276

Unternehmensmitbestimmung
und Unternehmenssteuerung

Lasse Pütz | Manuela Maschke (Hrsg.)

Compliance – ein Thema für Betriebs- und Aufsichtsräte

edition
Hans Böckler
Stiftung

Lasse Pütz | Manuela Maschke (Hrsg.)

Compliance – ein Thema für Betriebs- und Aufsichtsräte

edition 276

Lasse Pütz | Manuela Maschke (Hrsg.)

Compliance – ein Thema für Betriebs- und Aufsichtsräte

Oliver Emons leitet das Wirtschaftsreferat IV der Hans-Böckler-Stiftung.

Alexandra Krieger leitet das Wirtschaftsreferat I der Hans-Böckler-Stiftung.

Dr. Manuela Maschke leitet das Archiv Betriebliche Vereinbarungen der Hans-Böckler-Stiftung; www.boeckler.de/betriebsvereinbarungen.

Dr. Andreas Priebe leitet das Referat Arbeitsrecht der Hans-Böckler-Stiftung.

Lasse Pütz leitet das Referat Wirtschaftsrecht III der Hans-Böckler-Stiftung.

Dr. Sebastian Sick leitet das Referat Wirtschaftsrecht II der Hans-Böckler-Stiftung.

Maximilian Waclawczyk war im Jahr 2011 Praktikant bei der Hans-Böckler-Stiftung.

Das Whistleblower-Netzwerk e.V. fördert Whistleblowing und offenen Dialog. Es wurde 2006 gegründet und hat derzeit ca. 75 Mitglieder.

© Copyright 2012 by Hans-Böckler-Stiftung
Hans-Böckler-Straße 39, 40476 Düsseldorf
Produktion: Setzkasten GmbH, Düsseldorf
Printed in Germany 2012
ISBN: 978-3-86593-174-0
Bestellnummer: 13276

Alle Rechte vorbehalten. Dieses Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechts ist ohne schriftliche Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Mikroverfilmungen, Übersetzungen und die Einspeicherung in elektronische Systeme.

Inhaltsverzeichnis

Vorwort

Compliance als Bestandteil einer funktionierenden Corporate Governance

Eine funktionierende Corporate Governance gewinnt sowohl in der Weltwirtschaft als auch für die Führung jedes einzelnen Unternehmens immer mehr an Bedeutung.

Unter den Vorzeichen der Globalisierung bieten sich nicht nur Chancen für geschäftlichen Erfolg auf neuen Märkten, auch der Konkurrenzdruck wird größer, und es nehmen die rechtlichen Risiken für die Unternehmen zu.

Dazu kommt, dass sich das öffentliche Bewusstsein für die Notwendigkeit fairen Wettbewerbs geschärft hat und die Einhaltung von Gesetzten sowie die Berücksichtigung von Gemeinwohlinteressen immer mehr zum Maßstab für das Ansehen eines Unternehmens genommen wird.

Unternehmen tun deshalb gut daran, sich um Compliance, also die Einhaltung von gesetzlichen und unternehmensinternen Regeln, zu kümmern und entsprechende Verantwortlichkeiten wie Instrumentarien zu schaffen.

Doch dies allein reicht nicht mehr aus. Vielmehr muss die Unternehmensleitung eine Kultur der Integrität fördern, die sich durch Transparenz, Fairness, Respekt sowie die Übernahme und Delegation von Verantwortung auszeichnet.

Dieses Buch bietet wertvolle und vor allem praxisnahe Hinweise darauf, wie ein Compliance-System langfristig zu einer funktionierenden Corporate Governance beitragen kann: Neue Anforderungen müssen in bestehende Prozesse integriert, Bewährtes mit Neuem verknüpft werden; vor allem aber kommt es jedoch darauf an, von einem „one-size-fits-all approach" Abstand zu nehmen und stattdessen die individuelle Risikosituation der Branche und des Unternehmens zu berücksichtigen – so kann eine erfolgreiche Umsetzung gelingen.

Dr. Christine Hohmann-Dennhardt
(Vorstandsmitglied der Daimler AG, verantwortlich für Integrität und Recht)

Abkürzungen

AGG	Allgemeines Gleichbehandlungsgesetz
AN	Arbeitnehmer
AktG	Aktiengesetz
AR	Aufsichtsrat
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAG	Bundesarbeitsgericht
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BilMoG	Bilanzrechtsmodernisierungsgesetz
BPI	Bribe Payers Index
BR	Betriebsrat
BT-Drucks.	Bundestag-Drucksache
CMS	Compliance-Management-System
COSO	Committee of Sponsoring Organisations of the Treadway Commission
CPI	Corruption Perceptions Index
CSR	Corporate Social Responsibility
DCGK	Deutscher Corporate Governance Kodex
DGB	Deutscher Gewerkschaftsbund
DrittelbG	Drittelbeteiligungsgesetz
EGMR	Europäischer Gerichtshof für Menschenrechte
EMRK	Europäischen Menschenrechtskonvention
FCPA	Foreign Corrupt Practices Act
GewO	Gewerbeordnung
GG	Grundgesetz
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
IDW	Institut der Wirtschaftsprüfer
InvG	Investmentgesetz
InvMaRisk	Mindestanforderungen an das Risikomanagement für Investmentgesellschaften
InstitutsVergV	Instituts-Vergütungsverordnung

KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KSchG	Kündigungsschutzgesetz
KWG	Kreditwesengesetz
LAG	Landesarbeitsgericht
MaRisk (BA)	Mindestanforderungen an das Risikomanagement von Banken
MaComp	Mindestanforderungen an Compliance und die weiteren Verhalten, Organisations- und Transparenzpflichten nach §§ 31 ff. WpHG
MaRisk (VA)	Mindestanforderungen an das Risikomanagement von Versicherungen
MitbestG	Mitbestimmungsgesetz
NGO	Non-Governmental Organization
OLG	Oberlandesgericht
OWiG	Ordnungswidrigkeitengesetz
PR	Personalrat
SE	Societas Europaea (Europäische Aktiengesellschaft)
TKG	Telekommunikationsgesetz
VAG	Versicherungsaufsichtsgesetz
WpHG	Wertpapierhandelsgesetz

Wozu Compliance?

von Lasse Pütz und Manuela Maschke

„Wie ihr es immer dreht und wie ihr‘s immer schiebt,
erst kommt das Fressen, dann kommt die Moral.“
(Berthold Brecht 1928, Dreigroschenoper)

Gewinne erwirtschaften und dabei moralisch handeln, ist eine Herausforderung für Unternehmen. Laut einer Studie zu Wirtschaftskriminalität gaben etwa 52 % der befragten Unternehmen in Deutschland an, 2011 von mindestens einem Schadensfall aufgrund von Wirtschaftskriminalität betroffen gewesen zu sein (PricewaterhouseCoopers 2011, S. 17). Die Schäden, die dadurch in Deutschland pro Jahr verursacht werden, beziffern die Autoren auf durchschnittlich 8,39 Millionen Euro pro Unternehmen. Schwerer als die finanziellen Verluste wiegen zumindest für Großunternehmen die indirekten durch Wirtschaftskriminalität verursachten Auswirkungen wie z. B. Reputationsverluste. Ein beeinträchtigtes Verhältnis zu Geschäftspartnern und Behörden lässt sich kaum exakt messen, ist aber ein Risiko für Unternehmen. Die Bewältigung der Folgen von Wirtschaftsdelikten und anderen Gesetzesverstößen kostet viel Zeit und oftmals auch Geld.

Um solche Schäden zumindest zu begrenzen, werden von Rechtsanwälten und Unternehmensberatern bevorzugt Compliance und sogenannte Compliance-Management-Systeme (CMS) favorisiert. Auch Arbeitnehmervertreter im Betriebs- oder Aufsichtsrat werden insofern öfter mit Compliance und CMS konfrontiert. Auch der Deutsche Corporate Governance Kodex erklärt seit Juni 2007 Compliance zu einem Bestandteil guter Unternehmensführung. Trotz umfangreicher Diskussionen in Praxis und Fachliteratur besteht weiterhin die Frage: Was ist das und brauchen wir Compliance überhaupt?

Für Beschäftigte und ihre Interessenvertretungen ist nicht immer klar, welche Maßnahmen das Unternehmen mit der Begründung, dies sei wegen Compliance notwendig, durchführt und warum. Nicht alle Unternehmen bemühen sich, ihre Belegschaft bei der Einführung eines CMS entsprechend einzubinden. Arbeitnehmervertreter und -vertreterinnen in Aufsichtsräten müssen die Einhaltung der Geschäftsordnung überwachen. Ihnen stellt sich auch die Frage, welche Rolle sie im CMS einnehmen. Die nachfolgenden Ausführungen beantworten einige Fragen, die sich aus Arbeitnehmersicht beim Thema Compliance stellen.

Compliance wird in dieser Handlungshilfe verstanden als Gesamtheit aller Maßnahmen, um die Einhaltung von Recht, Gesetz und Richtlinien des Unternehmens, seiner Organmitglieder und Beschäftigten zu gewährleisten. Ein Compliance-Management-System ist entsprechend die Methode oder Herangehensweise, die das rechtmäßige und richtlinienkonforme Verhalten aller Beteiligten eines Unternehmens sicherstellen soll. Enger gefasste Definitionen stellen vor allem darauf ab, dass Gesetze eingehalten sowie Korruption und kriminelles Verhalten verhindert werden.

Unternehmen setzen unterschiedliche Prioritäten, je nach Branche, Unternehmensgröße und Struktur. Auch gesetzliche Vorschriften sind je nach Branche verschieden relevant (vgl. Kap. I). Beispielsweise gelten für das Versicherungs- und Kreditgewerbe besondere gesetzliche Vorgaben; für Unternehmen der Mineralölverarbeitung haben Umweltschutzgesetze eine größere Relevanz. Zusätzlich existieren börsenrechtliche Vorschriften und weitere Regelungen, z. B. der Deutsche Corporate Governance Kodex.

Wird Compliance weiter gefasst und werden unternehmensinterne Regelwerke entwickelt, dann verpflichten sich Unternehmen freiwillig, weitere Regeln und Vereinbarungen einzuhalten. Dabei können solche inhaltlich oft ähnlichen Regelwerke ganz unterschiedliche Bezeichnungen tragen: Code of Conduct, Verhaltenskodex, Grundsätze integren Verhaltens, Ethik-Charta, Corporate Compliance Policy oder Corporate Social Responsibility Principles etc. Compliance kann daher auch heißen, gesellschaftliche Verantwortung wahrzunehmen sowie die Menschenrechte und ILO-Kernarbeitsnormen im Unternehmen und entlang der Wertschöpfungskette zu beachten, wenn man eine entsprechende Richtlinie hat.

Die Bandbreite dessen, was geregelt wird, ist groß: Verhalten und Respekt im Umgang miteinander, Gesetzestreue und redliche Führung der Geschäfte, Vertraulichkeit, Umgang mit Interessenskonflikten, Trennung von Privat- und Konzerninteressen, Korruption und Bestechlichkeit, Prävention von Geldwäsche, gesetzeswidrige Aktivitäten, Wettbewerbs- und Kartellrecht, Schutz natürlicher Ressourcen und des Vermögens, Annahme und Gewährung von Geschenken und Vergünstigungen, Periodenabschlüsse und Finanzkommunikation, Insiderregeln, Datenschutz und IT-Sicherheit.

In welchem Umfang Schäden aus Regelverstößen eintreten, verdeutlicht auch ob wirksame Strukturen vorhanden sind, die helfen, Missstände frühzeitig zu erkennen und Verstößen zu begegnen. Dazu gehört vor allem die Einrichtung von Möglichkeiten, Hinweise und Meldungen abzugeben. Das können so genannte Whistleblowing-Kanäle sein. Im besten Fall ermutigt ein solches System einerseits

den oder die Hinweisgeber zur Zivilcourage, schützt Meldende vor arbeitsrechtlichen sowie persönlichen Nachteilen und verhindert zugleich Denunzierungen und falsche Verdächtigungen – eine anspruchsvolle Aufgabe (vgl. Kap. IV).

