Compliance-Risikomanagement

Kark

3. Auflage 2024
ISBN 978-3-406-79180-2
C.H.BECK

nen. Zum anderen ist es für die Kommunikation von Compliance-Risiken durch Mitarbeiter sehr viel förderlicher, wenn durch ein kompetentes, partnerschaftliches Auftreten der Compliance Officer ein Klima geschaffen wird, in dem es ihnen leichter fällt, auch schwierige Compliance-Situationen zu adressieren. Bereits in diesem frühen Stadium des Compliance-Risikomanagements entscheidet sich, ob die Compliance Officer durch die Mitarbeiter als Unterstützung wahrgenommen werden oder ob deren Tätigkeit eher als eine polizeiliche Überwachungsfunktion gefürchtet wird.

732 Wie auch bei klassischen Unternehmensrisiken gilt auch bei der Identifikation von Compliance-Risiken, dass man mögliche Ereignisse, die unter Umständen in der Zukunft stattfinden könnten, aufgreifen, dokumentieren und einem Bewertungs- und Risikosteuerungsprozess zuführen muss. Mangels perfekter Informationen über die Zukunft sind damit Unsicherheiten und Ungenauigkeiten verbunden und die subjektive Sicht des Einzelnen spielt eine nicht unerhebliche Rolle, je nachdem wie risikoavers der Mitarbeiter ist.

733 Dies gilt auch für Compliance-Risiken, vielleicht sogar noch mehr als für klassische Unternehmensrisiken, da Mitarbeiter, die bisher keine Gelegenheit hatten, sich mit diesen Themen zu befassen, noch keinen rechten Maßstab entwickeln konnten, für das was rechtlich noch akzeptabel ist oder jenseits dieser Grenze liegt. Auch wenn sie ein gesundes Rechtsverständnis mitbringen, so verschließen sich nicht selten maßgebliche Rechtsvorschriften genau diesem Zugang, wie dies in vielen Diskussionen zu Tage tritt, in welchen Nichtjuristen auf gesetzliche Regelungen mit kopfschüttelndem Unverständnis reagieren.

734 Auch dies sollte man beachten, wenn man nach einer Einführung dieses Prozesses das Ergebnis einer erstmaligen Identifikation von Compliance-Risiken betrachtet. Je mehr sich die Mitarbeiter daran gewöhnt haben, dass sie, und nicht eine ferne Compliance- oder Rechtsabteilung, für die rechtliche Korrektheit der Geschäftsabläufe in ihrem Verantwortungsbereich verantwortlich sind, umso besser werden die Ergebnisse der Identifikation von Compliance-Risiken sein.

Checkliste 25: Der Prozess des Compliance-Risikomanagements

- ❑ Hat die Unternehmensleitung, in Abhängigkeit von Branche, Größe sowie der Komplexität und des Grades der Internationalisierung der Gesellschaft, definiert, **welche Compliance-Risiken** zu betrachten sind?
- ❑ Wird im Unternehmen verdeutlicht, dass das Management von Compliance-Risiken sehr wichtig ist?
- ❑ Hat die **Geschäftsleitung** eigene Vorstellungen über mögliche Compliance-Risiken?
- ❑ Bestehen Geschäftsbeziehungen des Unternehmens zu **Hochrisikoländern?**
- ❑ Werden die Mitarbeiter vor einer Risikoabfrage mit dem Grundgedanken der Wichtigkeit von Compliance vertraut gemacht, zB iRv **Compliance-Schulungen?**
- ❑ Unterhält das Unternehmen ein immer **aktuelles Verzeichnis** der für das Unternehmen maßgeblichen **Gesetze** (Rechtskataster)?
- ❑ Werden entsprechende **Ressourcen** bereitgestellt, um den Prozess des Compliance-Risikomanagements adäquat zu begleiten?
- ❑ Wird ein Netzwerk **lokaler Compliance Officer** in den jeweiligen Geschäftsbereichen und Tochtergesellschaften aufgebaut?
- ❑ Werden die lokalen Compliance Officer von der jeweiligen Geschäftsleitung vor Ort **autorisiert,** ihre Kollegen zu Compliance-Themen zu befragen und diese zu beraten?
- ❑ Werden die Compliance Officer **regelmäßig geschult?**
- ❑ Wird der zentrale Compliance-Bereich **organisatorisch richtig angesiedelt** (CEO/CFO)?
- ❑ Werden alle Ergebnisse des Compliance-Risikomanagementprozesses ordnungsgemäß **dokumentiert?**
- ❑ Stellt der Prozess sicher, dass alle Compliance-Risiken erfasst werden, auch wenn die einzelnen Mitarbeiter **keine spezifischen juristischen Fachkenntnisse** besitzen?

