steuerrecht und Partner Counsel der auf Infrastrukturrecht spezialisierten Partnerschaft Becker Büttner Held. Zu ihren Schwerpunkten zählen neben der steuerlichen Beratung von Kommunen und ihren Betrieben gewerblicher Art (BgA), von Unternehmen der kommunalen Daseinsvorsorge wie Verkehrsbetrieben und Schwimmbädern sowie von Unternehmen der Energiewirtschaft auch die Beratung von Unternehmen bei der Implementierung und Überwachung von Tax-Compliance-Management-Systemen.

Joachim Weide, ehemaliger Direktor bei Alvarez and Marsal, war in unterschiedlichen leitenden Funktionen als CTO verschiedener Firmen tätig. Schwerpunkte waren IT-Transformation und Konsolidierung von komplexen SAP-Landschaften in unterschiedlichen Industrien wie Automotive, Manufacturing und Pharma. Im Rahmen von Digitalisierungsprojekten hat Herr Weide Unternehmen in den Themen Sicherheit und Cloud-Anwendungen im In- und Ausland beraten. Heute ist er Inhaber der Operatis Consulting und betreut verschiedene Kunden in SAP S/4 HANA und Sicherheitsthemen. Gleichzeitig unterstützt er den gemeinnützigen Verein G4C (German Competence Centre against Cyber Crime e.V.) in Wiesbaden als IT-Leiter und Berater. Dabei ist es ihm wichtig, den Schutz der Unternehmen gegen Cyberangriffe weiter zu erhöhen.

Ingmar Weitemeier, ehemaliger Direktor des Landeskriminalamts Mecklenburg-Vorpommern, hat die Behörde über 14 Jahre geleitet, davor war er Gründungsdekan des Fachbereiches Polizei der Fachhochschule für Verwaltung und Rechtspflege in Sachsen-Anhalt, vorherige Verwendung in unterschiedlichen Führungsfunktionen der Niedersächsischen Polizei. Er führt derzeit ein Unternehmen mit Schwerpunkt „Investigative Maßnahme". Gleichzeitig unterstützt er den gemeinnützigen Verein G4C (German Competence Centre against Cyber Crime e.V.) in Wiesbaden als Projektleiter und Berater und sein Hauptaugenmerk liegt darauf, den Schutz der Unternehmen gegen Cyberangriffe weiter zu erhöhen.

Prof. Dr. Ines Zenke ist Rechtsanwältin, Fachanwältin für Verwaltungsrecht und Partnerin der auf Infrastrukturrecht spezialisierten Partnerschaft Becker Büttner Held. Sie ist seit 25 Jahren in der Wirtschaft tätig, insbesondere der der Energie- und Infrastrukturen. In der Compliance begleitet sie Vorstände und Geschäftsführungen insbesondere in Fällen notwendiger Krisen-Compliance. Zu ihren Schwerpunkten zählen weiter die Politikberatung sowie die anwaltliche Begleitung im Infrastruktur-, Energie- und Umweltrecht. Ines Zenke ist Verfasserin und Mitverfasserin von zusammen rund 200 Fachpublikationen und Honorarprofessorin an der Hochschule für nachhaltige Entwicklung Eberswalde (HNEE), Fachbereich Wirtschaft, Studiengang Master Kommunalwirtschaft. Weiteres: https://www.die-bbh-gruppe.de/de/experten/info/ines-zenke.

Kapitel 1
Unternehmensorganisation, Risikomanagement, Compliance-Management

Die Neuauflage dieses Buches verfolgt wie bisher das Ziel, dem Leser die engen aber nicht durchweg offenkundigen Zusammenhänge zwischen Unternehmensorganisation, Risikomanagement und Compliance-Management erkennbar zu machen. Zugleich möchten wir aufzeigen, was sich seit Erscheinen der ersten Auflage im Jahr 2015 auf diesen Gebieten verändert und neu entwickelt hat. Der Stein des Anstoßes für die Erstentstehung dieses Werkes waren im Wesentlichen die Erfahrungen, die aus Beratungen mittelständischer (Versorgungs-)Unternehmen, bei denen Consultants, Wirtschaftsprüfer und Juristen gemeinsam an einer Aufgabenstellung gearbeitet haben, resultierten. Im Rahmen dieser Zusammenarbeit wurde deutlich, dass zwischen den genannten Funktionen vielfältige Schnittstellen und Wechselbeziehungen bestehen. Seither hat sich an dieser Feststellung nichts geändert. Vielmehr haben sich diese Beziehungen noch intensiviert.[1] **1**

Vor diesem Hintergrund fiel auch die Entscheidung, den Titel dieses Werkes anzupassen und den Oberbegriff „Corporate Governance" voranzustellen, um zu verdeutlichen, dass dieses Buch einen Leitfaden für die verantwortungsvolle Führung und Kontrolle im Unternehmen darstellen soll. „Corporate Governance" ist die Aufgabe des Managements, vielfältige Interessen, namentlich der Öffentlichkeit, des Kapitalmarkts und der „Stakeholder", zu berücksichtigen und einen Ordnungsrahmen für die Leitung und Kontrolle des Unternehmens zu schaffen.[2] **2**

Dass sich die Beziehungen zwischen den soeben genannten Akteuren intensiviert haben, überrascht zumindest dann nicht, wenn man die Aufgaben und Kompetenzen der Akteure – ggf. unter Einbeziehung der Internen Revision – als Teilelemente eines umfassenden „**Internen Kontrollsystems**" (IKS) versteht. **3**

Unter einem IKS soll an dieser Stelle die Gesamtheit aller von der Unternehmensleitung angeordneten Vorgänge, Methoden und Maßnahmen (Kontrollmaßnahmen) verstanden werden, die dazu dienen, einen ordnungsgemäßen und rechtskonformen Ablauf des betrieblichen Geschehens sicherzustellen.[3] Bei Verwendung **4**

1 Vgl. dazu *Schefold*, CB 2019, 181 ff., mit einer ausführlichen Darstellung zur Zunahme von Compliance-Bemühungen seit 2005.