Da jede Regel einen möglichen Regelverstoß mit sich bringt und jeder mögliche Regelverstoß ein Risiko für das Unternehmen bedeutet, ist Compliance eng mit dem Risiko-Management verbunden (vgl. Kap. VI). Im Zusammenhang mit Compliance dient ein Risiko-Management-System dazu, Schäden aus Pflichtverletzungen vorzubeugen. Hierzu muss das Unternehmen seine Risiken erkennen, bewerten und die Wirksamkeit seines Risiko-Managements laufend kontrollieren. Anschließend ist der mögliche Schaden zu bewerten. Dieser gesamte Prozess muss gesteuert werden, was auch die Risikoberichterstattung nach innen und außen umfasst.

Dass ein Compliance-System eingerichtet ist und funktioniert, liegt in der Verantwortung der Unternehmensleitung. In Unternehmen mit Aufsichtsrat kontrolliert dieser sowie ein Prüfungsausschuss (falls eingerichtet) die Geschäftsführung. Er muss überwachen, ob die Unternehmensleitung die Aufgaben ordnungsgemäß wahrnimmt und auf Maßnahmen hinwirken, falls Schwächen in der Funktionsfähigkeit des Compliance-Systems festgestellt werden. Die Berichterstattung an den Aufsichtsrat ist daher wichtig.

Unterstützt wird der Aufsichtsrat vom Abschlussprüfer, der in börsennotierten Aktiengesellschaften das Risiko-Management prüft und diesbezüglich auch Aussagen über das Compliance-System in seinem Prüfungsbericht treffen muss. Ein weiterer Berührungspunkt ergibt sich aus der Prüfung und Feststellung des Jahresabschlusses. Im Unterschied zur internen Berichterstattung an den Aufsichtsrat, ist die externe Berichterstattung jedoch eher von begrenzter Aussagekraft, weil einheitliche Vorgaben für den Bericht fehlen: Unternehmen müssen nur über solche Risiken berichten, die sich wesentlich auf die wirtschaftliche Lage auswirken können.

Inzwischen können Unternehmen ihr Compliance-System nach einem Standard extern prüfen und zertifizieren lassen, um den Erfolg Compliance-relevanter Maßnahmen nachzuweisen (vgl. Kap. VII). Kosten und Nutzen abzuwägen, ist sinnvoll, denn weder die grundsätzliche Haftung noch die Kontrollfunktion der Geschäftsführung und des Aufsichtsrats werden davon berührt. Die externe Zertifizierung ändert nichts an den Pflichten der Geschäftsleitung und des Aufsichtsrats. Sie unterstützt die Verantwortlichen lediglich dabei, ihre Aufgaben wahrzunehmen.

Bekennen sich Vorstand und Arbeitnehmervertreter gemeinsam in einer verbindlichen Vereinbarung zu Compliance, wirkt dies nach innen und außen anders als einseitig erlassene Richtlinien. Insofern spielt es eine wichtige Rolle, wer beteiligt ist, wenn ein Compliance-System aufgebaut wird, und wer für welche Aufgaben Verantwortung übernimmt: Wird ausschließlich die juristische Stabstelle im Unternehmen genannt? Oder ist z. B. auch die Personalabteilung eingebunden? Werden Weiterbildungsmaßnahmen entwickelt? Ist Compliance Bestandteil von Zielvereinbarungen und Mitarbeitergesprächen?

Es geht insofern um das Bekenntnis der Unternehmensleitung an die Beschäftigten, Regeln einzuhalten, und um die Beteiligung von Beschäftigten und Interessenvertretungen am Compliance-Management-Prozess. Die Beschäftigung mit der Einhaltung und Überwachung von Gesetzen und Regeln im Unternehmen ist nicht neu für Betriebsräte. Das Direktionsrecht des Arbeitgebers, der individuelle Arbeitsvertrag und die kollektive Betriebsordnung regeln das Verhalten aller Beschäftigten im Betrieb. Im besten Fall existiert bereits ein verbindlicher Standard, um einen reibungslosen Arbeitsablauf zu gewährleisten. Regeln zum Umgang miteinander, partnerschaftliches Verhalten, ein Konflikt- und Beschwerdemanagement gehören dazu. Wird z. B. gegen die Betriebsordnung verstoßen, kann das arbeitsrechtliche Konsequenzen (Abmahnung, Kündigung) nach sich ziehen. Der Betriebsrat hat in einigen Bereichen gute Mitbestimmungsmöglichkeiten (vgl. Kap. III). Beschäftigte haben auch Beschwerderechte, die sie mit Unterstützung des Betriebsrates durchsetzen können. Nicht zuletzt hängt die wirksame Einführung und Umsetzung von Maßnahmen vom guten Willen der Akteure, von transparentem und glaubwürdigem Handeln ab.

Ob Wert darauf gelegt wird, dass Gesetze und Richtlinien im Unternehmen eingehalten werden, wie wirkungsvoll Regelverstöße bekämpft, ob Meldende geschützt und Beschuldigte fair behandelt werden, sind Fragen der Betriebskultur: Auf die Einhaltung welcher Richtlinien wird besonderer Wert gelegt? Welche Prioritäten werden gesetzt? Welche Verhaltensweisen sind erwünscht? Welche werden nicht geduldet? Wird aktiv an einer Betriebskultur gearbeitet, die z. B. auch Vielfalt und Chancengleichheit der Beschäftigten fördert? Werden Mitbestimmungsrechte geachtet und wertgeschätzt?

Transparenz sowie die Einbindung der Beschäftigten und ihrer Interessenvertretungen sollten das Leitmotiv darstellen für die Entwicklung, Anwendung bis hin zur Überprüfung und Anpassung von Compliance-Richtlinien und Hinweisgeber-Systemen. Beteiligung von Beschäftigten, Mitwirkung und Mitbestimmung

durch Interessenvertretungen sind insofern kein Luxus, sondern Bedingung für das Gelingen von Vorhaben.

Die nachfolgenden Ausführungen geben einen Überblick über wesentliche Aspekte, die Betriebs- und Aufsichtsräte im Zusammenhang mit dem Thema Compliance kennen und beachten sollten. Zunächst werden in Kap. I juristische Grundlagen erörtert sowie die Aufgaben des Aufsichtsrates in Kap. II. Daran schließen sich arbeitsrechtliche Betrachtungen und die Rolle des Betriebsrats in Kap. III an. In Kap. IV werden Regelungen aus der betrieblichen Praxis zur Umsetzung von Whistleblowing-Systemen erläutert. Kap. V gibt einen Überblick über Compliance-Systeme in DAX-Unternehmen. Kap. VI befasst sich mit dem Zusammenspiel von Compliance- und Risiko-Management-Systemen. Dem folgen in Kap. VII Ausführungen zur externen Zertifizierung und Prüfung von Compliance-Systemen.

I Compliance-Management-Systeme – die Praxis von Unternehmen

von Lasse Pütz

1 Einleitung

Zunehmende Haftungsrisiken, (indirekte) Schadenersatzforderungen und Imageschäden haben Konsequenzen für Unternehmen und deren Management: Für sie gewinnt es an Bedeutung, sich im Einklang mit gesetzlichen Vorschriften zu verhalten. Auch ist es in der Praxis – aufgrund der Vielzahl von Regelungen, die Unternehmen im deutschen, europäischen und internationalen Umfeld einhalten müssen – oftmals eine Herausforderung, alle gesetzlichen und regulatorischen Verpflichtungen einzuhalten. Wirtschaftsunternehmen befassen sich daher immer stärker mit der Frage, wie sie Rechtsverstöße ihres Managements, ihrer Beschäftigten aber auch ihrer Zulieferer vermeiden können.

Von Rechtsanwälten und (Unternehmens-)Beratern werden so genannte Compliance-Management-Systeme (CMS) mitunter als „Allzweckwaffe" angepriesen. Die Einrichtung eines ganzheitlichen CMS und dessen organisatorische Eingliederung in das Unternehmen bestimmen die aktuelle Diskussion, sowohl in der Praxis als auch in der Fachliteratur.[1] Dementsprechend haben sich alle DAX 30-Unternehmen dieses Themas mehr oder weniger angenommen (vgl. Kap.V). Auch bei kleineren Unternehmen steht die Implementierung eines Compliance-Management-Systems immer öfter auf der Tagesordnung.[2]

Diese Entwicklung wird zusätzlich auch dadurch befördert, dass der Deutsche Corporate Governance Kodex seit Juni 2007 den Begriff Compliance gleich an unterschiedlichen Stellen aufgreift und Compliance zu einem Bestandteil „guter Unternehmensführung" erklärt. Nicht zuletzt deshalb stellt die Beschäftigung mit dem Thema Compliance in vielen Unternehmen inzwischen einen Baustein ihrer Corporate Governance dar.

1 Vgl. Pütz 2011.
2 Wermelt/Görtz 2011, S. 22 ff.

Vorschriften des Deutschen Corporate Governance Kodex (Stand: 15.05.2012)
Ziff. 3.4 Abs. 2, S. 1: Der Vorstand informiert den Aufsichtsrat regelmäßig, zeitnah und umfassend über alle für das Unternehmen relevanten Fragen der Strategie, der Planung, der Geschäftsentwicklung, der Risikolage, des Risikomanagements und der Compliance.
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. 5.2 Abs. 3, S. 1: Der Aufsichtsratsvorsitzende soll zwischen den Sitzungen mit dem Vorstand, insbesondere mit dem Vorsitzenden bzw. Sprecher des Vorstands, regelmäßig Kontakt halten und mit ihm Fragen der Strategie, der Planung, der Geschäftsentwicklung, der Risikolage, des Risikomanagements und der Compliance des Unternehmens beraten.
Ziff. 5.3.2, S. 1: Der Aufsichtsrat soll einen Prüfungsausschuss (Audit Committee) einrichten, der sich insbesondere mit der Überwachung des Rechnungslegungsprozesses, der Wirksamkeit des internen Kontrollsystems und des internen Revisionssystems, der Abschlussprüfung, hier insbesondere der Unabhängigkeit des Abschlussprüfers, der vom Abschlussprüfer zusätzlich erbrachten Leistungen, der Erteilung des Prüfungsauftrags an den Abschlussprüfer, der Bestimmung von Prüfungsschwerpunkten und der Honorarvereinbarung sowie – falls kein anderer Ausschuss damit betraut ist – der Compliance, befasst.

Für Beschäftigte und Betriebsrat spielt dagegen das CMS als Ganzes meist eine untergeordnete Rolle. Jedoch werden die Rechte des Betriebsrats oft durch Maßnahmen tangiert, die zu einem CMS gehören (vgl. Kap. III). Der Aufsichtsrat wiederum muss das System als Ganzes überwachen (Systemkontrolle), so dass die einzelnen Maßnahmen für diesen nur bedingt von Interesse sind.[3] Alle Beteiligten sollten indes wissen, was hinter den Begriffen Compliance und CMS steht. Nur so kann ein System kontrolliert werden bzw. können die einzelnen Maßnahmen eines CMS in seinem entsprechenden Kontext bewertet werden (z. B. bei Abschluss einer Betriebsvereinbarung). Der Aufsichtsrat sollte sicherstellen, dass er in das CMS integriert wird, z. B. indem ihm regelmäßig über die Arbeit der „Compliance-Abteilung“ berichtet wird.