- ❑ Werden **alle Informationsquellen** zur Identifizierung von Compliance-Risiken berücksichtigt?
- ❑ Erhalten die operativen Bereiche eine **Liste** der Informationsquellen, die sie ggf. nutzen können, um Compliance-Risiken zu identifizieren?
- ❑ Ist sichergestellt, dass die im Rahmen einer Risikoabfrage erhobenen Informationen **keiner Filterung** durch die operativen Geschäftsbereiche unterzogen worden sind?
- ❑ Werden alle gemeldeten Compliance-Risiken übersichtlich **dokumentiert,** sodass sie einer **Analyse** und **Bewertung** unterzogen werden können?
- ❑ Wird für eine unternehmensinterne Lösung bei der Implementierung eines **Hinweisgebersystems** ein Mitarbeiter des Unternehmens oder ein externer Compliance-Ombudsmann bestellt oder wird eine interne Hybridlösung umgesetzt?
- ❑ Wird zusätzlich eine externe, behördliche Lösung gewählt?
- ❑ Werden die Vorgaben des **Hinweisgeberschutzgesetzes** vollständig umgesetzt?
- ❑ Verfügt das Unternehmen über ein anonymes Hinweisgebersystem, und wenn nicht, warum?[464]
  - Wurde eine **Richtlinie** zum Compliance-Hinweisgebersystem erstellt?
  - Wie wurden Mitarbeiter und Dritte über die Existenz des Hinweisgebersystems **informiert?**
  - Ist der **Prozess der Bearbeitung** eingehender Hinweise definiert?
  - Wurde das Hinweisgebersystem genutzt?
  - Validiert das Unternehmen, ob die Mitarbeiter das Hinweisgebersystem kennen und sich bei dessen Nutzung wohl fühlen?
  - Wie geht das Unternehmen vor, wenn es darum geht, die Schwere der eingegangenen Anschuldigungen zu bewerten?
  - Hatte die Compliance-Funktion uneingeschränkten Zugang zu den Berichts- und Untersuchungsinformationen?
- ❑ Wurde eine dem Sachverhalt angemessene Untersuchung durch **kompetentes Personal** durchgeführt?
  - Wie stellt das Unternehmen fest, welche Hinweise oder Verdachtsmomente eine weitere Untersuchung erfordern?
  - Wie stellt das Unternehmen sicher, dass die **Untersuchungen** einen angemessenen **Umfang** haben?
  - Welche Schritte unternimmt das Unternehmen, um sicherzustellen, dass die Untersuchungen unabhängig, objektiv und angemessen durchgeführt sowie ordnungsgemäß dokumentiert werden?
  - Wie bestimmt das Unternehmen, durch wen eine Untersuchung durchgeführt werden sollte und wer trifft diese Entscheidung?
- ❑ War die **Vorgehensweise** bei der internen Untersuchung angemessen?
  - Wendet das Unternehmen zeitliche Kriterien an, um die Reaktionsfähigkeit zu gewährleisten?
  - Verfügt das Unternehmen über ein Verfahren zur Überwachung der Untersuchungsergebnisse und zur Sicherstellung der Verantwortlichkeit für die Reaktion auf etwaige Feststellungen oder Empfehlungen?
- ❑ Wie stellte sich der **Ressourceneinsatz** und das Ergebnis der Nachbearbeitung dar?
  - Wurde das Hinweisgebersystem und die interne Untersuchung ausreichend mit Ressourcen durch das Unternehmen ausgestattet?
  - Wie hat das Unternehmen Informationen aus seinem Berichtswesen gesammelt, verfolgt, analysiert und genutzt?

[464] Fragen in Anlehnung an DoJ/Criminal Division, Evaluation of Corporate Compliance Programs (Updated March 2023), https://www.justice.gov/criminal-fraud/page/file/937501/download, S. 5 ff., zuletzt aufgerufen am 5.8.2023.

- Analysiert das Unternehmen die Berichte oder Untersuchungsergebnisse regelmäßig auf Muster von Fehlverhalten oder andere Anzeichen für Compliance-Verstöße?
- Wird die Wirksamkeit des Hinweisgebersystems in regelmäßigen Abständen durch das Unternehmen zB durch die Verfolgung einer Meldung von Anfang bis Ende, geprüft.