2 Stober/Orthmann/*Thiel*, Compliance, Rn 147.

3 Vgl. statt vieler: PricewaterhouseCoopers (PwC), Internes Kontrollsystem – Führungsinstrument im Wandel, S. 4, abrufbar unter https://www.yumpu.com/de/document/read/21553700/interneskontrollsystem-fuhrungsinstrument-im-wandel-pwc; IDW Prüfungsstandard 261 n.F. (IDW PS 261 n.F.), Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken, 13.3.2013, Nr. 3.1.2.1.

https://doi.org/10.1515/9783110670493-001

eines weiten IKS-Verständnisses wird man mit Recht (auch) die Unternehmensorganisation, das Risiko- und Compliance-Management sowie die Interne Revision als Teil eines (integrierten) IKS ansehen dürfen.[4]

5 In diesem Kontext bildet die Unternehmensorganisation die formale Grundlage für das Risiko- und Compliance-Management im Unternehmen. Dabei ist die Unternehmensleitung originär für die Einhaltung entsprechender Maßnahmen zuständig.[5] Die Aufgabe der **Unternehmensorganisation**[6] ist es, die Verantwortlichkeiten der einzelnen Unternehmenseinheiten und dort tätigen Beschäftigten präzise festzulegen und die Ablauf- sowie die Zusammenarbeitsprozesse in und zwischen den Einheiten zu definieren. Die Unternehmensleitung und leitende Mitarbeiter sollen zudem eine Vorbildfunktion bei der Einhaltung der in diesem Rahmen festgelegten Regeln einnehmen.[7]

6 Diese Festlegungen bilden den Anknüpfungspunkt für das Rechts- und Compliance-Management. Beide Funktionen weisen ebenfalls diverse Schnittstellen bzw. Wechselwirkungen auf. Das **Risikomanagement** zielt bekanntlich darauf ab, die **ökonomischen Risiken** einer Organisation (frühzeitig) zu erkennen, zu analysieren und zu bewerten, um daran anknüpfend die erforderlichen Maßnahmen zu treffen, um die Realisierung dieser Risiken möglichst zu verhindern bzw. die daraus resultierenden Nachteile soweit wie möglich zu minimieren (**Risikosteuerung**) sowie entsprechende Risiken künftig zu vermeiden.[8] Daneben sind Risikokontrolle und Risikowälzung im Auge zu behalten.[9] Das **Compliance-Management** versucht, mit ähnlichen Mitteln die **rechtlichen Risiken** eines Unternehmens (rechtzeitig) zu erkennen, zu analysieren und zu bewerten, um deren Eintritt soweit wie möglich zu verhindern bzw. etwaige Nachteile aufgrund von Rechts- und Regelverletzungen so gering wie möglich zu halten.[10] Da Rechtsrisiken sich nicht selten in ökonomischen Risiken realisieren, kann ein Compliance-Management letztlich nicht ohne ein um-

4 Vgl. *Block*/*Teicke*, CB 2019, 105, die die Einrichtung eines IKS als Merkmal von Professionalisierung der Compliance-Arbeit eines Unternehmens verstehen.

5 So *Hastenrath*, CB 2019, 244.

6 Vgl. auch Gabler Wirtschaftslexikon, Stichwort: Organisation, abrufbar unter https://wirtschaftslexikon.gabler.de/definition/organisation-45094/version-137000.

7 Vgl. *Wiedmann*/*Greubel*, CCZ 2019, 89.

8 Vgl. zu den Grundelementen des Risikomanagements den Entwurf einer Neufassung des IDW Prüfungsstandards 340, S. 5 ff., abrufbar unter https://www.idw.de/blob/119140/b8324b4f7fbf5bcf9d590481a4251b9c/idw-eps-340-nf-data.pdf.

9 Vgl. statt vieler nur Gabler Wirtschaftslexikon, Stichwort: Risikomanagement, abrufbar unter https://wirtschaftslexikon.gabler.de/definition/risikomanagement-42454; IDW Prüfungsstandard 340 (IDW PS 340), Die Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB, 11.9.2000, Nr. 2; vgl. näher Kap. 3.

10 Vgl. dazu nur IDW Prüfungsstandard 980 (IDW PS 980), Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen, 11.3.2011, Rn 7 sowie näher ab Kap. 4.

fassendes Risikomanagement bestehen und beide Funktionalitäten sind damit als Teile eines (weit verstandenen) IKS eines Unternehmens zu begreifen.[11]

Dieser Befund ist wiederum der maßgebliche Grund für die integrierte Behand- 7
lung von Unternehmensorganisation, Risiko- und Compliance-Management in diesem Buch. Die gewählte Darstellungsweise soll dazu beitragen, der Komplexität eines umfassend verstandenen Risikomanagements in der täglichen unternehmerischen Praxis sowie in der Unternehmensberatung besser gerecht zu werden.

Wer sich im Unternehmen – sei es als Führungskraft, sei es als externer Be- 8
rater – mit Fragestellungen der Unternehmensorganisation, des Risiko- oder des Compliance-Managements befasst, wird – wie bereits eingangs angemerkt – feststellen, dass Problemlösungen in einem der genannten Bereiche sehr oft die Beantwortung von Fragestellungen aus dem einen oder anderen Bereich erfordert. Wer dann erwartet, für diese „interdisziplinäre" Fragestellung unschwer Hilfestellung in entsprechend angelegter Fachliteratur zu finden, wird erstaunt feststellen, dass das Angebot insoweit nicht übermäßig breit ist. Grundlegende und eingehende Darstellungen finden sich zwar mittlerweile zu allen genannten Bereichen[12] ebenso wie zu den angrenzenden Themen IKS und interne Revision.[13] Literatur, die die vorstehenden Disziplinen in Bezug auf ihre Schnittstellen, Wechselwirkungen und Abhängigkeiten eingehender beschreibt, ist dagegen weniger häufig anzutreffen.[14]

Eine integrierte Betrachtung von Unternehmensorganisation, Risikomanage- 9
ment und Compliance und daran anknüpfend ein holistisches Management dieser Funktionalitäten ist jedoch (auch) bei mittelständischen Unternehmen nicht bloß ein „Kostenverursacher",[15] und sollte insbesondere nicht als Verlangsamung, Behinderung oder Erschwerung von Geschäftsabläufen gesehen werden, um den Entwicklungen der letzten Jahre auf diesen Gebieten keinen Dämpfer zu verpassen.[16] Vielmehr schafft eine solche integrierte Betrachtung nicht unerhebliche Vorteile, wie folgende Überlegungen zeigen:

Die Existenz von Unternehmensorganisation, Risiko- und Compliance-Manage- 10
ment ebenso wie die Einrichtung einer Internen Revision werden zunehmend auch

11 Vgl. *Block/Teicke*, CB 2019, 107; *Krisor*, CB 2019, 29; zu Vorgaben im Wirtschaftsverwaltungsrecht, die ein Ineinandergreifen ebenfalls vorsehen Stober/Orthmann/*Ennuschat*, Compliance, Rn 1826; Bürkle/Hauschka/*Schulz/Galster*, Compliance Officer, § 4, Rn 12 ff.

