

Einleitung

Bernhard Kofler-Senoner

Zielsetzung dieses Buchs ist es, Unternehmen einen Compliance-Leitfaden aus Praktikersicht an die Hand zu geben, der die Entwicklungen der letzten Jahre in diesem Bereich berücksichtigt und es ermöglicht, ein maßgeschneidertes Compliance-Management-System („CMS“) der 2. Generation zu planen und umzusetzen.

Im Sinne eines ganzheitlichen Konzepts deckt dieses Buch neben den üblichen (und notwendigen) Themen der Planung und Implementierung eines CMS zwei Themenkomplexe ab, die zuletzt massiv an Bedeutung gewonnen haben, nämlich einerseits Krisenmanagement und andererseits Fragen zur internen und externen Kommunikation.

Gliederung und Konzept folgen dabei den Prinzipien der Praxisrelevanz und klaren Strukturierung, um dem Leser ein rasches Erfassen der wesentlichen Inhalte zu ermöglichen.

Vor diesem Hintergrund wurde gleich im *1. Kapitel* ein Beitrag des Compliance-Verantwortlichen der Telekom Austria AG aufgenommen, der eine **ganzheitliche Aufarbeitung des Themas „Konzeption und Umsetzung eines CMS in der Praxis“** bietet und eine in sich geschlossene Abhandlung in komprimierter Form darstellt.

Anschließend findet sich im *2. Kapitel* eine detaillierte Aufarbeitung der **Gründe für die Einführung eines CMS** aus (i) Sicht des Kommunikationsexperten, (ii) wirtschaftlicher und schließlich (iii) rechtlicher Sicht.

Kapitel 3 befasst sich mit dem Themenkomplex der **Konzeption, Umsetzung und Prüfung eines CMS**, erläutert dabei ua die **Eckpunkte der anwendbaren internationalen und nationalen Standards**, gibt Antworten auf die allgegenwärtigen **Fragen der rechtlichen Verantwortung eines Compliance Officers** und den **Vorgaben für ein Whistle Blowing System** und enthält nicht zuletzt Anregungen zur **Einbindung interner und externer Kommunikation** in ein Compliance-Projekt sowie ein zusätzliches Kapitel einer Compliance-Verantwortlichen zu den Herausforderungen bei der **Einführung eines Antikorruptions-Programms in der Praxis**.

Im 4. *Kapitel* erfolgt die Aufarbeitung der **materiellrechtlichen Kapitel**, angefangen von Kartell- und Strafrecht über Lobbying, Kapital-, Bank- und Finanzrecht bis hin zum Datenschutz- und Arbeitsrecht. Die einzelnen Rechtsgebiete wurden aus Gründen der Übersicht und besseren Lesbarkeit mit einem **Q&A-System** versehen.

Das 5. *Kapitel* bietet dem Leser abschließend einen Leitfaden für das **Krisenmanagement**, dh für den Fall, dass ein Compliance-Verstoß eintritt. Die Autoren decken dabei die wesentlichen Fragen der (i) **Kommunikation im Krisenfall**, (ii) Durchführung einer **Internal Investigation**, und (iii) anwendbaren **kartell- und strafrechtlichen Kronzeugenprogramme** ab.

1. Kapitel

Konzeption und Umsetzung eines Compliance-Management-Systems (CMS) – eine ganzheitliche Betrachtung aus der Sicht eines Compliance-Verantwortlichen

Martin Walter

I. Einleitung

Compliance hat in den letzten Jahren einen deutlichen Bedeutungszuwachs erfahren und ist zusammen mit Corporate Social Responsibility Bestandteil eines ganzheitlichen Integritätsmanagements. Compliance orientiert sich nicht allein daran, dass die Handlungen der Unternehmensmitarbeiter im Einklang mit den Gesetzen stehen, sondern ebenso im Einklang mit internen Richtlinien und ethischen Prinzipien. Zur bestmöglichen Sicherstellung von Compliance bedarf es eines auf die jeweilige Unternehmenssituation angepassten CMS. 1