❑ Wurden die **Folgen** im Fall eines Compliance-Verstoßes **beschrieben** (einschließlich daraus für das Compliance-Managementsystem zu ziehender Lehren)?
❑ Wurde die **Berichterstattung** an die Geschäftsleitung definiert?

2. Informationsrücklauf und Dokumentation der Compliance-Risiken

Wurden unter Ausnutzung der verschiedensten Informationsquellen Compliance-Risiken identifiziert, so werden diese dokumentiert und an die abfragende Stelle zurückgemeldet. 735

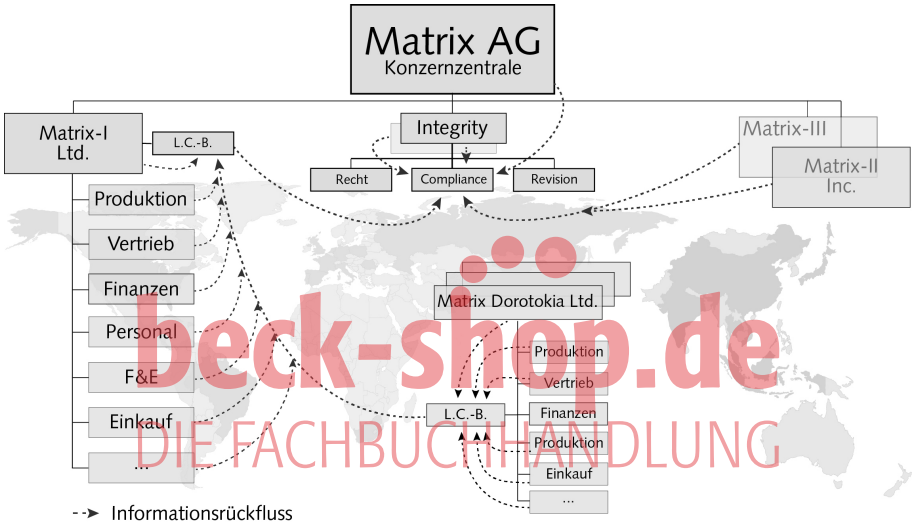

Abb. 15: Die Matrix AG: Die Rückmeldung der Compliance-Risiken

Das bedeutet, dass die Compliance-Verantwortlichen auf der Ebene von Tochtergesellschaften, wie zB der Matrix Dorotokia Ltd. aus allen Bereichen des Unternehmens Informationen über mögliche Compliance-Risiken erhalten. Abhängig von dem Grad der Zentralisierung der Compliance-Arbeit des Unternehmens findet nach der Dokumentation auch die Analyse und Bewertung auf der Ebene des lokalen Compliance-Verantwortlichen statt oder die Informationen über identifizierte Compliance-Risiken werden an die abfragende Stelle, in unserem Beispiel an den lokalen Compliance Officer der Matrix-I Ltd. weitergeleitet. 736

Zur Beschleunigung des Ablaufs ist auch eine Hybridversion des Prozesses denkbar: In einem ersten Schritt werden die Informationen über Compliance-Risiken vor Ort, in diesem Fall der Matrix Dorotokia Ltd., analysiert und bewertet. In einem zweiten Schritt werden die dokumentierten Ergebnisse dieses Prozesses vollständig, dh die Dokumentation aller identifizierten Compliance-Risiken sowie deren Analyse und Bewertung an den lokalen Compliance Officer der Matrix-I Ltd. gesendet. Dieser kann auf Basis der Analyse entscheiden, ob er diese in seine eigene Analyse der Compliance-Risiken des gesamten Geschäftsbereichs aufnimmt oder zunächst eine Überprüfung des Datenmaterials der Tochtergesellschaft vornimmt.

737 Beim lokalen Compliance Officer der Matrix-I Ltd. laufen in diesem Verfahren erhebliche Datenmengen zusammen. Nicht nur liefern diverse Tochtergesellschaften Informationen über identifizierte Compliance-Risiken. Auch aus der Zentrale des Geschäftsbereichs senden die verschiedenen Funktionalbereiche ihre Antworten auf die Abfrage der Compliance-Risiken. Ähnlich wie auf der Ebene der Tochtergesellschaften, kann eine weitere Analyse und Bewertung der Informationen auf der Geschäftsbereichsebene erfolgen, von deren Ergebnisse das zentrale Compliance-Management sodann informiert wird. Alternativ sind ebenfalls eine einfache Durchleitung der Informationen an die zentrale Compliance-Abteilung oder eine Hybridversion denkbar.