3 Vgl. Kap. II und Pütz 2011, S. 13 ff.

2 Definition von Compliance und Compliance-Management-System

Eine gesetzliche Definition für den angelsächsischen Begriff Compliance existiert nicht. Einen ersten Anhaltspunkt gibt jedoch die direkte Übersetzung des englischen Begriffs. Nach dieser bedeutet Compliance so viel wie „Einhaltung, Befolgung, Übereinstimmung". Zudem empfiehlt es sich, auf die bereits zitierte Ziffer 4.1.3 des Deutschen Corporate Governance Kodex zurückzugreifen. Beachtet man, dass Compliance nicht nur eine Aufgabe des Vorstandes ist, sondern auch des Aufsichtsrates und des gesamten Unternehmens,[4] so lautet eine allgemeine Begriffserklärung wie folgt: „Compliance umfasst die Gesamtheit aller Maßnahmen, um das rechtmäßige Verhalten der Unternehmen, der Organmitglieder und der Mitarbeiter im Blick auf alle gesetzlichen Gebote und Verbote zu gewährleisten." [5]

In der Praxis werden neben der Befolgung von gesetzlichen Geboten und Verboten regelmäßig unternehmensinterne Richtlinien in ein Compliance-Programm einbezogen, z. B. Ethik-Richtlinien (Codes of Conduct), freiwillige Selbstverpflichtungen im Rahmen einer CSR-Strategie oder Unternehmensleitlinien. Das mittlerweile vorherrschende Verständnis von Compliance in der Praxis ist folglich nicht nur die Verhinderung von Vermögensdelikten und Korruption, sondern vielmehr auch die Einhaltung aller Gesetze, Verordnungen und Richtlinien[6] sowie von vertraglichen Verpflichtungen und freiwillig eingegangenen Selbstverpflichtungen. Compliance ist folglich eine umfassende und interdisziplinäre Aufgabe, die in allen Gesellschaften und Bereichen eines Konzerns für alle Rechtsgebiete und Rechtsordnungen sowie auf allen Hierarchiestufen Anwendung finden soll.

Als CMS wird die Methode oder Herangehensweise bezeichnet, die das rechtmäßige und richtlinienkonforme Verhalten aller Beteiligten eines Unternehmens sicherstellen soll. Ziel eines solchen Systems ist es, dass alle Organmitglieder, Führungskräfte und Beschäftigte rechtskonform und entsprechend den Unternehmenswerten handeln und so Rechtsverstöße und ihre negativen Folgen für das Unternehmen vermieden oder zumindest reduziert werden. Wie die nachfolgenden Ausführungen zeigen werden, muss dabei jedes CMS auf die Besonderheiten und Bedürfnisse jedes einzelnen Unternehmens individuell angepasst werden. Ein CMS „von der Stange" kann es nicht geben. Demnach lässt sich der Begriff CMS nicht weitergehend definieren. Es ist vielmehr nur möglich, die sich in der

4 Vgl. Pütz 2011, S. 13 ff.
5 Schneider 2003, S. 645.
6 Vgl. Pütz 2011, S. 19.

Praxis herausgebildeten und in einer Vielzahl von Systemen enthaltenen Elemente, darzustellen (siehe Kap. 4.3).

3 Compliance als Aufgabe der Geschäftsleitung

Als Leitungsorgan der Gesellschaft trifft den Vorstand bzw. die Geschäftsführung eine Organisations- und Aufsichtspflicht. Die Unternehmensleitung ist verpflichtet, das Unternehmen so zu organisieren, dass gesetzliche und unternehmensinterne Vorschriften durch das Unternehmen und seine Beschäftigten eingehalten werden (Compliance).[7] Diese Verpflichtung, Gesetze zu befolgen, wird auch als „Legalitätspflicht" bezeichnet. Sie wurde z. B. vom OLG Düsseldorf[8] in seiner „IKB-Entscheidung" explizit hervorgehoben:

„Dem Vorstand eines Unternehmens steht bei der Begehung von Gesetzes- und Satzungsverstößen kein Ermessensspielraum zu. Zwingende Gesetzes- und Satzungsvorschriften haben die Funktion, Handlungsgrenzen zu setzen, die nicht nach Opportunitätsaspekten vom Normunterworfenen relativiert oder modifiziert werden dürfen. Der Schutz der Business Judgment Rule (§ 93 Abs. 1 Satz 2 AktG) besteht nicht bei Gesetzes- und Satzungsverstößen […]. Einen Beurteilungsspielraum haben Vorstandsmitglieder nur bei der Frage, wie sie innerhalb des gesetzlichen bzw. satzungsmäßigen Handlungsspielraums agieren, um das Unternehmen so erfolgreich wie möglich zu führen […]."

Die Organisations- und Aufsichtspflicht der Geschäftsleitung erstreckt sich dabei nicht nur auf die eigene Gesellschaft, sondern auch auf die nachgeordneten Konzernunternehmen (Tochter- und Enkelunternehmen). Auch bei diesen hat der Vorstand (bei der GmbH die Geschäftsführung) auf die Einhaltung der Vorschriften hinzuwirken. Vorrangig liegt die Verantwortung für die Durchführung von Compliance im Unternehmen und Konzern damit beim Vorstand bzw. der Geschäftsführung.

Soweit es sich um Gesetze, Verordnungen, Unfallverhütungsvorschriften, Tarifverträge und Betriebsvereinbarungen handelt, die zugunsten der Beschäftigten gelten, trifft den Betriebsrat die Überwachungspflicht aus § 80 Abs. 1 Nr. 1 BetrVG: Es gehört zu seinen Aufgaben, darüber zu wachen, dass die bezeichneten Regelungen und Vereinbarungen eingehalten bzw. durchgeführt werden.

7 Für die AG §§ 76 Abs. 1, 91 Abs. 2 AktG bzw. für die GmbH § 43 GmbHG.
8 Vom 9. 12. 2009 – I-6 W 45/09, ZIP 2010, 28, 31 („IKB").

3.1 Rechtspflicht zur Einführung von Compliance-Management-Systemen

Umstritten ist jedoch, ob neben dieser allgemeinen – eigentlich selbstverständlichen – Pflicht der Geschäftsleitung, sich an die Gesetze zu halten, auch eine ausdrückliche gesetzliche Pflicht zur Einführung eines CMS existiert.

3.1.1 Keine grundsätzliche Rechtspflicht im deutschem Recht

Eine allgemeine und zwingende gesetzliche Verpflichtung zum Aufbau eines CMS besteht nach herrschender Meinung im deutschen Recht nicht (Zöllner/Noack 2010, § 43 Rn. 17; Hauschka 2010, § 1 Rn. 23; Kort 2008, S. 81). Lediglich für einige Branchen, z. B. Finanzinstitute und Wertpapierdienstleistungsunternehmen, bestehen hierzu gesetzliche Regelungen.[9] Jedoch kann sich die Notwendigkeit zur Einrichtung eines CMS aus der allgemeinen Sorgfaltspflicht der Geschäftsführung und aus den Grundsätzen ordnungsgemäßer Unternehmensführung ergeben. Dies ist z. B. anerkannt für börsennotierte Gesellschaften ab einer gewissen Größe, deren Geschäft ein Risiko hinsichtlich möglicher Gesetzesverletzungen mit sich bringt.[10] Für die Aktiengesellschaft hebt § 91 Abs. 2 AktG die gesetzliche, allgemeine Aufgabe des Vorstandes nach § 76 AktG hervor und verpflichtet den Vorstand einer Aktiengesellschaft dazu, geeignete Maßnahmen zu ergreifen, um Risiken zu vermeiden.[11] Dies bedeutet nicht, dass zwingend ein CMS eingeführt werden muss. Dennoch kann sich aus dieser Norm bei Vorliegen eines entsprechenden Gefahrenpotenzials für die Aktiengesellschaft die Pflicht zur Implementierung eines CMS ergeben. Compliance kann damit ein Bestandteil des Risikomanagements nach § 91 Abs. 2 AktG sein.[12]

Wenngleich für die GmbH eine Regelung, die mit § 91 AktG vergleichbar wäre, fehlt – der Sorgfaltsmaßstab dieser Vorschrift dürfte dennoch abhängig von einer bestimmten Größe, Komplexität und Unternehmensstruktur analog oder gemäß § 43 GmbHG auf die GmbH Anwendung finden.[13]

Im Ergebnis bedeutet dies: Kommt es zu Gesetzesverstößen im Unternehmen, kann jedes Mitglied des Vorstandes/der Geschäftsführung einem Schadenersatzanspruch der Gesellschaft ausgesetzt sein – es sei denn, die Geschäftsleitung hat veranlasst, ein „Überwachungssystem", das den Anforderungen des Unternehmens angemessen ist, zu errichten und weiterzuentwickeln. Dieses System muss dabei

9 Vgl. z. B. §§ 33, 39 WpHG; siehe Kap. 3.1.2.
10 Hüffer 2012, § 76 Rn. 9a.
11 Risikofrüherkennungssystem, vgl. Müller 2009.
12 Fleischer 2007, Rn. 43; Ringleb 2010, Rn. 624; Vetter 2009, S. 35 und Kap. VI.
13 Bungart/Strobl 2011, S. 42 f.

nicht zwingend ein CMS sein oder so bezeichnet werden. Gerade bei einer „kleineren“ GmbH kann es ausreichen, eine Revisions- oder Controlling-Abteilung (oder beide) einzurichten.

3.1.2 Compliance bei Banken und Versicherungen

Anderes gilt für Finanzinstitute und Versicherungen. Im Gegensatz zu Unternehmen anderer Branchen sind Unternehmen aus diesen Bereichen gesetzlich explizit verpflichtet, ein CMS einzurichten. Die entsprechende Verpflichtung ergibt sich aus dem WpHG,[14] dem KWG,[15] dem InvG[16] oder dem VAG.[17] Konkretisiert werden diese gesetzlichen Verpflichtungen insbesondere durch die von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) herausgegebenen Rundschreiben und den dort festgelegten

- Mindestanforderungen an das Risikomanagement von Banken (MaRisk (BA)) (konkretisiert die Maßnahmen im Zusammenhang mit § 25 a KWG),[18]
- Mindestanforderungen an das Risikomanagement von Versicherungen (MaRisk (VA)) (konkretisiert die Maßnahmen im Zusammenhang mit § 64a VAG),[19]
- Mindestanforderungen an das Risikomanagement für Investmentgesellschaften (InvMaRisk) (konkretisiert die Forderungen des § 9a InvG in 12 Punkten)[20] und
- Mindestanforderungen an Compliance und die weiteren Verhaltens-, Organisations- und Transparenzpflichten nach §§ 31 ff. WpHG (MaComp).[21]

14 Gesetz über den Wertpapierhandel, in der Fassung der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2708), zuletzt geändert durch Artikel 5 des Gesetzes vom 26. Juli 2011 (BGBl. I S. 1554).

15 Gesetz über das Kreditwesen (Kreditwesengesetz), in der Fassung der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2776), zuletzt geändert durch Artikel 2 des Gesetzes vom 22. Juni 2011 (BGBl. I S. 1126).

16 Investmentgesetz, in der Fassung vom 15. Dezember 2003 (BGBl. I S. 2676), zuletzt geändert durch Artikel 1 des Gesetzes vom 22. Juni 2011 (BGBl. I S. 1126).

17 Gesetz über die Beaufsichtigung der Versicherungsunternehmen (Versicherungsaufsichtsgesetz), in der Fassung der Bekanntmachung vom 17. Dezember 1992 (BGBl. 1993 I S. 2), zuletzt geändert durch Artikel 3 des Gesetzes vom 1. März 2011 (BGBl. I S. 288).