II. Gründe für den Bedeutungszuwachs von Compliance in der Unternehmenspraxis

Stellt man die These auf, dass Compliance, also das regelkonforme Verhalten von Unternehmen und Personen in Unternehmen, in den letzten Jahren einen stetigen Bedeutungszuwachs erfahren hat, so wird wenig Widerspruch aufkommen. 2

Sinnfälligster Ausdruck hierfür ist die vielfältige und umfassende Berichterstattung zu compliance-relevanten Themen in der Tages- und Wirtschaftspresse. Ob es heutzutage mehr Fehlverhalten und damit einhergehend mehr Skandale gibt als früher oder ob nur genauer hingeschaut wird, sei dahingestellt. 3

Dies geht einher mit einer bis dato unbekanntenen Personalisierung des Fehlverhaltens. Nicht mehr allein das Unternehmen steht am Pranger, son- 4

dern vermehrt das Führungspersonal des Unternehmens. Dies ist einerseits vollkommen berechtigt, denn die widerrechtlichen und zu kritisierenden Handlungen werden ja von konkreten Personen beschlossen, in Auftrag gegeben und umgesetzt. Andererseits ist die mediale Aufmerksamkeit jedoch ungleich höher, wenn das Fehlverhalten nicht vom einfachen Mitarbeiter, sondern vom Vorstandsvorsitzenden begangen worden ist; dies umso mehr, wenn es sich bei ihm um eine auch in der breiteren Öffentlichkeit bekannte Person handelt. Der Presse kommt hier im Spannungsfeld von „Aufklärung und Auflage“ die hohe Verantwortung zu, nicht vorschnell zu personalisieren, denn mit einem Compliance-Makel behaftet zu sein bedeutet oft nicht nur das Ende der *aktuellen* Tätigkeit, sondern kann vielmehr das Ende der *Berufstätigkeit* bedeuten.

- 5 Dass sich in Anbetracht dieser die persönliche Betroffenheit drastisch erhöhenden Entwicklung Aufsichtsräte und Vorstände verstärkt mit Compliance befassen, ist mehr als verständlich. Und so ist es kein Zufall, dass in letzter Zeit die Compliance-Abteilung vermehrt einem Vorstands- bzw Geschäftsführungsmittglied direkt unterstellt wird oder in einigen Fällen in Deutschland sogar zu einem eigenständigen Vorstands- bzw Geschäftsführungsressort aufgewertet worden ist.
- 6 Ein zweiter Grund für den Bedeutungszuwachs sind formal-rechtliche Entwicklungen, in Deutschland namentlich das Bilanzrechtsmodernisierungsgesetz („BilMoG“). Es sieht eine Konkretisierung der Überwachungsaufgaben des Aufsichtsrats dahingehend vor, dass dieser sich von der *Wirksamkeit* des Internen Kontrollsystems und damit einhergehend von Teilaspekten eines umfassenden CMS zu überzeugen hat. Diese Aufgabe kann auf den Prüfungsausschuss delegiert werden. Auch der Deutsche Corporate Governance Kodex beinhaltet nunmehr Anforderungen an die Compliance.¹
- 7 In Österreich wurde mit dem Unternehmensrechtsänderungsgesetz 2008 („URÄG“) die Stellung des Prüfungsausschusses größer und börsennotierter Unternehmen gestärkt und die explizite Zuständigkeit für die Überprüfung

¹ Regelungen für den Vorstand: Ziff 4.1.3: Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin (Compliance). Ziff 3.4 Abs 2, S 1: Der Vorstand informiert den Aufsichtsrat regelmäßig, zeitnah und umfassend über alle für das Unternehmen relevanten Fragen der Planung, der Geschäftsentwicklung, der Risikolage, des Risikomanagements und der Compliance. Regelungen für den Aufsichtsrat bzw den Prüfungsausschuss: Ziff 5.3.2, S 1: Der Aufsichtsrat soll einen Prüfungsausschuss (Audit Committee) einrichten, der sich insbesondere mit Fragen der Rechnungslegung, des Risikomanagements und der Compliance, der erforderlichen Unabhängigkeit des Abschlussprüfers, der Erteilung des Prüfungsauftrags an den Abschlussprüfer, der Bestimmung von Prüfungsschwerpunkten und der Honorarvereinbarung befasst.

der *Wirksamkeit* des Internen Kontrollsystems, des Risikomanagementsystems und des Internen Revisionsystems gesetzlich festgeschrieben. Die Compliance-Regeln im Österreichischen Corporate Governance Kodex wurden sukzessive erweitert.