12 Vgl. z.B. Hauschka, Corporate Compliance, 3. Aufl.; *Diederichs*, Risikomanagement und Risikocontrolling; *Schreyögg*, Organisation.

13 Vgl. z.B. *Böhmer/Hengst/Hofmann/Müller/Puchta*, Interne Revision.

14 Vgl. z.B. *Laue/Mohr*, CB 2014, 334 ff.; *Marekfia/Nissen*, Strategisches GRC-Management, S. 5 ff., abrufbar unter http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-18915/FUB-2009-2.pdf.

15 Vgl. auch *Marekfia/Nissen*, Strategisches GRC-Management, S. 2 f., abrufbar unter http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-18915/FUB-2009-2.pdf.

16 Vgl. *Block/Teicke*, CB 2019, 108 f.

in mittelständischen Unternehmen zum „Stand der Technik".[17] Grund dafür dürften zum einen diverse gesetzliche Vorschriften sein,[18] zum anderen ebenso vielfältige untergesetzliche Regelwerke von Behörden und Organisationen.[19] Konkret sind an dieser Stelle insbesondere die Vorgaben für den Datenschutz seit Inkrafttreten der Datenschutzgrundverordnung im Jahr 2018 zu nennen, die es Unternehmen abverlangen, ihre datenschutzrelevanten Prozesse zu optimieren[20] sowie auch die erwartete Änderung des Deutschen Corporate Governance Kodex[21] und das beabsichtigte Verbandssanktionsgesetz.[22] Zu erwähnen ist weiterhin einerseits das Urteil des Landgerichts München I vom 10.12.2013,[23] das eine Reihe von konkreten Vorgaben für ein Compliance-Management macht, damit es den gesetzlichen Vorschriften entspricht[24] und andererseits das Urteil des Bundesgerichtshofs vom 9.5.2017, das der Einhaltung von Compliance-Management-Systemen eine bußgeldmindernde Wirkung bei Rechtsverstößen von Unternehmen zuspricht, ohne allerdings selbst Vorgaben aufzustellen.[25]

11 Diese aus volkswirtschaftlicher Sicht an sich begrüßenswerte Institutionalisierung und Strukturierung des Managements operativer und rechtlicher Risiken hat allerdings noch gewisse Schwächen bzw. Nachteile. Diese resultieren primär daraus, dass sämtliche genannten Funktionen, sofern implementiert, parallel vorgehalten werden und mehr oder weniger isoliert in ihrem jeweiligen „Zuständigkeitsbereich" arbeiten. Zumindest in Teilbereichen kommt es auf diese Weise zu inhaltlichen und/oder funktionalen Überschneidungen.[26] Entweder werden Sach-

17 Zur zunehmenden Verbreitung von Compliance-Management seit 2005 vgl. *Schefold*, CB 2019, S. 181 ff.; vgl. zur generellen Zunahme von entsprechenden Maßnahmen *Block/Teicke*, CB 2019, 104; *Fila/Püschel*, Newsdienst Compliance 2019, 210017.

18 Zu denken ist vor allem an § 93 Abs. 1 S. 1, 2 AktG (Aktiengesetz) v. 6.9.1965 (BGBl. I S. 1089), zuletzt geändert durch Gesetz v. 17.7.2017 (BGBl. I S. 2446), §§ 30, 130 OWiG (Gesetz über Ordnungswidrigkeiten (OWiG) v. 19.2.1987 (BGBl. I S. 602), zuletzt geändert durch Gesetz v. 20.11.2019 (BGBl. I S. 1724); vgl. dazu näher Kap. 5.

19 Vgl. dazu im Einzelnen näher Kap. 5, 7, 9, 20; Stichworte sind hier insbesondere: Deutscher Corporate Governance Kodex, MaRisk, MaComp, ONR 192050, ISO 19600 sowie die Prüfungsstandards 261, 340, 980 des IDW.

20 *Block/Teicke*, CB 2019, 107.

21 Deutscher Corporate Governance Kodex, Entwurf abrufbar unter https://www.dcgk.de/files/dcgk/usercontent/de/Konsultationen/2019/DCGK%202019/190522%20DCGK%202019%20mit%20Begruendungen.pdf.

22 Vgl. die ausführliche Darstellung zum Entwurf bei *Mayer/Jenne*, CB 2019, 405 ff.

23 Vgl. LG München I, Urt. v. 10.12.2013 – 5 HK O 1387/10 – DB 2014, 766.

24 Dies gilt ungeachtet der Tatsache, dass die Vorgaben des LG München I aus Verfahrensgründen nicht mehr einer Validierung durch das OLG München oder den BGH unterzogen werden.

25 BGH, Urt. v. 9.5.2017 – 1 StR 265/16 – BeckRS 2017, 114578.

26 Vgl. *Laue/Mohr*, CB 2014, 335, 336.

verhalte mehrfach bearbeitet oder es kommt zu Diskussionen über die „Bearbeitungszuständigkeit“ oder – noch schlimmer – zu beiden Effekten.[27]

Diese unbefriedigende Ineffizienz kann auch nicht immer auf Ebene der Ge- 12
schäftsleitung vermieden werden, da die beteiligten Funktionalitäten nicht durchweg auf Geschäftsleitungsebene in einem Ressort bzw. einer Person verbunden sind.[28] Auch unterhalb der Geschäftsleitung sehen die derzeit gängigen Organisationsmodelle in der Regel keine „Personalunion“ hinsichtlich der in Rede stehenden Funktionen vor.[29]

Durch die Fragmentierung, in Bezug auf die Gesamtrisikosituation, entstehen 13
vielfach nur Teilbilder, die wiederum nur Teillösungen von Problemen ermöglichen. Daneben kommt es durch die angesprochene Mehrfachbearbeitung zu redundanten Abfragen mit entsprechender „bürokratischer“ Belastung bei den operativen Bereichen und anschließend zu Mehrfachberichterstattungen an die Geschäftsleitung und/oder einzelne Mitglieder des Gremiums.