18 http://www.bafin.de/nn_722758/SharedDocs/Veroeffentlichungen/DE/Service/Rundschreiben/2010/rs__1011__ba__marisk.html

19 http://www.bafin.de/cln_228/nn_1214674/SharedDocs/Veroeffentlichungen/DE/Service/Rundschreiben/2009/rs__0903__marisk__va.html

20 http://www.bafin.de/cln_161/nn_722758/SharedDocs/Veroeffentlichungen/DE/Service/Rundschreiben/2010/rs__1005__wa__invmarisk.html

21 http://www.bafin.de/nn_2077192/SharedDocs/Artikel/DE/Service/Meldungen/2011/meldung__110614__macomp__neu.html

Die genauen Anforderungen ergeben sich aus den Vorgaben des jeweiligen Gesetzes und dem dazu korrespondierenden Rundschreiben der BaFin. Gleiches gilt für den Leitfaden des Bankenverbandes: Er dient als Beispiel bzw. Leitfaden dafür, wie die Vorgaben der BaFin umgesetzt werden können. Der Bankenverband gibt eine Best-Practice-Leitlinie für Wertpapier-Compliance heraus, die sich auch auf die Vorgaben der MaComp bezieht.[22]

3.1.3 Rechtspflicht in ausländischen Rechtsordnungen

Neben der deutschen Rechtsordnung sollte stets das Recht anderer Staaten bedacht werden. Auch aus deren Rechtsordnungen kann die Verpflichtung folgen, ein CMS einzurichten. Dies gilt etwa für Unternehmen, die z. B. an ausländischen Börsen notiert sind oder Verbindungen zu anderen Ländern unterhalten, z. B. enge wirtschaftliche Beziehungen.

Nachfolgend werden kurz die wichtigsten Regelungen aus den USA und Großbritannien geschildert, um hinsichtlich möglicher Risiken im internationalen Geschäftsbetrieb zu sensibilisieren.

Großbritannien

Derzeit wird unter Compliance-Gesichtspunkten vor allem der so genannte UK Bribery Act 2010[23] in der Fachliteratur diskutiert. Dieses Gesetz aus Großbritannien trat am 1. Juli 2011 in Kraft und gilt als das weltweit härteste Anti-Korruptionsgesetz. Nach diesem Gesetz können Verstöße von natürlichen Personen mit bis zu 10 Jahren Haft und die von Unternehmen mit unbegrenzten Bußgeldern bestraft werden.

Auch für deutsche Unternehmen ist dieses Gesetz relevant: Denn selbst dann, wenn das Unternehmen nicht in Großbritannien angesiedelt ist und nur einen Teil seiner Geschäfte dort ausübt, unterliegt es dem UK Bribery Act. Dies gilt für alle Firmenaktivitäten weltweit. In der Praxis gelten die Regelungen damit für nahezu alle global agierenden Unternehmen. So findet der UK Bribery Act immer Anwendung, wenn ein Unternehmen einen „geschäftlichen Bezug“ zu Großbritannien aufweist. Wenngleich nicht abschließend geklärt ist, was hierunter zu verstehen

22 http://www.bankenverband.de/downloads/082011/110728-compliance-best-practice-leitlinien.pdf
23 http://www.legislation.gov.uk/ukpga/2010/23/pdfs/ukpga_20100023_en.pdf

ist,[24] gilt dies jedenfalls für Zweitniederlassungen, Repräsentanzen und Produktionsstätten in Großbritannien. Wie weit der Arm des Gesetzes darüber hinaus reicht, kann derzeit noch nicht abschließend beurteilt werden.[25]

Anwendung findet der UK Bribery Act zum einen bei einer direkten Täterschaft. Hierfür muss die Tat a) entweder teilweise im Vereinigten Königreich begangen worden sein oder b) die Handlung im „Ausland" eine Straftat nach dem Recht des Vereinigten Königreichs darstellen und der Täter eine „close connection" (enge Verbindung) zu diesem Rechtskreis aufweisen.[26] Als Tathandlungen kommen nach Section 1 u. a. das Anbieten, Versprechen oder Gewähren von finanziellen oder anderen Vorteilen in Betracht, wenn dies in der Absicht erfolgt, hierdurch eine pflichtwidrige Handlung zu belohnen oder zu fördern. Die Tathandlung ist damit vergleichbar mit der Bestechung nach deutschem Recht (§ 299 StGB). Neben der klassischen Bestechung werden auch so genannte „facilitation payments" bestraft. Dies entspricht mehr oder weniger dem Straftatbestand der Vorteilsgewährung nach § 331 StGB. Danach genügt es, wenn eine Zahlung geleistet wird, um einen Vorgang unrechtmäßig zu beschleunigen. Anders als im deutschen Recht gilt dies jedoch nicht nur für Amtsträger (d. h. den öffentlichen Bereich), sondern auch für den Bereich der Privatwirtschaft. Die Tathandlung kann dabei aktiv, durch Handeln, oder passiv, durch Unterlassen, erfolgen.[27] Mögliche Täter sind juristische und natürliche Personen mit enger Verbindung zum Vereinigten Königreich.

Neben der direkten Tatbegehung kommt zum anderen eine Verantwortlichkeit für das Handeln Dritter in Betracht. Unternehmen können sogar dann haften, wenn korrupte Handlungen nicht im Unternehmen selbst begangen werden, sondern diese vielmehr „nur" durch einen Geschäftspartner begannen werden. In der Praxis besteht damit die Gefahr, dass sich eine deutsche Firma nach englischem Recht strafbar macht, weil ein Geschäftspartner ihrer ausländischen Tochtergesellschaft Schmiergeld verteilt.

24 An einer genauen Definition fehlt es. In Section 7 Abs. 5 des UK Bribery Act 210 heißt es lediglich: „relevant commercial organisation means relevant commercial organisation" means – (a) a body which is incorporated under the law of any part of the United Kingdom and which carries on a business (whether there or elsewhere), (b) any other body corporate (wherever incorporated) which carries on a business, or part of a business, in any part of the United Kingdom, (c) a partnership which is formed under the law of any part of the United Kingdom and which carries on a business (whether there or elsewhere), or (d) any other partnership (wherever formed) which carries on a business, or part of a business, in any part of the United Kingdom, and, for the purposes of this section, a trade or profession is a business."

25 Kappel/Ehling 2011, S. 2116.

26 Vgl. Modlinger/Richter 2011, S. 16.

27 Vgl. Modlinger/Richter 2011, S. 16.

Der Verantwortlichkeit für Straftaten von Unternehmensangehörigen kann sich ein Unternehmen allerdings durch die (einzige) im Gesetz genannte Verteidigungsmöglichkeit entziehen: Es muss nachweisen können, dass eine „adequate defense" – mit anderen Worten: ein angemessenes CMS – vorhanden ist. Existiert ein solches CMS, werden die Verstöße von Beschäftigten als Exzesstat qualifiziert. Für diese muss nicht mehr das Unternehmen einstehen.[28] Wie ein angemessenes CMS gestaltet sein kann, wurde in einem Leitfaden des Justizministeriums veröffentlicht.[29] Den Unternehmen wird danach in Form von sechs „Prinzipien" ein Rahmen gegeben, in dem sie ihr CMS gestalten können.[30] Diese sechs Prinzipien lauten:

- Verhältnismäßiges Verfahren (proportionate procedures): Hiernach soll ein CMS in einem angemessenen Verhältnis zu den Bestechungsrisiken stehen, die sich aus der Natur, dem Umfang und der Komplexität der unternehmerischen Aktivitäten ergeben. Die Maßnahmen sollen klar, praktikabel und effektiv durchgesetzt werden.
- Verpflichtung des Top-Managements (top-level commitment): Hierunter wird u. a. die Verpflichtung des Top-Managements verstanden, eine unternehmensweite Kultur der Ächtung von Korruption zu schaffen (tone from the top).
- Risikobeurteilung (risk assessment): Unter diesem Punkt wird u. a. darauf hingewiesen, dass die notwenigen Compliance-Maßnahmen von den jeweiligen Risiken abhängen. Daher sollte eine Risikobeurteilung bzw. -analyse erfolgen. Mögliche unterschiedliche Risikobereiche werden benannt.
- Gebührende Sorgfalt/Überprüfung (due diligence): Suggeriert u. a. die Forderung, dass ein Unternehmen sich Kenntnis über seine Geschäftspartner und seine Geschäftsbeziehungen aneignet.
- Kommunikation und Trainings (communication including training): Die Präventions-/Compliance-Maßnahmen und Regeln sollen durch entsprechende Kommunikation und Schulungen im Unternehmen vermittelt werden.
- Überwachung und Prüfung (monitoring and review): Das letzte Prinzip beinhaltet die Überwachung des zuvor eingeführten CMS. Unternehmen sollen ihr CMS danach einer Selbstkontrolle unterwerfen und auf Veränderungen reagieren.

Abschließend lässt sich feststellen, dass diese Prinzipien selbstverständlich für jedes CMS sein sollten (vgl. Kap. 4.3). Hinsichtlich der Anforderungen an ein CMS bringt der UK Bribery Act damit nichts Neues. Zumindest werden sich be-

28 Modlinger/Richter 2011, S. 18.

29 http://www.justice.gov.uk/downloads/guidance/making-reviewing-law/bribery-act-2010-guidance.pdf

30 Vgl. Modlinger/Richter 2011, S. 18 f.

stehende CMS mit vertretbarem Aufwand an die Anforderungen des UK Bribery Act anpassen lassen.[31] Die möglichen Haftungen und Strafen, die aus dem UK Bribery Act folgen, unterstreichen, dass sich Unternehmen ab einer bestimmten Größe mit dem Thema Compliance beschäftigen sollten.

USA

In den Vereinigten Staaten wurde Compliance in den letzten Monaten vielfach aufgrund ausländischer Gesetze, insbesondere aufgrund des UK Bribery Act 2010 diskutiert. Ausgelöst wurde diese Diskussion jedoch durch die Gesetzgebung der USA selbst: durch den Erlass des US-amerikanischen Bundesgesetzes Sarbanes-Oxley-Act (SOX) im Jahr 2002. Hintergrund für dieses Gesetz war der Vertrauensverlust aufgrund von fehlerhaften Finanzberichtserstattungen und Bilanzmanipulationen. Der SOX sollte das Vertrauen durch verstärke Transparenzanforderungen wieder herstellen.[32] Das Gesetz regelt dabei u. a. neben verschiedenen Aspekten der Corporate Governance auch die Compliance von Unternehmen, die Berichterstattungspflichten von Publikumsgesellschaften sowie die damit zusammenhängende Durchsetzung. Die so genannte SOX-Compliance wurde daher schnell ein Bestandteil deutscher Unternehmen, die an einer US-Börse gelistet waren bzw. sind. Noch heute wird Compliance oft mit diesem Gesetz in Verbindung gebracht.

Wie der UK Bribery Act verfügt die USA mit dem Foreign Corrupt Practices Act von 1977 zudem auch über ein Bundesgesetz. Es verbietet Zahlungen und Wertgeschenke an ausländische staatliche Amtsträger, wenn diese Leistungen bezwecken, den Zuschlag für ein Geschäft zu bekommen oder eine Geschäftsbeziehung aufrechtzuerhalten. Anders als der UK Bribery Act betrifft der Foreign Corrupt Practices Act jedoch nur die Bestechung von Amtsträgern. Vergleichbar sind beide Gesetzte in ihrem weltweiten Anwendungsbereich.