Die Leitungsverantwortung des Vorstandes zur Implementierung angemessener Compliance-Strukturen findet auch im österreichischen Verbandsverantwortlichkeitsgesetz seinen Niederschlag, wonach ein Unternehmen für Straftaten seiner Entscheidungsträger oder bei *Unterlassen wesentlicher organisatorischer, technischer oder personeller Maßnahmen zur Verhinderung von strafgesetzwidrigen Handlungen* durch Mitarbeiter zur Verantwortung gezogen werden kann. Ähnliche Bestimmungen enthält auch das deutsche Ordnungswidrigkeitengesetz (§§ 30 und 130 OWIG). 8

Drittens haben die finanziellen Konsequenzen nicht-regelkonformen Verhaltens mitunter eine Dimension erreicht, die eine verstärkte Befassung von Aufsichtsrat und Vorstand geboten erscheinen lässt. Dies betrifft sowohl mögliche Umsatzeinbußen, zB durch Reputationsverlust bei den Kunden oder gerichtlich angeordneten Marktaustritt, als auch Kosten für Ermittlungen, Verteidigung und Gutachten sowie aus Strafzahlungen bzw Bußgeldern. Gleichzeitig kann sich das Top-Management in einer möglichen Phase externer Ermittlungen zur Sachverhaltsaufklärung nicht mehr uneingeschränkt um die strategischen und operativen Aufgaben im Unternehmen kümmern. Diese Defokussierung wird zu weiteren Ergebniseinbußen führen. 9

Und viertens hat die Schuldenkrise Anlass gegeben zu einer verstärkten öffentlichen Diskussion über unternehmerisches Fehlverhalten. Vor dem Hintergrund der massiven Sozialisierung von Verlusten privater Unternehmen insbesondere im Bankensektor ist es zwingend, dass von den Managern eine Position eingefordert wird zu den Themen Fehlverhalten, unternehmerische Verantwortung und Moral bzw Ethik. 10

III. Zielsetzungen von Compliance aus Sicht der Unternehmenspraxis

Aus den genannten Gründen für den Bedeutungszuwachs lassen sich unmittelbar die Zielsetzungen der Unternehmen ableiten, die mit der Befassung mit dem Thema Compliance verfolgt werden. 11

Primäres Ziel aus Sicht des Aufsichtsrates und des Vorstands bzw der Geschäftsführung ist zweifelsfrei die Vermeidung von Karriereschäden und persönlicher Haftung, ein in Anbetracht der möglichen gravierenden Konsequenzen verständliches Anliegen. 12

Daneben ist es eine wesentliche Zielsetzung für das Unternehmen Haftungsschäden und insbesondere Reputationsverlust zu vermeiden. Beides 13

wirkt sich – unmittelbar oder mittelbar – auf das Unternehmensergebnis aus, sei es zB in Form von Bußgeldern, Umsatzverlust durch verunsicherte Kunden oder sinkende Attraktivität als Arbeitgeber.

- 14 Und drittens tritt neben die Vermeidung negativer persönlicher Konsequenzen und negativer Auswirkungen auf die GuV des Unternehmens verstärkt eine weitere Zielsetzung: regelkonformes Handeln als konstitutives Merkmal einer als „Integres Unternehmen“ wahrgenommenen Organisation. Mit anderen Worten: Compliance nicht als Mittel zur Erreichung persönlicher Zwecke oder finanzieller Unternehmensziele, sondern „weil es sich so gehört“. Wenn man in diesem Sinne das „Integre Unternehmen“ als oberstes Ziel akzeptiert, dann wird deutlich, dass aus dieser Perspektive Haftungsvermeidung und Reputationsverlust weniger eigenständige *Ziele* sind, als vielmehr das *Ergebnis* rechtschaffenen Verhaltens.²