Trotzdem – oder gerade deswegen – entstehen auf diese Weise unerwünschte 14
Informationslücken in Bezug auf die Risikosituation.[30] Fehlende Abstimmung und asymmetrische Informationen in Bezug auf eine Risikosituation können unvernetzte (Ad-hoc-)Aktivitäten einzelner Führungsverantwortlicher im Krisenfall erzeugen, die nicht zwingend die für das Gesamtunternehmen beste Lösung darstellen. Es fehlt mit anderen Worten eine optimale Gestaltung der relevanten Geschäftsprozesse.[31]

Eine faktisch-wissenschaftlich fundierte Aufarbeitung der vorstehenden Prob- 15
lematik steht – soweit ersichtlich – derzeit noch weitgehend aus. Aktuell finden sich diverse Ansätze für Verbesserungsvorschläge, ohne dass sich bisher ein allgemein akzeptierter Lösungsansatz durchgesetzt hätte.[32]

Zur Auflösung der Fragmentierung steht ein sog. **GRC-Ansatz in der Diskussi-** 16
on, wobei „GRC“ für Governance Risk und Compliance steht. Darunter wird ein integrierter, holistischer Ansatz verstanden, der auf unternehmensweit angelegte Organisationssteuerung (Governance) unter Einschluss des Risiko- und Compliance-Managements abzielt und gewährleisten soll, dass sich das Unternehmen insgesamt entsprechend dem festgelegten Risikoappetit unter Beachtung rechtlicher und ethischer Vorgaben verhält. Dies soll durch eine Abstimmung von Organisation, Prozes-

27 Vgl. auch die Darstellung bei *Hastenrath*, CB 2019, 243 ff.
28 Vgl. *Laue/Mohr*, CB 2014, 334, 335; *Dederichs/Fricke/Macke*, DB 2011, 1461 ff.
29 Eine ähnliche Kritik findet sich bei *Hastenrath*, CB 2019, 243 ff.; *Block/Teicke*, CB 2019, 103 ff.
30 Ähnlich auch *Laue/Mohr*, CB 2014, 334, 336.
31 Vgl. auch *Marekfia/Nissen*, Strategisches GRC-Management, S. 5, abrufbar unter http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-18915/FUB-2009-2.pdf.
32 Vgl. *Laue/Mohr*, CB 2014, 334, 335; ähnlich auch *Sonnenberg*, JuS 2017, 918; vgl. für einen Lösungsansatz aber bspw. *Hastenrath*, CB 2019, 243 ff.

sen und Strategien erreicht werden, die auf der integrierten Praktizierung der genannten Funktionalitäten beruht.[33]

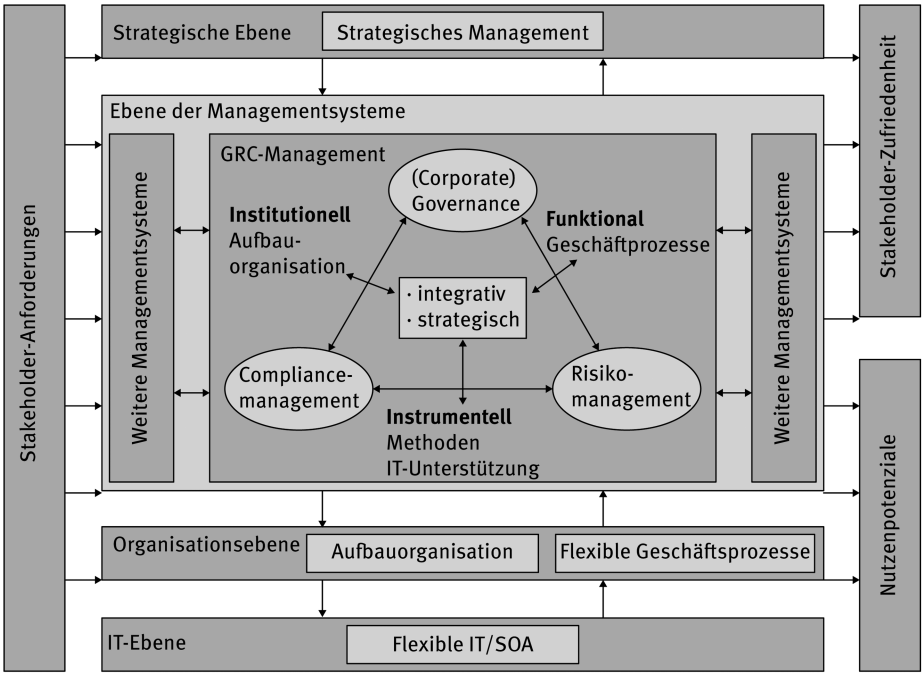

Abb. 1: GRC-Ansatz[34]

17 Auf dieser Basis werden auch die Einführung eines „**Chief Governance Officers**" (CGO) bzw. eines „GRC-Officers" oder auch eines „GRC-Komitees" vorgeschlagen.[35]

18 Der CGO bzw. das GRC-Office sollen als Stabstelle bei der Geschäftsleitung bzw. deren Vorsitzendem eingerichtet werden und unmittelbar an diese(n) berichten. Dabei wird eine Zusammenlegung mit der Funktion des Chief Compliance Officers oder des Leiters der Rechtsabteilung erwogen.

19 Der Aufgabenumfang des CGO soll neben der Entwicklung von unternehmensinternen Richtlinien, der Schulung des Aufsichtsrats, der Beratung der Geschäftslei-

33 Vgl. *Marekfia/Nissen*, Strategisches GRC-Management, S. 4 ff., abrufbar unter http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-18915/FUB-2009-2.pdf; De Decker/Schaumüller-Bichl/*Racz/Weippel/Seufert*, Communications and Multimedia Security, S. 106 ff.

34 *Marekfia/Nissen*, Strategisches GRC-Management, S. 8, abrufbar unter http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-18915/FUB-2009-2.pdf.

35 Vgl. etwa *Laue/Mohr*, CB 2014, 334, 336; *Marekfia/Nissen*, Strategisches GRC-Management, S. 9 f., abrufbar unter http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-18915/FUB-2009-2.pdf.

tung (insbesondere auch im Zusammenhang mit der Besetzung von Schlüsselpositionen im Unternehmen) sowie die Berichterstattung über die einzelnen Teilsysteme des GRC-Komplexes umfassen.[36]

Diese Vorschläge dürften für große börsennotierte Unternehmen zweifellos eine angemessene Lösung darstellen und werden deshalb dort auch schon zum Teil praktiziert.[37] In Bezug auf mittelständische Unternehmen wird man dagegen genau überlegen müssen, welche Lösung hier das relative Optimum zwischen Kosten und Nutzen eines GRC-Ansatzes bieten kann. Fällt es Großunternehmen in der Regel leicht, entsprechende Maßnahmen zu treffen, kann die Implementierung richtiger Lösungen für KMU schnell eine große Herausforderung darstellen.[38] **20**