Neben dem SOX und dem Foreign Corrupt Practices Act führen vor allem die United States Sentencing Guidelines[33] dazu, dass sich Unternehmen mit Bezug zum US-amerikanischen Markt verstärkt mit Compliance beschäftigen.[34] Dabei handelt es sich um die Strafzumessungsrichtlinien des amerikanischen Bundesrechts. Sie regeln seit 1991 die Bestrafung von Unternehmen z. B. bei Korruption. Bei der Strafzumessung wird insbesondere die Frage betrachtet, ob ein angemessenes CMS vorliegt und wie auf die Entdeckung einer Tat reagiert wird. Auch

31 Modlinger/Richter 2011, S. 21.
32 Ausführlich zum SOX: Grummer/Seeburg 2011.
33 Erlassen durch die US-Behörde United States Sentencing Commission. Sie ist zuständig für die Festlegung von Grundsätzen für die Strafbemessung an Bundesgerichten.
34 Abrufbar unter http://www.ussc.gov

kann die Erstellung eines Compliance-Programms eine Sanktion – quasi eine Bewährungsstrafe – nach den Guidelines darstellen.[35] Für Compliance-Praktiker sind die Vorgaben der United States Sentencing Guidelines von Interesse, da sie umfangreich darlegen, wie ein Compliance-Management-System gestaltet sein muss. Sie gehen beispielsweise davon aus, dass externe Berater bei der Evaluierung eines CMS mit größerer Objektivität Schwachstellen ausfindig machen (und ausräumen). Unternehmen sollten sich daher intensiv mit einer externen Evaluierung ihres CMS auseinandersetzen.[36] Zertifizierungen, die neuerdings angebotenen werden, können dies ggf. sicherstellen – sofern sie Evaluierungen umfassen (vgl. Kap. VII).

3.2 Kosten eines Compliance-Management-Systems

Wie die nachfolgenden Ausführungen zeigen, können zahlreiche Maßnahmen Bestandteil eines CMS sein. Im Rahmen dessen sollte stets abgewogen werden, welche Maßnahmen für das jeweilige Unternehmen angemessen sind – es sei nicht verschwiegen, dass Compliance durchaus mit Kosten verbunden ist. Nur ein Compliance-Team, das mit genügend finanziellen und personellen Ressourcen ausgestattet ist, kann die Funktionsfähigkeit eines CMS gewährleisten. Welche Aufwendungen erforderlich sind für eine angemessene Ausstattung, wird maßgeblich durch die individuellen Risiken vorgegeben, denen ein Unternehmen ausgesetzt ist. Eine pauschale Aussage, welche Kosten für ein „gutes“ CMS aufgewendet werden müssen, lässt sich daher seriös nicht treffen.

In diesem Zusammenhang sollte allen Beteiligten bewusst sein, dass die Anforderungen an und die Aufwendungen in ein CMS zukünftig weiter steigen werden.[37] Oft handelt es sich jedoch um gut investiertes Geld, mithilfe dessen Imageschäden und Bußgelder[38] vermieden oder reduziert werden können. Dementsprechend bestätigt eine aktuelle Umfrage, dass die Kosten für Compliance-Maßnahmen deutlich niedriger liegen als die Kosten bei regelwidrigem Verhalten.[39]

35 Engelhart 2011, S. 126 ff.
36 Engelhart 2011, S. 127.
37 Vgl. Der Aufsichtsrat 01/2011, S. 11.
38 Diese können in großen Unternehmen wie z. B. Siemens durchaus bei dreistelligen Millionenbeträgen liegen; vgl. Becker u. a. 2011.
39 Vgl. Bungart/Strobl 2011, S. 41 ff.

4 Aufbau eines Compliance-Management-Systems

Jedes Unternehmen ist unterschiedlichen Risiken ausgesetzt.[40] Daher lässt sich kein einheitliches CMS etablieren. Jedes System muss spezifisch auf das jeweilige Unternehmen und den jeweiligen Konzern angepasst werden. Hierfür gilt es, die relevanten Risiken des Unternehmens zu ermitteln. Zudem ist abzuwägen, welchen Risiken man mit einem CMS begegnen möchte – nur so kann es effektiv implementiert werden. Ein Compliance-Management-System stellt damit ein Unikat dar, das auf das jeweilige Unternehmen bzw. den jeweiligen Konzern abgestimmt sein sollte.

Zwar unterscheiden sich die Risiken jedes Unternehmens, weshalb sich die Compliance-Struktur nicht allgemein festlegen oder beschreiben lässt. Dennoch werden mit einem CMS erfahrungsgemäß ähnliche Ziele verfolgt. Alle Systeme wollen Regelverstöße verhindern – sei es, um die Haftung zu reduzieren, um Imageschäden zu vermeiden oder um (strafrechtlichen) Sanktionen zu entgehen. Darüber hinaus sollen die meisten CMS sowohl Dritte schützen als auch die eigenen Beschäftigten sowie ein positives Image in der Öffentlichkeit bewirken. Aus diesem Grund sind einige Elemente entweder unabdingbar oder zumindest regelmäßig Bestandteil eines CMS (Kap. 4.3; Kap. V).

4.1 Risikoermittlung als zentraler Bestandteil

Für jedes Unternehmen ist relevant, unterschiedliche rechtliche, ethische und moralische Regelungen einzuhalten. Das CMS muss unternehmensbezogene Unterschiede berücksichtigen und die konkreten Compliance-relevanten Risikofelder des Unternehmens ermitteln (Risikoanalyse, Risk Assessment). Bei einer solchen Risikoanalyse müssen z. B. die Geschäftsfelder, die Absatzmärkte sowie die Organisationsstruktur des jeweiligen Unternehmens bzw. Konzerns berücksichtigt werden.[41] Bei der Bewertung des Geschäftsfelds sind u. a. der Auftragsumfang, die Geschäftspartner (z. B. öffentliche Hand), die Branche (bestehen korruptionsanfällige Geschäftsfelder?), die vertriebenen Produkte (gelten besondere Import- und Exportbestimmungen?) oder Umweltrisiken zu beachten. Hinsichtlich der Märkte

40 Pütz 2011, S. 19.
41 Vgl. Pütz 2011, S. 17 ff; vgl. Kap. VI.

sollte hinterfragt werden, ob sich darunter so genannte „Risikoländer“[42] befinden. Zudem sollte man auf kulturelle Besonderheiten, eventuelle Sprachbarrieren und gesetzliche Unterschiede eingehen. Bei der (eigenen) Unternehmensorganisation gilt es insbesondere, die Konzern- und Verkaufsstruktur (Handelsvertreter) zu beleuchten.[43]

Beispiel:
Im Finanzsektor müssen die Unternehmen aufgrund der zunehmend geforderten Risikoorientierung der internationalen Aufsichtsbehörden die jeweils lokalen Rechtsgrundlagen aller konzernweit relevanten Tochtergesellschaften (z. B. Schweiz, Deutschland, Frankreich, USA) berücksichtigten – nicht zuletzt, da ein konzernweites Compliance-Management-System all diesen Regelungen gerecht werden sollte.

Die Analyse dieser Risikofelder sollte dabei in vier Stufen erfolgen: Zunächst sollten alle grundsätzlich möglichen Risiken ermittelt und beschrieben werden. Danach werden diese Risiken sinnvollerweise strukturiert und kategorisiert. In einem dritten Schritt werden die tatsächlichen Risiken für das Unternehmen analysiert und beziffert. Dabei müssen z. B. die mögliche Schadenshöhe und deren Eintrittswahrscheinlichkeit ermittelt werden. Zuletzt sollten bereits an dieser Stelle mögliche risikomindernde Maßnahmen bedacht werden. Der Vorteil dieses Vorgehens: Nach einer Analyse des jeweiligen Geschäfts, der Märkte und der Unternehmensorganisation sind in der Regel zunächst zahlreiche grundsätzlich relevante Compliance-Einsatzfelder identifiziert. Dennoch kann ein Compliance-System oftmals nicht alle ermittelten möglicherweise relevanten Bereiche erfassen. Wichtig ist es daher, unter den ermittelten Bereichen Schwerpunkte zu setzen. Man muss abwägen: Welche Themen erweisen sich als so wichtig, dass sie in einem CMS berücksichtigt werden müssen? Dabei gilt es, darauf zu achten, dass bestimmte Bereiche und Themen bereits in anderen (Fach-)Abteilungen wie z. B. Controlling oder Revision bearbeitet werden. Solche bereits vorhandenen Strukturen sollten bei der Einführung eines CMS genutzt und darauf aufgebaut werden. In diesem Zusammenhang müssen auch die Strukturen beachtet werden, die hinsichtlich einer eventuell vorliegenden CSR-Strategie geschaffen wurden.

42 Vgl. z. B. den Korruptionswahrnehmungsindex/Corruption Perceptions Index (CPI) und den Bestecher-Index/Bribe Payers Index (BPI) von Transparency International, abrufbar unter http://www.transparency.de/Korruptionsindices.382.0.html

43 Die möglichen Risikofelder werden hier nicht abschließend aufgezählt; vgl. Pütz 2011, S. 17 ff.

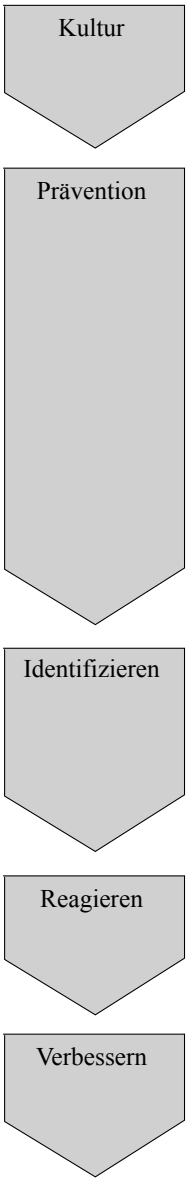
Zuletzt gilt es zu bedenken, dass es sich bei Compliance um einen stetigen Prozess handelt. Die Risiken eines Unternehmens verändern sich, sie müssen daher regelmäßig analysiert werden.

4.2 Das Compliance-Management-System

Sobald die relevanten Bereiche ermittelt sind, kann ein CMS entwickelt werden. Dies gelingt auf längere Sicht nur, wenn auftretende Verstöße schnell entdeckt werden, so dass umgehend reagiert werden kann. Compliance ist damit ein immerwährender Prozess, der sich zudem stets weiterentwickelt.
Ein CMS sollte darauf abzielen,

- Compliance-Verstöße zu verhindern (Prävention),
- auftretende Verfehlungen so schnell wie möglich zu erkennen (Detection),
- auf Verfehlungen schnell, effektiv und konsequent zu reagieren (Response).

In der Praxis existieren zahlreiche Organisationsformen von CMS, die in ihrer genauen Ausgestaltung voneinander abweichen. Gleichwohl folgen alle CMS häufig einem ähnlichen System und enthalten ähnliche Bestandteile (vgl. Kap. V). Vielfach wird versucht, eine „Compliance-Kultur“ im Unternehmen zu schaffen. Dies geschieht u. a. durch ein unmissverständliches Bekenntnis der Geschäftsleitung und des Managements zur Compliance, was oft durch die Einführung einen Verhaltenskodex begleitet wird. Um Compliance-Verstöße zu vermeiden, sind oft konzernweite, regelmäßige Schulungen (Präsenz- und/oder Onlinetrainings), die Bereitstellung von Hinweisgebersystemen (Whistleblowing) oder die Präsenz von Compliance Officers Bestandteil eines CMS. Mit der Prävention geht die Identifikation von Verstößen einher. Auch hier helfen Hinweisgebersysteme, Sonderuntersuchungen oder Mitarbeiterbefragungen. Für den Fall, dass Verstöße ermittelt wurden, regeln viele CMS auch die Reaktion hierauf, indem sie z. B. die Sanktionsmaßnahmen vereinheitlichen oder ein Sanktions-Komitee schaffen. Zuletzt sollten sich alle CMS mit der Frage beschäftigen, wie das System kontinuierlich verbessert werden kann. Hierfür kann ein Compliance-Dialog mit Dritten, z. B. Geschäftspartnern, Behörden, aber auch mit den Beschäftigten und deren Vertretern sinnvoll sein. Zudem sollten Compliance-Strukturen regelmäßig überprüft werden. Die folgende Abbildung gibt einige (weitere) Compliance-Maßnahmen wieder.



Quelle: Angelehnt an eine Präsentation von Olaf Schneider; LL.M. (Chief Compliance Officer MAN SE): http://www.boeckler.de/pdf/v_2010_04_29_schneider.pdf; siehe auch Pütz, Hans-Böckler-Stiftung (Hrsg.), Arbeitshilfe für Aufsichtsräte Nr. 15, Compliance, Düsseldorf 2011, S. 22.