738 Es ist jedoch für die Qualität der weiteren Prozessschritte von Bedeutung, dass in diesem frühen Stadium der Identifikation der Compliance-Risiken des Unternehmens das Ergebnis nicht nach größeren Compliance-Risiken gefiltert wird, die man dokumentieren sollte, und kleineren, unmaßgeblichen Risiken, die keine weitere Erwähnung finden brauchen.

739 Zum einen sollte aus Sicht der Qualität des Risikomanagementprozesses eine frühzeitige Filterung des Ergebnisses ohne einen entsprechenden Prozess unterbleiben. Es ist dabei zunächst einerlei, ob dieser nächste Schritt auf der Ebene der Tochtergesellschaften, Geschäftsbereiche oder in der zentralen Compliance-Abteilung vollzogen wird. Wichtig ist dabei vielmehr, dass die Analyse und Bewertung und die damit einhergehende Filterung in beachtenswerte und nicht beachtenswerte Compliance-Risiken nur auf Basis eines systematischen, transparenten und auch für Dritte nachvollziehbaren Prozesses erfolgt. Die Auswahl muss daher dem folgenden, separaten Prozessschritt, der Analyse und Bewertung der Compliance-Risiken, vorbehalten bleiben.

740 Zum anderen wäre es aus Compliance-Sicht unklug, identifizierte Risiken nicht zu dokumentieren. Schlägt ein solches Risiko in einen Schaden um, kann sich die Frage stellen, warum dieses Risiko, ohne das Ergebnis des dafür vorgesehenen Prozessschrittes abzuwarten, aus der weiteren Risikobetrachtung entfernt worden ist. Damit kann sowohl die Qualität des gesamten Compliance-Risikomanagementprozesses in Frage gestellt als auch ein unnötiger Verdacht auf eine gezielte Manipulation des Prozesses ausgelöst werden.

741 Daher sollten identifizierte Compliance-Risiken so vollständig wie möglich und in einer für Dritte nachvollziehbaren Weise **dokumentiert** werden. Am Ende dieses Prozessabschnittes steht dem Unternehmen eine Liste aller identifizierten Compliance-Risiken zur Verfügung.

III. Analyse und Bewertung der Compliance-Risiken

742 Die identifizierten Compliance-Risiken werden in einem weiteren Prozessschritt einer inhaltlichen Analyse unterzogen. Um zu einer Priorisierung der Compliance-Risiken zu gelangen, sind sodann die möglichen Folgen dieser Risiken zu quantifizieren.

1. Analyse der Compliance-Risiken

743 Zunächst sind die erfassten Compliance-Risiken zu sichten. Je größer das Unternehmen ist, umso komplexer wird diese Aufgabe. Auch hier bietet es sich an, eine Gruppierung der Compliance-Risiken vorzunehmen. Diese kann zB nach regionalen Gesichtspunkten erfolgen oder sich an den zugrundeliegenden Sachverhalten orientieren.

744 Eine Aufteilung der Compliance-Risiken, die in als Hochrisikoländern definierten Staaten identifiziert wurden, bietet den Vorteil, dass leicht Quervergleiche gezogen werden können. So können Antworten auf die Compliance-Risikoabfrage gezielt hinterfragt werden. Hat zB die Matrix Dorotokia Ltd. Compliance-Defizite identifiziert, die in einem ähnlich risikoreichen zweiten Marktgebiet jedoch nicht als Risiken gemeldet worden sind, sollte dies Anlass genug für die Compliance Officer sein, die Verantwortlichen dieses zwei-

ten Marktgebietes zu fragen, ob sie sich sicher sind, dass kein derartiges Compliance-Risiko vorhanden ist.

Die Gliederung der identifizierten Compliance-Risiken im Rahmen einer Zuordnung nach Geschäfts- bzw. Funktionalbereichen bietet den Vorteil, dass ähnlich gelagerte Geschäfte oder Fachfunktion mit vergleichbaren Compliance-Risiken konfrontiert werden. Auch kann es, je nach Unternehmen, sinnvoll sein, die identifizierten Risiken den einzelnen Stufen der Wertschöpfungskette zuzuordnen. Dadurch würden Compliance-Risiken zB im Vertrieb, unabhängig von der regionalen oder produktspezifischen Kategorisierung in Gruppen zusammengefasst und einer weiteren Analyse zugänglich gemacht. 745