IV. Was soll unter Compliance verstanden werden?

- 15 Oberstes Ziel des klassischen Managementprozess ist es, durch einen integrierten Einsatz aller Managementinstrumente und durch konsequente Umsetzung im Realgüterprozess kurz-, mittel- und langfristig die finanziellen und operativen Ziele zu erreichen. Im Fokus stehen somit „*The right results*“.
- 16 Das Compliance-Management befasst sich demgegenüber mit der Frage, wie sichergestellt werden kann, dass diese Ziele ausschließlich mit den richtigen Mitteln erreicht werden. Neben die richtigen Ergebnisse tritt der richtige Weg: „*The right way*“.
- 17 Compliance kann nicht eigenständig und isoliert betrachtet werden, sondern ist – zusammen mit Corporate Social Responsibility Bestandteil eines ganzheitlichen Integritätsmanagements zur Umsetzung einer ethisch fundierten (und damit zugleich ökonomisch und gesellschaftlich nachhaltigen) Unternehmensführung.
- 18 Compliance selbst ist zweckmäßigerweise zu differenzieren in „Business Process Compliance“ und „Business Conduct Compliance“.³ Dabei bezieht sich Business Process Compliance auf die Integrität organisatorischer Prozesse und Business Conduct Compliance auf die Integrität des Verhaltens der Mitarbeiter eines Unternehmens. Unter Business Process Compliance sind etwa zu subsumieren Maßnahmen in den Bereichen Anti-Money-Laudring,

2 Grüninger in Wieland/Steinmeyer/Grüninger (Hrsg), Handbuch Compliance-Management² (2014) 41 (51).

3 Wieland in Wieland/Steinmeyer/Grüninger (Hrsg), Handbuch Compliance-Management² (2014) 15 (30 ff).

„Know Your Customer“, Embargo, Vendor Integrity Management⁴ oder IT-Compliance/Datensicherheit. Diese Bereiche weisen entweder rechtlich sehr standardisierte Grundlagen auf oder sind stark IT-unterstützt und sind in der betrieblichen Praxis aufgrund des damit einhergehenden hohen Maßes an Spezialisierung oftmals eigenständig organisiert. Wichtig ist jedoch, sie hinsichtlich ihrer verhaltensrelevanten Konsequenzen in die Business Conduct Compliance zu integrieren.

Business Process Compliance weist auch einen engen Bezug auf zum Internen Kontroll-System („IKS“). Aus Compliancesicht muss das IKS so gestaltet sein, dass ein zentraler Fokus der Kontrollaktivitäten auf der Detektion von allfälligen Zahlungen liegt, die für unlautere Zwecke erfolgt sind. 19

Im Mittelpunkt der nachfolgenden Ausführungen steht die Business Conduct Compliance. Bei dieser ist es zunächst sinnvoll, eine begriffliche Differenzierung einzuführen, nämlich „*Compliance im engeren Sinne*“ von „*Compliance im weiteren Sinne*“ zu unterscheiden.⁵ In der Compliance-Praxis wird dieser Unterschied bereits sichtbar. Er wird durch die zugrunde liegenden Annahmen zur Motivation der Mitarbeiter und zur Komplexität des Regelungsbedarfs markiert. 20

Compliance ieS zeichnet sich dadurch aus, dass durch die Vorgabe rechtlicher und organisationsinterner Verhaltensnormen Fehlverhalten verhindert oder aufgedeckt werden soll. Das soll durch Anreize (Belohnungen und insbesondere Bestrafungen) erreicht werden; man unterstellt also im Prinzip einen Wirkungszusammenhang, der menschliches Handeln als überwiegend durch *extrinsische Motivation* veranlasst sieht. Auch wird unterstellt, dass in jeder Entscheidungssituation eine eindeutige Verhaltensnorm existiert und dass diese den Mitarbeitern bekannt ist, was nur in einer nicht-komplexen und statischen Umwelt der Fall sein kann. 21

Compliance iwS gibt diese Voraussetzungen auf. Unternehmensführung hat es bei der Steuerung mit einem komplexen und offenen System zu tun; es ist klug damit zu rechnen, dass Verhaltensnormen nicht vollständig sind, nicht hinreichend genau spezifiziert bzw nicht umfassend kommuniziert oder verstanden worden sind. Das bedeutet aber, dass es *den Mitarbeitern selbst* 22

4 Walter/Kaven-Moser in Wieland/Steinmeyer/Grüniger, Handbuch Compliance-Management² (2014) 799.

5 Vgl hierzu den klassischen Aufsatz von Paine, Managing for Organizational Integrity, Harvard Business Review 1994, 106.