Praxistipp:
In 11 Schritten zum Compliance-Management-System:

1. Bekenntnis der Geschäftsleitung und idealerweise des BR und AR (Commitment)
2. Risikoanalyse (Risk Assessment)
3. Ziel eines CMS festlegen
4. Elemente des CMS entwickeln und erstellen (Hinweisgebersystem, Richtlinien, Merkblätter, Schulungen, Beratung, Sanktionskatalog etc.)
5. Organisation und Berichtslinien festlegen (Stabstelle, Rechtsabteilung, Revisionsabteilung, intern oder extern)
6. Compliance Team angemessen ausgestattet?
7. Spätestens hier, idealerweise bei allen Schritten: Mitbestimmung der AN berücksichtigen
8. Beschluss der Geschäftsleitung und ggf. des AR einholen
9. Kommunikation (Schulungen, E-Learning, Inter-/Intranet-Portal)
10. Umsetzung der Elemente
11. CMS überprüfen und verbessern

Zu einem Compliance-Management-System gehört neben den oben bezeichneten Maßnahmen und den Grundsätzen, Compliance im Unternehmen zu organisieren.[44] Hierbei sind wiederum verschiedene Ansätze möglich, die jeweils auf das Unternehmen abzustimmen sind. Beispielsweise kann eine eigene Stabstelle (Compliance-Abteilung) eingerichtet werden. In anderen Fällen wird es etwa der Abteilung Recht bzw. Revision zugeordnet. Dabei sollte jedoch berücksichtigt werden, dass die Revisionsabteilung ab einer bestimmten Unternehmensgröße nicht mehr mit Compliance-Aufgaben betraut werden sollte. Andernfalls lassen sich Konflikte nicht mehr ausschließen. Wichtig ist bei allen Organisationsformen, dass die Berichtslinien sowie die (internen) Zuständigkeiten aller Beteiligten (auch des Aufsichtsrats) eindeutig festgelegt sind.

Rechtlich gibt es verschiedene Möglichkeiten, die „Pflichten" umzusetzen, die sich für die Beschäftigten eines Unternehmens aus einem Compliance-Programm ergeben. Die betroffenen Mitarbeiterinnen und Mitarbeiter sowie die Mitbestimmungsakteure sollten spätestens bei der Umsetzung sorgfältig prüfen, ob diese

44 Mögliche Compliance-Strukturen siehe Fett/Theusinger 2010.

rechtlich zulässig ist und ob ihre Mitbestimmungsrechte eingehalten wurden.[45] Hierfür sollten sie ggf. externen Rat einholen.

Praxistipp:
Transparenz stellt einen wichtigen Bestandteil von Compliance dar. Daher sei allen Unternehmen empfohlen, bei allen Schritten – d. h. bereits vor der Umsetzung des CMS – die Arbeitnehmervertreter einzubinden, insbesondere den Betriebsrat. Wenngleich dies nicht für alle Maßnahmen und Schritte gesetzlich zwingend ist, schafft es doch das nötige Vertrauen in ein CMS. Die Frage, wie vertrauensvoll der Dialog zwischen Arbeitgeber und Arbeitnehmern bzw. Betriebsräten geführt wird, entscheidet oft über das Gelingen eines CMS.

4.3 Bestandteile eines Compliance-Management-Systems

Wie das Schaubild in Kap. 4.2 zeigt, kann ein CMS zahlreiche Maßnahmen enthalten. Es erweist sich als schwierig, alle Maßnahmen detailliert und abschließend darzustellen. Untersuchungen zeigen, dass einzelne Maßnahmen in vielen CMS vorhanden sind (vgl. Kap. V). Einige von ihnen werden im Folgenden genauer betrachtet (ausführlich Kap. IV).

4.3.1 Der Compliance Officer

Zu den beschriebenen Systemen gehört regelmäßig, dass im Unternehmen ein so genannter Compliance Manager oder Compliance Officer eingesetzt wird. Er agiert sinnvollerweise unabhängig von bestehenden Hierarchien und trägt unternehmensweit Verantwortung. Er gehört daher meist entweder selbst der Geschäftsführung an oder ist ihr (oder dem Aufsichtsrat) direkt unterstellt. Zwingend erforderlich ist die Stelle eines Compliance Officers für eine Complinace-Organisation jedoch nicht.

Sollte der Compliance Officer dem Aufsichtsrat unterstellt sein, kann dies nur hinsichtlich der Berichtslinie erfolgen. Arbeitsrechtlicher Vorgesetzter des

45 Beispielsweise befand das LAG Düsseldorf, dass ein weltweit gültiger Verhaltenskodex für Wal-Markt-Angestellte dem Grundgesetz zuwiderlaufe und damit unwirksam sei. Er bestimmt, dass Beschäftigte nicht mit Personen ausgehen oder eine Liebesbeziehung eingehen dürfen, die die Arbeitsbedingungen beeinflussen oder deren Arbeitsbedingungen von der bzw. dem Beschäftigten beeinflusst werden können (LAG Düsseldorf vom 14.11.2005 – 10 TaBV 46/05 = DB 2006, 162).

Compliance Officer bleibt immer die Geschäftsleitung. Zudem kann die Berichtslinie nicht durch den Aufsichtsrat bestimmt werden. Vielmehr entscheidet die Geschäftsleitung, ob und wann der Officer direkt an den Aufsichtsrat berichtet. Trotzdem sollte der Aufsichtsrat darauf hinwirken, dass eine direkte Berichtslinie an ihn besteht.

Die Funktion eines Compliance Officers kann intern mit einer bzw. einem Angestellten des Unternehmens besetzt werden oder mit externen Personen. Bei letzteren handelt es sich häufig um Rechtsanwälte oder Anwaltskanzleien. Welche Variante besser ist, hängt vom jeweiligen Unternehmen ab. Ein internes System hat den Vorteil, dass der Compliance Officer über bessere Kenntnis des Unternehmens verfügt, meist schneller reagieren kann und der Geschäftsleitung zur Berichtserstattung verpflichtet ist. Mit diesen Vorteilen gehen jedoch auch Nachteile einher: Ein interner Compliance Officer genießt oft geringeres Vertrauen der Beschäftigten und gerät möglicherweise in Loyalitätskonflikte. Für eine externe Besetzung sprechen ggf. eine besondere Expertise, die bessere Vertraulichkeit sowie eine größere Unabhängigkeit der externen Fachkräfte. Dem stehen allerdings meist geringe Unternehmenskenntnisse sowie eine längere Bearbeitungsdauer gegenüber.[46]

Der Umfang der Gesetze und Regularien, die berücksichtigt werden müssen, ist groß. Daher kann deren Einhaltung in einigen Unternehmen nicht immer durch eine Person oder Abteilung kontrolliert werden. Mitunter ist es angebracht, dass sich in jedem Geschäfts- oder Unternehmensbereich eine Person – neben deren eigentlicher Tätigkeit – Spezialwissen hinsichtlich Compliance aneignet und sich so zum Compliance-Beauftragten etabliert. Diese Person berichtet direkt an den (Chief) Compliance Officer.

4.3.2 Hinweisgebersysteme

Ein weiterer (vermehrt diskutierter) Bestandteil einer Compliance-Organisation kann eine so genannte Hinweisgeber- bzw. Whistleblower-Hotline oder der Einsatz eines Ombudsmanns sein.[47] Für Unternehmen, die in den USA börsennotiert sind, ergibt sich aus dem Sarbanes Oxley Act die Verpflichtung, ein derartiges System einzurichten. Anders hierzulande: In Deutschland besteht diese Pflicht nicht. Gleichwohl wollen einige Unternehmen die Möglichkeit schaffen, Fälle

46 Pütz 2011, S. 24 f.
47 Vgl. Schulz 2011.

zu melden, die Compliance betreffen könnten, und dabei den Hinweisgeber zu schützen.[48]

Argumente für und gegen ein solches Hinweisgebersystem finden sich zahlreich. Es sei hervorgehoben, dass die Einführung einer Whistleblower-Hotline oder eines Ombudsmanns nur Erfolg haben wird, wenn die Beschäftigten dieser Einrichtung vertrauen und sie akzeptieren.[49] Die Mitbestimmungsakteure können sich dafür engagieren, dass im Unternehmen eine Kultur herrscht, die die Hemmschwelle für Beschäftigte senkt, intern Hinweise zu geben und grobe Missstände und Gefahren abzustellen (vgl. Kap. III, Kap. IV).

4.3.3 Unternehmensinterne Untersuchungen

Unternehmensinterne Untersuchungen können als Präventionsmaßnahme oder als Reaktion auf Verstöße ebenfalls Bestandteil einer Compliance-Organisation sein. In einigen Situationen können nur mittels solcher Untersuchungen die notwendigen internen Maßnahmen veranlasst werden, z. B. eine Korruptionsprävention bei konkreten Verdachtsmomenten. Aufklärung bildet zudem meist den ersten Schritt, um Lücken im Kontrollsystem zu schließen.

Eine unternehmensinterne Untersuchung kann durch externe Ermittler oder durch interne Ermittlungen erfolgen, z. B. durch die Revisions- oder Compliance-Abteilung. Welches Vorgehen sinnvoll ist, ist eine Frage des Einzelfalles. Bei allen Untersuchungen müssen – insbesondere wegen des Compliance-Gedankens – die einschlägigen Gesetze beachtet werden. Dabei sollte auch erwogen werden, ab wann amtliche Stellen eingeschaltet bzw. informiert werden sollten. Bei der unternehmensinternen Untersuchung sollte darauf geachtet werden, dass nicht der Anschein „amtlichen“ Handelns z. B. durch die Staatsanwaltschaft oder Kartellbehörde entsteht.

48 Mit seinem Urteil vom 21.07.2011 hat der Europäische Gerichtshof für Menschenrechte (EGMR) gegen Deutschland geurteilt wegen einer Verletzung von Art. 10 (Freiheit der Meinungsäußerung) der Europäischen Menschenrechtskonvention (EMRK) (Beschwerde-Nr. 28274/08). Er setzte sich damit für den Schutz von Whistleblowern ein. Im konkreten Fall hatte eine Altenpflegerin ihren Arbeitgeber, einen Klinikbetreiber, des Betrugs beschuldigt. Die Ermittlungen der Staatsanwaltschaft gegen die Klinikbetreiber wurden indes eingestellt. Die Klägerin erhielt eine fristlose Kündigung. Die deutschen Gerichte bestätigten diese Entlassung mit dem Argument der Verletzung von Loyalitätspflichten gegenüber dem Arbeitgeber. Der EGMR gelangt jedoch zu dem Ergebnis, dass die deutschen Gerichte keinen angemessenen Ausgleich herbeigeführt hätten: zwischen der Notwendigkeit, den Ruf des Arbeitgebers zu schützen, einerseits und der Notwendigkeit, das Recht auf Freiheit der Meinungsäußerung der Altenpflegerin zu schützen, andererseits.

49 Rohde-Liebenau, 2005.

4.3.4 Kooperation mit Behörden und anderen Institutionen

Selbst wenn eine Compliance-Organisation eingesetzt wurde, können Regelverstöße nicht vollständig ausgeschlossen werden. Es kann daher zu staatlichen Ermittlungen z. B. durch die Staatsanwaltschaft kommen, wenn unternehmensinterne Vorfälle einen gewissen Umfang haben. Denkbar sind aber auch Untersuchungen von Geschäftspartnern oder anderen Institutionen, z. B. Projektfinanzierern, die diese im Zuge ihrer Compliance-Organisation durchführen. Ist man von einer solchen externen Ermittlung betroffen, sollte über eine Kooperation mit diesen Stellen über die bestehenden rechtlichen Verpflichtungen hinaus nachgedacht werden, z. B. als Kronzeuge in Kartellverfahren. So lassen sich spätere Strafzahlungen und andere Sanktionen vermeiden oder zumindest verringern. Oft wird damit ein drohender Imageschaden begrenzt.