Natürlich sind eine Vielzahl anderer Möglichkeiten gegeben, unternehmensspezifische Compliance-Risiken zu strukturieren und einer weiteren Analyse, die den konkreten Bedürfnissen und Anforderungen des Unternehmens Rechnung trägt, zuzuführen. Wichtig ist jedoch, unabhängig von der Art der Strukturierung der Compliance-Risiken, dass sie den beteiligten Bereichen gestattet, durch Quervergleiche mögliche Defizite im Prozess der Compliance-Risikoidentifikation aufzudecken. Darüber hinaus sollte es die Gliederung ermöglichen, eine **Kumulation** von Compliance-Risiken zu erkennen. Verantwortet zB eine Tochtergesellschaft den Vertrieb von unterschiedlichen Produktreihen in einem **Hochrisikoland,** so ist das Korruptionsrisiko bereits hoch genug, wenn ein Produkt ausschließlich an Behörden verkauft wird. Stellt sich jedoch heraus, dass die weitere Produktpalette Abnehmer u. a. auch in öffentlichen Einrichtungen findet, kann das Compliance-Risiko für die Tochtergesellschaft bestandsgefährdende Ausmaße erreichen. 746

Checkliste 26: Analyse der Compliance-Risiken

- ❑ Werden die identifizierten Compliance-Risiken entsprechenden **Kategorien** zugeordnet, sodass sie optimal gesichtet und analysiert werden können?
- ❑ Gibt es eine Aufteilung zwischen Compliance-Risiken der **Funktionalbereiche** und jenen der **operativen Einheiten?**
- ❑ Werden **Querverbindungen hergestellt** zwischen Risiken, die zum Beispiel in einem Hochrisikoland gemeldet worden sind, in anderen jedoch nicht?
- ❑ Wird eine Gliederung der Compliance-Risiken entlang der **Wertschöpfungskette** vorgenommen?
- ❑ Können durch die Kategorisierung eventuelle **Defizite** im Prozess der Compliance-Risikoidentifikation einzelner Bereiche aufgedeckt werden?
- ❑ Stellt die Kategorisierung der Compliance-Risiken sicher, dass **Kumulationen** erkennbar werden?

2. Bewertung identifizierter Compliance-Risiken

Ist die Bewertung klassischer Unternehmensrisiken weder einfach noch frei von Unsicherheiten, wird diese Aufgabe bei Compliance-Risiken nicht gerade leichter. Dennoch kommt man nicht umhin, iRd Analyse eine Bewertung der identifizierten Risiken vorzunehmen, da nicht alle Compliance-Risiken die gleiche Bedeutung für den Fortbestand des Unternehmens haben. Vielmehr möchte man als Geschäftsleitung vorrangig denjenigen Risiken entgegenwirken, welchen ein besonders hohes Gefährdungspotential für das Unternehmen zukommt. 747

Darüber hinaus ermöglicht eine Bewertung der Compliance-Risiken eine **Priorisierung** der erforderlichen Gegenmaßnahmen und damit eine **Fokussierung** der begrenzten Unternehmensressourcen. Dadurch kann den besonders akuten und gefährlichsten Risiken gezielt und mit angemessenen Maßnahmen entgegengewirkt werden, statt Ressourcen auf die Mitigierung aller identifizierten Compliance-Risiko gleichzeitig und gleichmäßig einzusetzen. Dies kann allzu leicht dazu führen, dass die relevantesten Risiken nicht schnell und effektiv genug mitigiert werden können, während relativ unbedeutenden Risiken mit 748

der gleichen Dringlichkeit und einem vergleichbaren Ressourceneinsatz entgegengewirkt werden. Im Zweifel kann eine solche „Gießkannenmethode" dazu führen, dass mangels hinreichender Gegenmaßnahmen identifizierte Compliance-Risiken zu Compliance-Verstößen werden.