Vor diesem Hintergrund ist es Ziel des vorliegenden Werkes, einen Beitrag zur integrierten Darstellung und Handhabung von Unternehmensorganisation, Risiko- und Compliance-Management zu leisten. Der Fokus liegt dabei weniger auf der wissenschaftlichen Aufbereitung der einzelnen Gebiete als vielmehr auf dem Nutzen der gebotenen Informationen und Überlegungen für die tägliche Praxis in mittelständischen Unternehmen. Das Buch richtet sich deshalb vornehmlich an Vorstände, Geschäftsführer und Aufsichtsräte in mittelständischen Unternehmen sowie an die Leiter Risikomanagement, Risikocontrolling, Interne Revision, Compliance und deren Mitarbeiter. Ebenso angesprochen werden die Leitungsebene und die Beschäftigten der öffentlichen Verwaltung und der Gerichtsbarkeit, die Organisationsverantwortung tragen. Allen Adressaten soll die Thematik des Werks praxisnah und anwenderfreundlich aufbereitet und vermittelt werden. **21**

36 Vgl. anschaulich *Laue/Mohr*, CB 2014, 334, 337.
37 Vgl. die Nachweise *Laue/Mohr*, CB 2014, 334, 337, Fn 15 ff.
38 Ähnlich *Schefold*, CB 2019, 184; *Hastenrath*, CB 2019, 243 f.

Kapitel 11
Datenschutzrechtliche Compliance

A. Einleitung

Bereits vor Geltung der Datenschutz-Grundverordnung waren in den Medien zahl- 1
reiche Fälle unzulässiger Verwendungen von Daten durch private und kommunale Unternehmen aufgegriffen worden. Dies hing nicht zuletzt damit zusammen, dass die datenschutzrechtlichen Vorgaben in Europa und der Bundesrepublik Deutschland weiter verschärft bzw. differenziert wurden. Zugleich hat sich zunehmend die Frage in das Bewusstsein der Öffentlichkeit gedrängt, wie öffentliche und private Stellen mit personenbezogenen Daten der Bürgerinnen und Bürger umgehen.

Mit Geltung der Datenschutz-Grundverordnung[1] (DS-GVO) ab dem **25.5.2018** 2
wurde das Datenschutzrecht in Europa auf ein einheitliches Schutzniveau gehoben. Die DS-GVO verfolgt dementsprechend das ausdrückliche Ziel, „die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten" zu schützen. Die DS-GVO hat dabei nicht nur neue Begrifflichkeiten und Inhalte gebracht, sondern auch eine Vielzahl neuer Verpflichtungen. Entsprechend groß war und ist mitunter die Verunsicherung bei Unternehmen, Freiberuflern, Organisationen und Vereinen bei der Umsetzung des aktuellen Rechtsrahmens. Bemängelt wurde der hohe Aufwand für kleinere Unternehmen und Vereine. Ein Anstieg der Beschwerden über Datenschutzverstöße hat zugleich zu einem erkennbaren Anstieg der behördlichen Verfahren und verhängten Bußgelder geführt. Hatten die Behörden im Jahr 2018 „nur" 40 Bußen ausgesprochen, waren es im Jahr 2019 bereits mindestens 185 Bußgelder. Bundesweit sollen innerhalb der ersten 18 Monate seit dem Start des neuen Regelwerks insgesamt rund 21.000 Datenpannen gemeldet worden sein.[2]

Compliance-Strukturen kommen in diesem Bereich daher eine wichtige **präven-** 3
tive Wirkung zu. Unternehmen haben sicherzustellen, dass ihre Datenverarbeitung nach Maßgabe der gesetzlichen Bestimmungen erfolgt, nicht zuletzt um **Haftungsrisiken** zu **mindern**. Neben den materiell-rechtlichen Vorgaben zum Datenschutz hat ein Unternehmen mittlerweile zahlreiche organisatorische datenschutzrechtli-

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates v. 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl EU Nr. L 127 S. 2).
2 Vgl. https://www.abendblatt.de/politik/article228039147/Datenschutz-Verstoesse-Firmen-mussten-185-Bussgelder-zahlen.html.

https://doi.org/10.1515/9783110670493-011

che Verpflichtungen zu erfüllen (z.B. Bestellung eines Datenschutzbeauftragten, Verzeichnis aller Verarbeitungstätigkeiten).

4 Die Einhaltung der gesetzlichen Vorgaben sollte für ein Unternehmen indes nicht der einzige Beweggrund für die **Einführung eines datenschutzrechtlichen Compliance-Systems**[3] sein. Ein Datenverlust kann für ein Unternehmen erhebliche wirtschaftliche Auswirkungen haben. Zugleich rückt die **Vermeidung von Imageschäden durch Reputationsverluste** in den Mittelpunkt, was zu einem ganz erheblichen Vertrauensverlust bei Kunden oder auch Mitarbeitern führen kann. Vor diesem Hintergrund lässt sich Datenschutz auch als Wettbewerbsvorteil begreifen, weil ein offener Umgang mit datenrelevanten Verarbeitungsvorgängen regelmäßig zu einer Kundenbindung der Bestandskunden führen und zudem den Gewinn von Neukunden erleichtern kann.[4] Unternehmen legen daher zunehmend Wert auf den Schutz und die ordnungsgemäße Verarbeitung der Daten.

5 Eine gelungene datenschutzrechtliche Compliance bezweckt daher auch, die einzelnen **Mitarbeiter** in die Pflicht zu nehmen und ihnen ihre Verantwortung für den **rechtskonformen Umgang mit Daten** bewusst zu machen. Die Mitarbeiter sind dabei so zu schulen, dass sie Daten unter Wahrung der Persönlichkeitsrechte des Einzelnen rechtskonform verarbeiten.