In dem hier zitierten Aufsatz stellt die Verfasserin einen im obigen Sinne engen Compliance-Ansatz einem ganzheitlichen Integritätsansatz gegenüber. Da sich in der Unternehmenspraxis durchgängig die Abteilung „Compliance“ und nicht die Abteilung „Integrität“ herausgebildet hat, soll hier weiterhin vom – im obigen Sinne weiten – Compliance-Management gesprochen werden. Inhaltlich entspricht dies dem Integritätsansatz von Paine.

ermöglicht werden muss, in solchen kritischen, nicht vorhersehbaren Situationen eigenständig und intrinsisch motiviert Verantwortung für das richtige normengetreue Verhalten zu übernehmen. Neben Recht und Richtlinien (wie bei der Compliance ieS) tritt bei der ComplianceiwS somit die Ethik als übergeordnetes handlungsleitendes Prinzip, da wie gesagt (glücklicherweise) nicht jede Entscheidungssituation durch Gesetz oder Richtlinie vollständig determiniert sein kann. In der Praxis bedeutet dies den Rückgriff auf ein allgemeines moralisches Grundverständnis bzw den kategorischen Imperativ von Kant: „Handle so, dass die Maxime deines Willens jederzeit zugleich als Prinzip einer allgemeinen Gesetzgebung gelten könnte.“ Ethik hat so gesehen eine Ergänzungsfunktion zum Recht.⁶

23 Es ist offensichtlich, dass in der Unternehmenspraxis eine Compliance ieS zu kurz greift und daher das *weitere* Verständnis von Compliance zugrunde gelegt werden muss.

24 Daneben bedarf es zweckmäßigerweise einer weiteren definitorischen Festlegung. Nicht jede Handlung, durch die Recht, Richtlinien oder ethische Grundsätze verletzt werden, soll als compliance-relevant betrachtet werden. Schon allein, um im Tagesgeschäft eine völlige Arbeitsüberlastung der Compliance-Abteilung zu verhindern, soll dies nur der Fall sein, wenn eine *vorsätzliche* Schädigung des Unternehmens oder Dritter intendiert ist oder billigend in Kauf genommen wird. Handlungsbedarf für die Compliance-Abteilung bei nicht-vorsätzlichen Regelverletzungen ergibt sich gegebenenfalls in Form eines Schulungsbedarfs für die jeweiligen Mitarbeiter.

25 Auch wird deutlich, dass Compliance kein Zustand ist, der sich von selbst einstellt. Er muss vielmehr durch den zielgerichteten und konsistenten Einsatz von Instrumenten aus dem Bereich der Führungsfunktionen Planung, Kontrolle, Organisation, Leitung und Personal herbeigeführt werden. Mit anderen Worten: es bedarf eines verantwortlich durch den Compliancebereich eingeführt und umgesetzten CMS. Dabei ist klar, dass das Management in der Verantwortung für regelkonformes Verhalten ist und bleibt. Genauso wenig, wie sich die Ergebnisverantwortung in den Controlling-Bereich delegieren lässt, genauso wenig ist die Compliance-Abteilung in der Letztverantwortung für Regeltreue im Unternehmen.

6 Generell wird der Unternehmensethik eine dreifache Brückenfunktion zum Recht zugewiesen. Neben der Ergänzungsfunktion steht zweitens die (moralische) Pflicht der Unternehmensführung, geltendes Recht anzuwenden (Legalitätsprinzip) und drittens als Kritikfunktion die Pflicht, wo erforderlich an einer Fortentwicklung von (rechtlichen) Normen mitzuarbeiten, um die Anwendung von Unrecht zu verhindern und/oder unfaire Spielregeln zu verbessern. Vgl hierzu *Steinmann*, Unternehmensethik und Recht – Einige Überlegungen zur Meta-Regulierung gesellschaftlicher Verantwortung der Unternehmensführung, in *Zeitschrift für Internationale Strafrechtsdogmatik* 2011, 6 (100–109).