749 Regelmäßig wird die Bewertung von Compliance-Risiken durch den Umstand erschwert, dass diese, sofern sie in einen Gesetzesverstoß umgeschlagen sind, in der Öffentlichkeit anders wahrgenommen werden als Schäden, die aus klassischen Unternehmensrisiken herrühren. Wurde von einem Unternehmen zB bekannt, dass Vertreter des Unternehmens Beamte bestochen haben, um einen Auftrag zu erhalten, so kommt es nicht darauf an, in welchem Staat sich dieser Gesetzesverstoß ereignet hat. Vielmehr führt das sich nicht an die „Spielregeln" halten fast automatisch zu einem **Reputationsverlust,** der sich keineswegs nur auf das Land beschränkt, in dem der Gesetzesverstoß erfolgte. Das Unternehmen erleidet weltweit einen Reputationsverlust und wird unter Umständen die direkten wirtschaftlichen Konsequenzen zeitnah zu spüren bekommen, indem es von den verschiedenen **Stakeholdern** des Unternehmens abgestraft wird, sei es von Kunden, Lieferanten oder Aufsichtsbehörden. Aufträge werden zurückgezogen und an Wettbewerber vergeben, die Teilnahme an Ausschreibungen wird verweigert, Betriebsprüfungen durch die Finanzbehörden angeordnet und ggf. werden auch Ermittlungsverfahren eingeleitet. Damit kann dieser Gesetzesverstoß eine **Kettenreaktion** von Rechtsfolgen auslösen, die wie ein Lauffeuer ein global tätiges Unternehmen in Bedrängnis bringen kann und die zu einer weiteren Erhöhung des Reputationsschadens führt.[465]

750 Es ist daher sinnvoll, die Elemente der klassischen Unternehmensrisikobewertung, potenzielle maximale Schadenshöhe und Eintrittswahrscheinlichkeit, um die Komponente des Reputationsschadens zu ergänzen.

a) Bemessung der möglichen Gesamtschadenshöhe

751 Rechtsvorschriften sind regelmäßig mit Sanktionen in Form von Strafen oder Geldbußen sowie Gewinnabschöpfung bewehrt. Dadurch kann dem Risiko eines Compliance-Verstoßes ein konkreter Schadensbetrag, der dem Unternehmen durch diesen entstehen könnte, zugeordnet werden.

752 So sieht zB das **Kartellrecht** eine Geldbuße von bis zu **10 Prozent** des in dem der Behördenentscheidung vorausgegangenen Geschäftsjahres erzielten weltweiten Gesamtumsatzes des Unternehmens bzw. des Konzerns vor (§ 81c Abs. 2 GWB). Das **OWiG** sieht eine Geldbuße im Falle einer vorsätzlichen Straftat, die aus dem Unternehmen heraus begangen worden ist und durch die Pflichten, welche das Unternehmen treffen, verletzt worden sind oder es dadurch bereichert worden ist oder werden sollte, bis zu zehn Mio. EUR vor. Handelt es sich um eine fahrlässige Straftat, kann eine Geldbuße bis zu fünf Mio. EUR verhängt werden (§ 30 Abs. 2 OWiG). Der bisher noch nicht verabschiedete Entwurf der Bundesregierung des Gesetzes zur Stärkung der Integrität in der Wirtschaft enthält Vorschriften für ein neues **Verbandssanktionengesetz.** Gem. § 9 Abs. 2 VerSanG beträgt eine Verbandsgeldsanktion bei einem Unternehmen bzw. einem nicht rechtsfähigen Verein oder einer rechtsfähigen Personengesellschaft mit einem durchschnittlichen Jahresumsatz von mehr als 100 Mio. EUR bei einer vorsätzlichen Verbandstat mind. 10.0000 EUR und bis zu **10 Prozent** des durchschnittlichen Jahresumsatzes, bzw. bei einer fahrlässigen Verbandstat mind. 5.000 EUR und höchstens 5 Prozent des durchschnittlichen Jahresumsatzes.[466]

---

[465] S. das Beispiel zum Compliance-Risiko, bei dem eine Bestechung in China Rechtsfolgen nicht nur dort, sondern auch in Deutschland, den USA und Großbritannien nach sich zieht, → Rn. 61 ff.

[466] Bundesregierung „Entwurf eines Gesetzes zur Stärkung der Integrität in der Wirtschaft", Bearbeitungsstand: 16.6.2020 10:03 Uhr, https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/RegE/RegE_Staerkung_Integritaet_Wirtschaft.pdf?__blob=publicationFile&v=3, zuletzt abgerufen am 28.2.2023.

Darüber hinaus sehen die Vorschriften zB des StGB auch die des OWiG auch eine **Gewinnabschöpfung** vor, da sich Straftaten und Ordnungswidrigkeiten nicht lohnen dürfen (§ 73 ff. StGB sowie § 17 OWiG).[467] Die Höhe eines möglichen Verfalls mag zunächst schwer abzuschätzen sein. Doch auch hier, ähnlich wie bei anderen gravierenden Compliance-Verstößen, kann man davon ausgehen, dass es sich aus Sicht der Täter lohnen sollte. Daher kann die **Umsatzrendite** des Geschäftssegmentes, in dem ein Compliance-Risiko im Unternehmen besteht, zusammen mit dem durch das Compliance-Risiko betroffene **Geschäftsvolumen** herangezogen werden, um die Höhe der behördlichen Gewinnabschöpfung zu errechnen. 753