6 Nach einer kurzen Einführung zu den Eckpunkten der DS-GVO widmet sich ein Abschnitt dieses Kapitels der **Umsetzung der Datenschutz-Compliance**. Dabei werden zunächst die **zentralen Datenschutzprozesse** dargestellt, wie sie sich im Schwerpunkt insbesondere für die Energiewirtschaft ergeben und aus denen sich zahlreiche konkrete Handlungsempfehlungen ableiten lassen.[5] Neben Datenschutzprozessen bedarf es jedoch auch organisatorischer Strukturen zur Umsetzung der Anforderungen, was durch Erläuterung der **zentralen Datenschutzstrukturen** aufgezeigt wird.[6] Ein weiterer Teil widmet sich der **Datenschutzdokumentation**, die für den Verantwortlichen gemäß der DS-GVO in vielen Fällen verpflichtend ist.[7] Ohne entsprechendes **Datenschutzbewusstsein und Schulungen** der Mitarbeiter lassen sich die vielfältigen datenschutzrechtlichen Vorgaben nicht umsetzen, was in einem weiteren Abschnitt aufgezeigt wird.[8] Die **Überwachung des Datenschutzes und Rechtsfolgen bei Verstößen** beschließen dieses Kapitel.[9]

---

3 Vgl. hierzu den Überblick bei Theobald/Kühling/*Bartsch*, Energierecht, Datenschutz, Rn 121 ff.

4 Vgl. ausführlich Wecker/van Laak/*Bauer*, Compliance in der Unternehmenspraxis, S. 170; *Bauer*, WISO 2009, 504 ff.

5 Siehe dazu Rn 15 bis 97.

6 Siehe dazu Rn 98 bis 111. Zu den insoweit praktisch relevanten unternehmensinternen Richtlinien und sonstigen Maßnahmen vgl. schon Kap. 6.

7 Siehe dazu Rn 112 bis 122.

8 Siehe dazu Rn 123 bis 132.

9 Siehe dazu Rn 133 bis 146.

Kapitel 12
Cyberkriminalität und Cybersicherheit

A. Vormerkungen

In dem nachfolgenden Text soll die Cyberkriminalität in all ihren Aspekten betrachtet werden. Gleichzeitig werden Handlungsempfehlung für Unternehmen und Behörden gegeben, um Cyberprävention umzusetzen. 1

Dazu bedarf es einer Betrachtung des Lagebildes Cyberkriminalität, das unterschiedliche Erkenntnisse umfasst. Neben der Sicht auf technische Vorgehensweisen darf man nicht außer Acht lassen, dass die Komponenten „Mensch" (Ausbildung, Bewusstsein, Innentäter) und „Compliance" (zusätzliche Sicherungserfordernisse der Digitalisierung, der Geschäftsprozesse und des täglichen Arbeitens in einer digitalisierten Welt) ebenfalls eine entscheidende Rolle für die Sicherheit im Netz spielen. Es sind modi operandi zu betrachten, die die jeweilige Basis für wirksame Präventionsmaßnahmen schaffen. Um die richtigen Maßnahmen zu treffen, muss – wie bereits angeführt – natürlich das aktuelle Lagebild herangezogen werden. 2

Offizielle **Lagebilder** werden durch das Bundesamt für Sicherheit in Informationstechnik (BSI) und das Bundeskriminalamt (BKA) erstellt. Ein überwiegender Nachteil bei diesen Lagebildern liegt darin, dass jeweils retrograde Betrachtungen über das vergangene Jahr vorgenommen werden. Die Inhalte des jeweiligen Jahreslagebildes sind vielfach dann bereits ein Jahr alt und das ist bei der Schnelllebigkeit der Handlungen im Netz für eine zielorientierte Bewertung und die Schaffung eines effizienten Abwehrsystems gegen Angriffe nicht erfolgreich. 3

Um wirkungsvoll Angriffe abwehren zu können, sind aktuelle Erkenntnisse unerlässlich. Aktuelle Lagebilder können durch Zusammenarbeit mit Unternehmen und Behörden erstellt werden, die darauf spezialisiert sind, technische Aspekte der Cyberkriminalität zeitnah zu beobachten und Präventionsmaßnahmen zu erarbeiten. 4

Damit Unternehmen aus all diesen Informationsquellen für sich eine eigene aktive Präventionsstrategie umsetzen können, erhalten sie Unterstützung von den Unternehmen, die sich auf die Erhebung aktueller Abläufe und Angriffe im Netz spezialisiert haben oder von Vereinen wie „G4C – German Competence Centrum of Cyber Crime e.V.". 5

Als eigenständiger, operativ tätiger, gemeinnütziger Verein ist G4C Know-how-Träger, Frühwarnsystem und Informationsplattform, in dem wichtige Erkenntnisse über aktuelle Bedrohungen ausgetauscht werden. Die Mitglieder wie Banken und Versicherungen bilden eine Interessensgemeinschaft, um sich gegen Verbrechen im Cyberraum zur Wehr zu setzen. 6

Prävention von Cyberkriminalität funktioniert aber nur in Kooperation. Das BKA und das BSI sind bei G4C in diese Kooperation eng eingebunden. 7

https://doi.org/10.1515/9783110670493-012

B. Cyberkriminalität im engeren Sinne

8 Unter diese Zuordnung fällt der **Computerbetrug**. Dieses Delikt wird seit 1.1.2016 in folgende Betrugsarten aufgeschlüsselt:

- betrügerisches Erlangen von Kraftfahrzeugen gem. § 263a StGB[1],
- weitere Arten des Kreditbetruges gem. § 263a StGB,
- Betrug mittels rechtswidrig erlangter Daten von Zahlungskarten gem. § 263a StGB,
- Betrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel gem. § 263a StGB,
- Leistungskreditbetrug gem. § 263a StGB,
- Abrechnungsbetrug im Gesundheitswesen gem. § 263a StGB,
- Überweisungsbetrug gem. § 263a StGB,
- sonstiger Computerbetrug gem. § 263a Abs. 1 und 2 StGB sowie
- Vorbereitungshandlungen gem. § 263a Abs. 3 StGB (soweit nicht unter die nachfolgenden Betrugsarten bzw. die „Missbräuchliche Nutzung von Telekommunikationsdiensten" gefasst),
- das Ausspähen und Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei (§§ 202a, 202b, 202c, 202d StGB) umfasst den Diebstahl und die Hehlerei digitaler Identitäten, Kreditkarten-, E-Commerce- oder Kontodaten (z.B. Phishing).
- Die entwendeten Daten werden in der Regel als Handelsware in der „Underground Economy" zum Kauf angeboten und täterseitig missbräuchlich eingesetzt. Die Verwertung erfolgt damit in zwei Stufen: dem Verkauf der Daten und dem betrügerischen Einsatz erworbener Daten. Auf beiden Ebenen werden erhebliche Gewinne generiert.
- Die Straftatbestände Fälschung beweiserheblicher Daten bzw. Täuschung im Rechtsverkehr (§§ 269, 270 StGB) beinhalten die Täuschung (einer Person) durch die Fälschung von Daten. Durch einen Dateninhaber werden Daten gefälscht bzw. verfälscht und zur Täuschung im Rechtsverkehr genutzt. Dies geschieht z.B. durch die Zusendung von E-Mails unter Vorspiegelung realer Identitäten oder Firmen. Unter Vortäuschung einer Legende soll der Geschädigte z.B. zur Preisgabe von Account-Informationen, Kreditkartendaten oder auch zu Zahlungen bewegt werden. Ebenso erfasst ist das Zusenden von als Rechnungen getarnter Schadsoftware in E-Mail-Anhängen.
- Bei Datenveränderung/Computersabotage (§§ 303a, 303b StGB) handelt es sich um eine Art digitale Sachbeschädigung. Es wird die Veränderung von Daten in einem Datenverarbeitungssystem bzw. das Verändern des Systems durch ande-