Bei jeder Kooperation sind jedoch unbedingt die rechtlichen Grenzen einzuhalten. Beispielsweise können bestimmte personenbezogene Daten zulasten von Beschäftigten nicht ohne weiteres weitergegeben werden.[50] Auch die Fürsorgepflicht des Arbeitgebers gegenüber den Arbeitnehmenden muss beachtet werden. Andererseits kennt diese Fürsorgepflicht auch Grenzen: Bei bestimmten schweren Verstößen müssen die entsprechenden Behörden, z. B. die Kartellbehörde oder die Staatsanwaltschaft, unterrichtet werden. Generell sollten solche Kooperationen nur im Einvernehmen mit dem Betriebsrat und ggf. den Arbeitnehmervertretern im Aufsichtsrat eingegangen werden.

5 Compliance: Chance oder Gefahr für die Mitbestimmung?

Für Arbeitnehmervertreter bedeutet die Einrichtung eines CMS sowohl eine Chance als auch eine Gefahr. Es besteht das Risiko, dass Compliance dazu „missbraucht“ wird, Mandatsträger bei ihren Entscheidungen unter Druck zu setzen. Möglicherweise werden die Zustimmung zu Maßnahmen mit dem Verweis auf Compliance verlangt und Bedenken der Arbeitnehmervertreter ignoriert. Ein in der Praxis gängiges Beispiel stellen Ethik-Richtlinien des ausländischen Mutterkonzerns dar, die ohne Beachtung der deutschen Gesetze eins zu eins umgesetzt werden. Dies entspricht jedoch nicht dem Compliance-Gedanken.[51] Vielmehr sollte Compliance ein Schritt zu mehr Transparenz und Beteiligung sein. Arbeitnehmervertreter im Aufsichtsrat und Betriebsräte sollten daher bei der Einrichtung

50 Hinsichtlich der wichtigsten Fragen und Antworten zum Arbeitnehmerdatenschutz siehe DGB Bundesvorstand 2009, https://www.dgb-bestellservice.de/besys_dgb/pdf/DGB31098.pdf [17.05.2011]

51 Siehe hierzu auch: Hexel/Pütz, 2012.

eines CMS eine aktive Rolle übernehmen und ihre Erfahrungen und Kompetenzen einbringen. Hierbei gilt: Bei der Einführung von Bestandteilen eines CMS wie z. B. Ethik-Richtlinien (Codes of Conduct) müssen die Mitbestimmungsrechte des Betriebsrats unbedingt beachtet werden (vgl. Kap. III). Ausländische Vorschriften, die zur Einführung eines Compliance-Systems verpflichten, schließen Mitbestimmungsrechte nach dem BetrVG nicht aus, sofern keine wirksame Transformation dieser ausländischen Vorschriften in deutsches Recht vorliegt.[52]

Neben möglichen Risiken bietet die Umsetzung von Compliance im Unternehmen auch Chancen für die Mitbestimmungsakteure: Sie kann dazu beitragen, die Entscheidungsfindung transparent zu gestalten und dem Vorwurf der Vetternwirtschaft vorzubeugen. Zudem kann Compliance als Instrument der Mitbestimmung dienen: Ein CMS erleichtert es Betriebsräten und Arbeitnehmervertretern im Aufsichtsrat, z. B. über den Rahmen ihrer betriebsverfassungs- und aktienrechtlich definierten Rechte hinaus mitzugestalten. Leider gelingt dies meist nur jenen Akteuren auf der Arbeitnehmerseite, die bereits über eine starke und gefestigte Position im Unternehmen verfügen.

Auch die Geschäftsleitung sollte an einer guten Zusammenarbeit mit den Arbeitnehmervertretern interessiert sein. Denn der bewusste Austausch ihrerseits bzw. des Compliance Officers mit den Arbeitnehmervertretern im Aufsichts- und Betriebsrat liefert oft wichtige Erkenntnisse. Letztlich setzt ein erfolgreiches CMS in der Praxis immer die Zusammenarbeit unterschiedlicher Organe, Bereiche und Abteilungen voraus. Nur so kann gewährleistet werden, dass die zahlreichen öffentlich-rechtlichen Pflichten, Gebote und Verbote wie z. B. Zollvorschriften, Umweltbestimmungen, Kapitalmarkt- und Kartellrecht, Recht der Arbeitssicherheit oder Datenschutz überhaupt erkannt und eingehalten werden. Zuletzt sollte auch der Berichtsweg über den Betriebsrat an die Geschäftsleitung und/oder den Aufsichtsrat berücksichtigt werden.

6 Fazit

Publikationen zum Thema Compliance nehmen deutlich zu. Dennoch steckt hinter dem aus dem angloamerikanischen Rechtskreis übernommenen Begriff grundsätzlich wenig Neues. Letztlich bezeichnet er nichts anderes als die aus juristischer Sicht selbstverständliche Pflicht, Gesetze, Richtlinien sowie auch freiwillige Kodizes in Unternehmen einzuhalten.

52 Vgl. BAG vom 22.07.2008 – 1 ABR 40/07.

Neu sind allerdings die Mechanismen – das Compliance-System bzw. die Compliance-Organisation –, mit denen die Einhaltung der Regeln sichergestellt werden soll.[53] Genügte es früher, eine Controlling- oder Revisionsabteilung zu unterhalten, führen heute immer mehr Unternehmen teils umfangreiche Compliance-Management-Systeme ein. Neu ist auch, dass deutsche Gesetze und Verordnungen mittlerweile den Begriff Compliance verwenden und manche Branchen, insbesondere den Finanzbereich, zur Einführung eines CMS verpflichten.[54] Diese Pflicht ergibt sich auch vermehrt aus vertraglichen Bindungen, z. B. innerhalb von Lieferketten. Üblicherweise werden (ausländische) Zulieferer vertraglich dazu verpflichtet, gewisse Mindeststandards bei Arbeits- und Umweltschutz einzuhalten. Dadurch wird ein CMS auch auf die Zulieferer ausgeweitet.

Arbeitnehmervertreter sollten sich durch den Begriff Compliance nicht unter Druck setzen lassen. Sie sollten vielmehr umgekehrt darauf hinweisen, dass zu einer guten Compliance die Beachtung ihrer Rechte gehört. Dabei ist es wichtig, sich die notwendige Zeit zu nehmen und möglicherweise externe Berater zu holen, um alle Bereiche eines CMS umfassend zu diskutieren. Letztlich erscheinen die meisten Fragestellungen und Probleme im Zusammenhang mit einem CMS nur unter einer neuen Überschrift. Bei genauerer Betrachtung stellt sich schnell heraus, dass die meisten Themen für Betriebsräte „alte Bekannte“ sind (vgl. Kap. III).

Die Arbeitnehmervertreter sollten von Anfang an ihre Chance in der Einführung eines CMS suchen: So lassen sich über die reine Mitbestimmung hinaus Gestaltungsspielräume nutzen.

53 Klindt u. a. 2010.

54 Vgl. z. B. §§ 31 ff. WpHG. Die konkrete Ausgestaltung des Compliance-Systems ergibt sich dabei aus den Rundschreiben der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) MaRisk und MaComp sowie § 2 InstitutsVergV. Eine allgemeine Pflicht zur Einführung einer Compliance-Organisation kann sich, wenn überhaupt, nur aus § 130 OWiG ergeben (ist im Ergebnis jedoch abzulehnen).

Literatur

Becker, Wolfgang/Holzmann, Robert/Ulrich, Patrick: Non-Compliance in Organisationen – Wie lässt sich wirtschaftskriminelles Handeln vermeiden? In: Zeitschrift für Corporate Governance (ZCG), 6. Jg. (2011), Nr. 1, S. 5-12.
Bungart, Oliver/Strobl, Gregor: Lean Risk Management für den Mittelstand. In: Risk, Compliance & Audit, 2011, Heft 2, S. 41-45.

DGB Bundesvorstand (Hrsg.): Arbeitnehmerdatenschutz, 2009, Download unter www.dgb-bestellservice.de

Engelhart, Marc: Reform der Compliance-Regelungen der United States Sentencing Guidelines. In: Neue Zeitschrift für Gesellschaftsrecht (NZG), 2011 Heft 4, S. 126-129.

Fett, Torsten/Theusinger: Ingo, Compliance im Konzern – Rechtliche Grundlagen und praktische Umsetzung. In: Betriebsberater-Spezial, 2010, Heft 4, S. 11–14.

Feuchte, Beate: Positionspapier der Hans-Böckler-Stiftung zu CSR, 2009, Download unter www.boeckler.de

Fleischer, Holger in: Spindler, Gerald/Stilz, Eberhard: AktG, München, 2007, § 91.

Grummer, Jan-Menko/Seeburg, Julia: SOX und BilMoG Compliance. In: Behringer, Stefan (Hrsg.): Compliance kompakt, 2. Auflage, Berlin, 2011, S. 146-166.

Hauschka, Christoph (2010): Corporate Compliance, 2. Auflage, München, 2010, § 1 Rn. 23.

Hexel, Dietmar/Pütz, Lasse: Compliance aus gewerkschaftlicher Sicht. In: Audit Committee Quarterly II/2012, S. 40 – 43, Download unter www.audit-commitee-institute.de/docs(aci_quarterly_2012_2.pdf#page=40

Hüffer, Uwe: AktG, 9. Auflage, München, 2010.

Kappel, Jan/Ehling, Jan: Wie viel Strafe ist genug? – Deutsche Unternehmen zwischen UK Bribery Act, FCPA und StGB. In: Betriebsberater , 2011, Heft35, S. 2115-2121.

Klindt, Thomas/Pelz, Christian/Theusinger, Ingo: Compliance im Spiegel der Rechtsprechung. In: Neue Juristische Wochenschrift (NJW), 2010, S. 2385-2391.

Kort, Michael: Verhaltensstandardisierung durch Corporate Compliance. In: Neue Zeitschrift für Gesellschaftsrecht (NZG), 2008, S. 81-86.

Modlinger, Florian/Richter, Wolf-Dietrich: Der UK Bribery Act 2010. In: Zeitschrift für Risk, Fraud & Compliance (ZRFC), 2011, Heft 1, S. 16-21

Müller, Matthias: Praktische Hinweise zum sog. Risikomanagement, Hans-Böckler-Stiftung (Hrsg.), Arbeitshilfe für Aufsichtsräte Nr. 13, Düsseldorf, 2009 Download unter www.boeckler.de

Pütz, Lasse: Compliance – Eine Einführung in die Thematik, Hans-Böckler-Stiftung (Hrsg.), Arbeitshilfe für Aufsichtsräte Nr. 15, Düsseldorf, 2011, Download unter www.boeckler.de

Rohde-Liebenau, Björn: Whistleblowing, edition der Hans-Böckler-Stiftung, Düsseldorf, 2005.

Ringleb, Henrik-Michael (2010): in: Ringleb/Kremer/Lutter/v. Werder, Deutscher Corporate Governance Kodex, 4. Auflage, München 2010.

Schneider, Uwe H.: Compliance als Aufgabe der Unternehmensleitung. In: Zeitschrift für Wirtschaftsrecht (ZIP), 2003, S. 645-650.

Schulz, Mike: Compliance – Internes Whistleblowing. In: Betriebsberater, 2011, Heft 10, S. 629-634.

Vetter, Eberhard: Compliance in der Unternehmenspraxis. In: Wecker, Gregor/van Laak, Hendrik: Compliance in der Unternehmerpraxis, 2. Auflage, Wiesbaden, 2009, S. 29-42.

Wermelt, Andreas/Görtz, Birthe: Wie viel Compliance braucht der Mittelstand? In: Zeitschrift für Risk, Fraud & Compliance (ZRFC), 2011, Heft 1, S. 22-26.