Darüber hinaus werden zB im Fall einer Preisabsprache die beteiligten Unternehmen von ihren übervorteilten Kunden regelmäßig auf Schadensersatz in Anspruch genommen. Auch dies ist ein zu quantifizierender Schaden, der in die Kalkulation der Gesamtschadenshöhe aufzunehmen ist. Auch hier lassen sich Näherungswerte verwenden. So geht eine Studie für die EU-Kommission auf eine kartellbedingte Verteuerung für Kunden von durchschnittlich rund 20 Prozent aus.[468] Ähnlich wie bei der Gewinnabschöpfung würde man den von der Kartellabsprache betroffenen Umsatz mit diesem Prozentwert von zB 20 % multiplizieren, um näherungsweise die zu erwartenden Schadensersatzforderungen der Kunden zu quantifizieren. 754

Noch schwieriger wird die Bewertung, wenn ggf. weitere Sanktionen, wie zB der **Ausschluss von öffentlichen Ausschreibungen** (v.g. § 124 GWB) drohen oder Kunden **Zulieferverträge** stornieren oder sich ein **Joint Venture** von einem Partner trennt, der sich einen schweren Compliance-Verstoß hat zuschulden kommen lassen.[469] Hier kann man, je nach Geschäftsmodell des betroffenen Unternehmens, durchaus zu dem Ergebnis kommen, dass in Folge solcher Sanktionen das Unternehmen in seinem Bestand gefährdet ist. 755

Von einer solchen Bedrohung des wirtschaftlichen Fortbestandes des Unternehmens ist auch auszugehen, wenn zwar jede Sanktion für sich genommen verkraftbar erscheint, diese jedoch in Summe zur Insolvenz des Unternehmens führen können. 756

Grds. sollte daher auf dieser Betrachtungsebene mit den schlimmsten anzunehmenden Sanktionsfolgen gerechnet werden. Gleiches gilt für mögliche Schadensersatzforderungen von Seiten Dritter, die durch den Compliance-Verstoß einen Nachteil erlitten haben. 757

Darüber hinaus sollten auch die internen Kosten, die durch einen Compliance-Verstoß verursacht werden, erfasst werden, selbst wenn diese vielleicht nur sehr grob geschätzt werden können. Dies kann Kosten umfassen, die zB in Zusammenhang mit einem notwendigen Produktrückruf entstehen[470] oder auch Kosten für die zusätzliche Arbeitszeit und Managementattention, die ein Ermittlungsverfahren usw. verursacht. 758

Beispiel:

Die Matrix AG hat iRd Compliance-Risikoidentifikation ein massives Risiko bei ihrer Tochtergesellschaft, der Matrix Dorotokia Ltd. entdeckt. Es steht zu befürchten, dass beim geplanten Ausbau der Fertigungshallen, der zur Erweiterung der Produktion im Hochrisikoland Dorotokia dringend erforderlich ist, Bestechungsgelder an die zuständigen Beamten der örtlichen Baubehörde und den Bürgermeister fließen könnten. Da das Unternehmen

[467] KK-OWiG/Mitsch OWiG § 17 Rn. 112 ff.

[468] Study prepared for the European Commission, Quantifying antitrust damages, Towards non-binding guidance for courts, Oxera, December 2009, S. 90, https://op.europa.eu/en/publication-detail/-/publication/fc667387-4658-48de-aa44-0f9b0dd3327d, zuletzt abgerufen am 28. 02. 2023.

[469] So zB: Nach Korruptionsaffaire: Daimler und Thyssen wenden sich von Ferrostaal ab, Augsburger Allgemeine, 9.8.2010, Daimler steigt aus Rüstungsprojekt mit Ferrostaal aus, https://www.augsburger-allgemeine.de/wirtschaft/Daimler-steigt-aus-Ruestungsprojekt-mit-Ferrostaal-aus-id8291681.html, zuletzt abgerufen am 28.10.2023.

[470] Produktüberarbeitung, Produktion, Kommunikation mit Händlern und Kunden, Austausch der bereits ausgelieferten Ware uvm.

auch über US-Dollarkonten verfügt, ist es auch völlig offen, in welcher Währung diese illegalen Zahlungen erfolgen und welchen Weg diese nehmen würden.