1 Strafgesetzbuch v. 13.11.1998 (BGBl. I S. 3322), zuletzt geändert durch Gesetz v. 19.6.2019 (BGBl. I S. 844).

Kapitel 13
Kartellrecht

A. Überblick

Unternehmen, die mit anderen Unternehmen um Absatzmärkte und Kunden konkurrieren, sind in ihrem Marktverhalten prinzipiell frei, solange sie dabei mit den herkömmlichen Mitteln des Leistungs- und Produktwettbewerbs agieren. Dies ist ein fundamentales Grundprinzip freier Marktwirtschaft in Deutschland und Europa. Produkte oder Dienstleistungen sollen sich über Qualität und Preis durchsetzen, sich also entsprechend der Nachfrage ihren Absatz erschließen. Dieser unternehmerischen Freiheit werden jedoch durch unterschiedliche Wettbewerbsregeln, insbesondere aus dem Kartellrecht, Grenzen gesetzt: Der Wettbewerb, die hieran teilnehmenden Akteure und nicht zuletzt der Verbraucher sollen durch den Einsatz wettbewerbsfremder Mittel keinen Schaden nehmen. **1**

Inzwischen entspricht es allgemeiner Auffassung, dass sich eine umfassende Compliance zwingend auch auf den Bereich des Kartellrechts zu erstrecken hat. Verstöße hiergegen können mit empfindlichen Nachteilen für das Unternehmen verbunden sein. Ausgehend von einem Blick auf die Bedeutung des Kartellrechts,[1] auf die besondere Motivation seiner Beachtung und auf die Ziele einer kartellrechtlichen Compliance[2] beschäftigt sich dieses Kapitel mit wesentlichen Vorgaben[3] und Rechtsfolgen[4] des Kartellrechts. Praktische Hinweise schließen diese Darstellung ab.[5] **2**

B. Bedeutung des Kartellrechts am Beispiel der Energiewirtschaft

In der liberalen Marktwirtschaft fußt die Funktionsfähigkeit von Wettbewerb grundlegend auf einem Wechselspiel von Angebot und Nachfrage, über die sich Produkte und Preise im Markt etablieren. Sowohl ein „zu viel" (Extremfall: vollkommene Konkurrenz) als auch ein „zu wenig" (Extremfall: Monopol) an Wettbewerb kann dabei jedoch wohlfahrtsökonomisch schädlich sein.[6] Ordnungspolitisch nehmen **3**

1 Vgl. Rn 3 ff.
2 Vgl. Rn 7 ff und 12 f.
3 Vgl. Rn 14 ff.
4 Vgl. Rn 49 ff.
5 Vgl. Rn 102 ff.
6 Grundlegend zur Angebotsmacht zwischen vollkommener Konkurrenz und Monopol aus wettbewerbsökonomischer Sicht Wiedemann/*Ewald*, Kartellrecht, § 7 Rn 26 ff.

https://doi.org/10.1515/9783110670493-013

vor allem solche Märkte eine Sonderstellung ein, die auf Infrastrukturangeboten basieren, wie sie etwa in den Bereichen der Energieversorgung, der Telekommunikation, des Postwesens und des Bahnverkehrs vorzufinden sind. Kennzeichnend für die wettbewerbliche Bewertung solcher Märkte ist ein Spannungsverhältnis gegenläufiger Effekte auf Anbieter- und Abnehmerseite. So besteht einerseits die Gefahr von Marktmacht bzw. Abhängigkeiten, wenn Infrastruktur in der Hand weniger oder gar einzelner Unternehmen gebündelt wird. Andererseits ist es vielfach ökonomisch wenig sinnvoll, einen unbeschränkten Wettbewerb paralleler Infrastrukturen vorzuhalten, weil Mehrkosten aus hierfür notwendigen Investitionen beim Verbraucher landen. Die Aufgabe des Kartellrechts ist es, in solchen, aber ganz grundsätzlich auch auf herkömmlichen Produktmärkten, funktionsfähigen Wettbewerb zu ermöglichen oder dort wohlfahrtsschädliche Auswüchse zu verhindern, wo der Wettbewerb gestört ist.

4 Exemplarisch für die grundsätzlichen Schwierigkeiten, Infrastrukturmärkte kartellrechtlich „in den Griff" zu bekommen bzw. auf diesen einen gesunden Wettbewerb zu ermöglichen, steht die Energiewirtschaft: Auf den Märkten der Strom- und Gasversorgung bestand bis 1998 quasi kein Wettbewerb. Die Abnehmer hatten aufgrund der – (kartell-)rechtlich sogar abgesicherten – Gebietsmonopole nebst einer klar vorgezeichneten Lieferantenkette keine Möglichkeit, ihren Strom- bzw. Gasanbieter frei zu wählen und auf andere als den örtlich etablierten Versorger zurückzugreifen.[7] Lange Zeit überwog die Ansicht, dass Wettbewerb in der Energieversorgung volkswirtschaftlich schädlich sei, weil der Aufbau paralleler Versorgungsstrukturen die Verbraucher mit Mehrkosten belasten würde.[8] Um die befürchteten Schäden abzuwenden, gestattete es der Gesetzgeber den Energieversorgern, die Belieferung ihrer Kunden durch langfristige Demarkationsverträge mit anderen (angrenzenden) Versorgern, Vertriebsabreden, Weiterverkaufsverbote und langfristige Lieferantenbeziehungen abzusichern. Dies alles wurde mit Blick auf eine sichere und preisgünstige Versorgung unter dem früheren § 103 GWB a.F. kartellrechtlich gebilligt. Erst mit der Neufassung des Energiewirtschaftsgesetzes (EnWG)[9] und der begleitenden Novelle des Gesetzes gegen Wettbewerbsbeschränkungen[10] im April 1998 wurde der Startschuss für die Liberalisierung der deutschen Strom- und Gaswirtschaft gesetzt. Ihren Ausgangspunkt nahm diese Entwicklung dabei auf europäischer Ebene, wo zuvor mit der Richtlinie 96/92/EG betreffend gemeinsame Vor-

7 Theobald/Kühling/*Judith*, Energierecht, B1 WettR, Rn 1 m.w.N.; *Funk*/*Millgramm*/*Schulz*, Wettbewerbsfragen, S. 69 ff.; vgl. auch die umfassende Darstellung bei *Zenke*, Genehmigungszwänge, S. 92 ff.

8 Ausdrücklich BT-Drucks. 8/2136, S. 17.

9 Energiewirtschaftsgesetz (EnWG) v. 24.4.1998 (BGBl. I S. 730).

10 Sechstes Gesetz zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen (6. GWB-Novelle) v. 26.8.1998 (BGBl. I S. 2521).

Kapitel 15
Tax-Compliance-Management-System

A. Einleitung

Steuerliche Betriebsprüfungen verlaufen heute weitaus kritischer als früher. Unternehmen sehen sich immer häufiger mit Vorwürfen durch die Bußgeld- und Strafsachenstellen konfrontiert. Das weitere Vorgehen der Behörden hängt von der Frage ab, wie es verfahrensrechtlich zu werten ist, wenn Sachverhalte aufgedeckt werden, die bisher entweder gar nicht, nicht vollständig oder falsch deklariert worden sind. Handelt es sich bei der anstehenden Korrektur der Steuererklärung noch um eine (strafrechtlich nicht relevante) Berichtigung nach § 153 AO[1] oder ist damit schon ein steuerstrafrechtlicher Vorwurf verbunden? **1**

Das Steuerrecht ist komplex. Die Gesetzgebung ist umfangreich. Und von der Steuer erfasst wird nahezu jeder Sachverhalt im Unternehmen, sowohl der Einzelfall als auch das Massengeschäft. Lässt es sich bei dieser Ausgangslage wirklich vermeiden, dass dabei mal eine Sache „durchrutscht"? Und was ist, wenn es dann doch einmal passiert ist? Trotz größter Sorgfalt sind Fehler bei der Abgabe von Steuererklärungen bzw. -anmeldungen nicht auszuschließen. **2**

Die Antwort auf diese Fragen hat in den letzten Jahren einen erheblichen Wandel durchlaufen. In dieser Gemengelage hat die Finanzverwaltung dem Steuerpflichtigen eine goldene Brücke gebaut: Das Vorhandensein eines wirksamen Tax-Compliance-Management-Systems („**Tax CMS**") kann ein wesentlicher Baustein zur Begrenzung von Haftungsrisiken für Unternehmen, Geschäftsführung und Mitarbeiter sein. **3**

Was allerdings die Ausgestaltung und den Aufbau eines wirksamen Tax CMS angeht, gibt die Finanzverwaltung[2] den Unternehmen keine Hilfestellung. Allein aus dem Praxishinweis 1/2016 des IDW zum PS 980 vom 31.5.2017[3] lassen sich anhand der sieben Grundelemente die Leitplanken eines wirksamen Tax CMS ableiten. Dies ist der Rahmen, in dem die Unternehmen selbst die Standards für die Umsetzung setzen (können). **4**

---

1 Abgabenordnung (AO) v. 1.10.2002 (BGBl. I S. 2003, I S. 61) zuletzt geändert durch Gesetz v. 21.12. 2019 (BGBl. I S. 2875).

2 Näheres hierzu unter Rn 6 und 7 ff.

3 Näheres hierzu unter Rn 15 ff.

https://doi.org/10.1515/9783110670493-015

B. Rechtsrahmen für die Ausgestaltung eines Tax CMS

5 Der Rechtsrahmen für die Ausgestaltung eines Tax CMS leitet sich ab aus § 153 AO, dem Schreiben des Bundesfinanzministeriums zu § 153 AO vom 16.5.2016 (nunmehr Anwendungserlass-Abgabenordnung (AEAO) zu § 153 – Berichtigung von Erklärungen (**„AEAO zu § 153“**) und dem IDW Praxishinweis 1/2016 vom 31.5.2017.

I. § 153 AO

6 Aus § 153 AO selbst ergibt sich kein Hinweis auf die Erforderlichkeit eines Tax CMS. § 153 AO hat folgenden Wortlaut:

> „(1) Erkennt ein Steuerpflichtiger nachträglich vor Ablauf der Festsetzungsfrist,
> 1. dass eine von ihm oder für ihn **abgegebene Erklärung unrichtig oder unvollständig** ist und dass es **dadurch zu einer Verkürzung von Steuern kommen kann oder bereits gekommen ist** oder
> 2. dass eine durch Verwendung von Steuerzeichen oder Steuerstemplern zu entrichtende Steuer nicht in der richtigen Höhe entrichtet worden ist,
>
> so ist er verpflichtet, dies unverzüglich anzuzeigen und die erforderliche Richtigstellung vorzunehmen. Die Verpflichtung trifft auch den Gesamtrechtsnachfolger eines Steuerpflichtigen und die nach den §§ 34 und 35 für den Gesamtrechtsnachfolger oder den Steuerpflichtigen handelnden Personen.
> (2) Die Anzeigepflicht besteht ferner, wenn die Voraussetzungen für eine Steuerbefreiung, Steuerermäßigung oder sonstige Steuervergünstigung nachträglich ganz oder teilweise wegfallen.
> (3) Wer Waren, für die eine Steuervergünstigung unter einer Bedingung gewährt worden ist, in einer Weise verwenden will, die der Bedingung nicht entspricht, hat dies vorher der Finanzbehörde anzuzeigen.“

II. Schreiben des BMF vom 23.5.2016

7 Die Anwendung des § 153 AO wird flankiert durch das **Schreiben des Bundesfinanzministeriums vom 23.5.2016**.[4] Der Schwerpunkt der Ausführungen liegt auf der Abgrenzung der Berichtigung nach § 153 AO von einer strafbefreienden Selbstanzeige.

8 Beiden Erklärungen gemein ist, dass eine **im Zeitpunkt der Abgabe objektiv unrichtig Steuererklärung** voranging. Ob eine Richtigstellung durch den Steuerpflichtigen als Berichtigung einer Erklärung nach § 153 AO oder eine strafbefreiende Selbstanzeige einzuordnen ist, richtet sich also nach dem **subjektiven Tatbestand.**

---

4 Nunmehr Anwendungserlass-Abgabenordnung (AEAO) zu § 153 – Berichtigung von Erklärungen.