759 Im obigen Beispiel der Matrix AG muss der lokale Compliance Officer bei der Bewertung des Compliance-Risikos vom schlimmsten Fall ausgehen. Das bedeutet, es werden Amtsträger bestochen und die Bestechungsgelder werden in USD auf ein Konto außerhalb Dorotokias gezahlt. Damit würde gegen das Recht des Landes Dorotokia und darüber hinaus gegen deutsche, amerikanische sowie britische Anti-Korruptionsbestimmungen verstoßen, ggf. Steuer- und Bilanzierungsvorschriften sowie Bestimmungen zur Geldwäsche verletzt. Darüber hinaus würden verschiedene interne Vorschriften ignoriert.

760 Diese Betrachtungsweise zeigt, dass der Kreis der zu erwartenden Schäden relativ groß werden kann. Den Radius der möglichen Schäden zu verringern indem man zB den zeitlichen Betrachtungshorizont verkürzt oder interne Kosten vernachlässigt, die durch einen Compliance-Verstoß verursacht würden, ist ebenso wenig hilfreich wie die jeweils geringste Geldbuße bei der Bewertung des zu erwartenden Schadens einzustellen.

761 Wie auch bei der Bewertung klassischer Unternehmensrisiken sollten der zu erwartenden Schadenshöhe keine Chancen gegengerechnet werden. Denn auch wenn die Chancen das Compliance-Risiko überwiegen würden, bleibt jedoch das Risiko bestehen. Es würde daher der Transparenz des Prozesses nicht dienlich sein, wenn ein solches Compliance-Risiko unerwähnt bliebe oder nur ein Nettorisikowert anstelle des vollen erwarteten Schadensbetrages dargestellt würde.

762 Unabhängig von diesem eher systematischen Argument kommt eine solche Gegenrechnung schon aus **unternehmensethischen** Gesichtspunkten nicht in Frage. Eine Geschäftsleitung, die sich im Rahmen ihrer Anstrengungen, ein Compliance-Management-System einzuführen, um die Identifizierung der Compliance-Risiken ihres Unternehmens bemüht, kann die Ernsthaftigkeit ihres Anliegens gegenüber ihren Mitarbeitern und anderen Stakeholdern kaum glaubhaft kommunizieren, wenn sie Compliance-Risiken mit Ertragschancen aus möglicherweise rechtswidrigen Geschäftsaktivitäten aufrechnet.[471]

763 Grds. besteht bei der Bewertung von erwarteten Schäden durch Compliance-Risiken die Gefahr, dass ein erheblicher Aufwand getrieben werden müsste, um möglichst genaue Daten erheben zu können. Dieser kann vor allem bei der Neueinführung dieses Prozesses das Compliance-Risikomanagement nicht nur erheblich verlangsamen, sondern das Compliance-Risikomanagement für die gesamte Organisation so arbeitsintensiv gestalten, dass Compliance als solche negativ belegt wird.

764 Daher ist hier ein besonderes Augenmaß gefragt. Gerade bei internen Kosten kann man unter Umständen nur näherungsweise bestimmen, wie hoch ein Schaden durch einen Compliance-Verstoß sein mag. Dennoch ist es für die weiteren Prozessschritte des Compliance-Risikomanagements und damit letztlich für die Geschäftsleitung wichtig zu wissen, dass der potenziell zu erwartenden Schaden auch interne Kosten von oftmals nicht unerheblicher Höhe umfassen kann. Aus Gründen der Transparenz ist es insoweit richtig, diese Kosten ggf. nur zu schätzen und den angegebenen Wert als Schätzung zu kennzeichnen. Insgesamt sollte durch eine offene Kommunikation der Eindruck mathematischer Präzision vermieden werden, wo es an dieser aufgrund der wenig stabilen Daten mangeln muss. Scheingenauigkeit treiben nicht nur die Kosten des **Compliance-Risikobewertungsprozesses** in die Höhe. Sie können auch zu einer unrichtigen Darstellung der Compliance-Risikolandschaft führen und am Ende sogar dafür sorgen, dass das Ergebnis angreifbar und somit die Professionalität und damit wiederum die Glaubwürdigkeit der Compliance-Funktion in Frage gestellt wird.

765 Daher kann es sich auch anbieten, statt mit „präzisen" Zahlenwerten eher mit **Bandbreiten** zu arbeiten. Die Bandbreite kann in Geldwerten bemessen oder zB auch in Prozentwerten vom Operating Profit oder Umsatz angegeben werden. Die Höhe der einzel-

[471] S. Maßnahmen der Compliance-Risikosteuerung → Rn. 828 ff.