Zöllner, Wolfgang/Noack, Ulrich (2010): In: Baumbach, Adolf/Hueck, Alfred: GmbHG, Kommentar, 19. Auflage, München 2010.

Internethinweise

Transparency International, eine weltweit agierende nichtstaatliche Organisation, die sich in der nationalen und internationalen Korruptionsbekämpfung engagiert: http://www.transparency.de/

Global Compact: www.globalcompact.de

Rechtliche Grundlagen des Global Compact im deutschen Recht: http://www.globalcompact.de/fileadmin/PDFs/GC/Rechtliche_Grundlagen_Global_Compact_Prinzipien.pdf

II Die Aufgabe des Aufsichtsrats im Compliance-Management-System

von Lasse Pütz und Sebastian Sick

1 Einleitung: Compliance und Corporate Governance

Risiken, die einem Unternehmen aufgrund von Compliance-Verstößen drohen, wurden in Kap. I bereits beschrieben. Je nach Schwere des Verstoßes kann dieser sich existenzbedrohend auswirken. Daher ist es wichtig, dass sich nicht nur die Geschäftsleitung mit diesem Thema befasst, sondern auch der Aufsichtsrat.[55] Dieser ist verpflichtet zu überwachen, ob die Geschäftsleitung ein angemessenes System eingerichtet hat, das Rechts- und Regelverstöße im Unternehmen verhindert oder zumindest erschwert.

Nach Ziffer 4.1.3 des Deutschen Corporate Governance Kodex (DCGK) wird die Kompetenz zur Einrichtung eines CMS der Geschäftsführung zugewiesen: „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)." Daneben empfiehlt der Kodex in Ziffer 3.4 Abs. 2 S. 1, dass der Vorstand den Aufsichtsrat regelmäßig, zeitnah und umfassend über alle für das Unternehmen relevanten Fragen der Planung, der Geschäftsentwicklung, der Risikolage, des Risikomanagements und der Compliance informiert. Nach Ziffer 5.3.2 DCGK soll der Aufsichtsrat darüber hinaus einen Prüfungsausschuss (Audit Committee) einrichten, „der sich insbesondere mit Fragen der Rechnungslegung, des Risikomanagements und der Compliance […] befasst".

Wie der DCGK bekräftigt, ist es zunächst die Aufgabe der Geschäftsleitung, dafür zu sorgen, dass ein CMS implementiert und durchgeführt wird. Sie entscheidet darüber, ob überhaupt ein CMS eingeführt und wie es ausgestaltet wird. Die Aufgabe des Aufsichtsrats beschränkt sich nach § 111 Abs. 1 AktG auf die Überwachung der Geschäftsleitung.

55 Ausführlich vgl. Pütz 2011.

2 Kontrollpflichten hinsichtlich Compliance

Nach § 111 Abs. 1 AktG obliegt es dem Aufsichtsrat, den Vorstand bzw. die Geschäftsführung zu überwachen und zu beraten.[56] Er überwacht dabei insbesondere, dass die Geschäftsführung ihre unternehmerische Leitungsfunktion wahrnimmt. Im Rahmen seiner Kontrollaufgabe stellt der Aufsichtsrat fest, a) ob sich die Unternehmensleitung rechtmäßig verhalten hat, b) ob sie ihren Pflichten nachgekommen ist und c) ob die von ihr getroffenen Entscheidungen im Unternehmensinteresse lagen. Zu den Pflichten der Geschäftsführung bzw. des Vorstandes kann auch die Einrichtung und Überwachung eines CMS gehören. Daher obliegt es dem Aufsichtsrat zu kontrollieren, ob die Geschäftsleitung dieser Verpflichtung nachkommt. Die Kontrolle beschränkt sich dabei jedoch regelmäßig auf eine System-Kontrolle: Der Aufsichtsrat prüft, a) ob die getroffenen Vorkehrungen risikoangemessen und ausreichend sind, b) ob ein umfassenderes Compliance-Management-System erforderlich ist und – wenn ja –, c) ob ein solches eingerichtet wurde und funktionsfähig ist. Die genaue Ausgestaltung des Systems obliegt jedoch allein dem Vorstand. Allerdings könnte der Aufsichtsrat auch diesbezüglich Zustimmungsvorbehalte zu seinen Gunsten festlegen.

2.1 Ausgestaltung der Überwachungsfunktion des Aufsichtsrats

Wie gezeigt wurde, obliegt dem Aufsichtsrat jedoch „nur“ die Überwachung der Geschäftsleitung dahingehend, dass die Geschäfte rechtmäßig, ordnungsgemäß, wirtschaftlich und zweckmäßig geführt werden.[57] Bei der Leitung des Unternehmens verfügt die Geschäftsleitung über einen Ermessenspielraum, den der Aufsichtsrat grundsätzlich respektieren muss.[58] In diesem Rahmen entscheidet der Aufsichtsrat bei seiner Kontrolltätigkeit, wie er seiner Überwachungspflicht nachkommt. Denkbar ist dies z. B. mittels Berichterstattung durch die Geschäftsleitung, mittels Verankerung von Zustimmungsvorbehalten oder durch zusätzliche Unterstützung externer Dienstleister.[59] So ist es etwa möglich, die Prüfung des CMS mit in den Prüfauftrag des Abschlussprüfers einzubeziehen. Die Berichterstattung kann dabei gegenüber dem gesamten Aufsichtsrat oder ggf. gegenüber dem Prüfungsausschuss (§ 107 Abs. 3 S. 2 AktG) erfolgen. Das Recht, einzelne

56 Für die GmbH folgt dies aus § 111 Abs. 1 AktG i. V. m § 25 Abs. 1 Nr. 2 MitbestG bzw. § 1 Abs. 1 Nr. 3 DrittelbG.

57 Fissenewert/Lehr 2011, S. 354; Köstler u. a. 2009, S. 317 ff.

58 Vgl. Winter 2010, S. 1109; Fissenewert/Lehr 2011, S. 355.

59 Vgl. Grüninger 2010, S. 140.

Beschäftigte direkt zu befragen hat der Aufsichtsrat hingegen grundsätzlich nicht. Daher kommt gerade hier den Arbeitnehmervertretern im Aufsichtsrat eine besondere Rolle zu. Sie verfügen oftmals über wichtige Kenntnisse aus dem Unternehmen, die bei einer System-Kontrolle hilfreich sein können.

Der Aufsichtsrat hat zudem die Pflicht, zukünftige Fehlentwicklungen präventiv zu verhindern. Laut Ziffer 5.1.1 DCGK ist es „Aufgabe des Aufsichtsrates […], den Vorstand bei der Leitung des Unternehmens regelmäßig zu beraten und zu überwachen. Er ist in Entscheidungen von grundlegender Bedeutung für das Unternehmen einzubinden." Diese präventive Überwachung erfolgt hauptsächlich durch die Beratung des Vorstandes in zentralen Fragen sowie durch Zustimmungsvorbehalte bei wichtigen Geschäften (§ 111 Abs. 4 AktG).[60] Die Zustimmungsvorbehalte sollten dabei in der Geschäftsordnung des Aufsichtsrates, des Vorstandes oder der Geschäftsführung geregelt werden. Zustimmungsvorbehalte, die bereits in der Satzung enthalten sind, schließen nicht aus, dass der Aufsichtsrat weitere festlegt. Bei der Beratung der Geschäftsleitung sollten sich die Aufsichtsratsmitglieder und insbesondere die Arbeitnehmervertreter bewusst sein, dass sie oft über wichtige Kenntnisse verfügen, z. B. über Risiken oder Geschäftspraktiken des Unternehmens. Sie können es der Geschäftsleitung erleichtern, ein CMS einzurichten. Ein weiteres Kontrollinstrumentarium bildet die Berichtspflicht des Vorstandes nach § 90 AktG.

Der Aufsichtsrat sollte regelmäßig überprüfen, ob die Vorgaben an den Vorstand umgesetzt sowie die Geschäftsordnungen eingehalten werden. So kann er sicherstellen, dass der Berichtspflicht und den Vorgaben von zustimmungspflichtigen Geschäften nachgekommen wird. Zu den Grundsätzen ordnungsgemäßer Aufsichtsratstätigkeit gehört, dass der Aufsichtsrat darauf hinwirkt, dass ihn der Vorstand bzw. die Geschäftsführung „regelmäßig, zeitnah und umfassend über alle relevanten Fragen der Strategie, der Planung, der Geschäftsentwicklung, der Risikolage und des Risikomanagements und der Compliance" informiert.[61] Er sollte daher bei der Einführung eines CMS darauf dringen, regelmäßig über die Entwicklung des Systems sowie der Compliance im Unternehmen informiert zu werden.

Die Kontrollpflicht des Aufsichtsrats erstreckt sich grundsätzlich nur auf den Vorstand bzw. die Geschäftsführung der Konzernmutter. Daher besteht keine direkte Überwachung der Unternehmensleitung der Tochtergesellschaften. Jedoch

60 Einen Überblick über die Rechte des Aufsichtsrats (in mitbestimmten Unternehmen) geben: Köstler 2009a und Köstler 2009b, Überblick über zustimmungspflichtige Geschäfte vgl. Sick/Köstler 2009, S. 33 ff.

61 Hans-Böckler-Stiftung 2011, S.12, These 22.

erfolgt durch die Überwachung der konzernweiten Führungsverantwortung des Konzernvorstandes (Konzernleitungspflicht) eine indirekte Kontrolle der Vorstände der Tochter- und Enkelgesellschaften (Konzernaufsicht). Der Konzern-Aufsichtsrat prüft daher das konzernweite CMS.

Zuletzt muss sich der Aufsichtsrat die relevanten Fragen hinsichtlich Compliance selbst stellen und für „Compliance im Aufsichtsrat" sorgen.[62] Es ist daher falsch, wenn er sich allein auf die Prüfung der Geschäftsleitung zurückzieht. Dies gilt insbesondere, da die Verantwortung der Mitglieder des Aufsichtsrats in den letzten Jahren gestiegen ist. Der Aufsichtsrat sollte sich vielmehr selbst Compliance-Regeln auferlegen, indem er eine angemessene Geschäftsordnung inklusive Informationsordnung und Katalog zustimmungsbedürftiger Angelegenheiten erarbeitet.[63] Ein wichtiger Bestandteil dieser Bestimmungen kann eine regelmäßige Selbstevaluation (Effizienzprüfung) sein, wie sie der DCGK in Ziffer 5.6 für börsennotierte Unternehmen empfiehlt.[64] Daneben trägt auch die Kontrollwirkung durch Mitbestimmung der Arbeitnehmervertreter im Aufsichtsrat sowie durch regelmäßige Schulung der Aufsichtsratsmitglieder in Compliance-relevanten Themen zur internen Aufsichtsrats-Compliance bei.

2.2 Der Prüfungsausschuss

Der DCGK empfiehlt in Ziffer 5.3.2, die Überwachung von Compliance-Fragen in den Prüfungsausschuss zu delegieren. Die Möglichkeit, einen solchen Ausschuss zu gründen, sieht § 107 Abs. 3 AktG ausdrücklich vor.[65] In der Praxis bereiten Aufsichtsratsausschüsse überwiegend Aufsichtsratsbeschlüsse vor. Insbesondere wenn die Aufsichtsräte sehr groß sind, können in den Ausschüssen schwierige Fragen intensiver beraten werden. Jedoch kann die Funktion des Gesamtaufsichtsrats schwinden, wenn zunehmend Entscheidungsbefugnisse auf Ausschüsse übertragen werden. Insoweit ist Vorsicht geboten: Die Übertragung von Funktionen darf das Plenum nicht entwerten.[66]

Ob ein Prüfungsausschuss gegründet wird und ob sich dieser mit dem Thema Compliance befasst, sollte daher im Einzelfall entschieden werden. Verschiedene Faktoren spielen hierfür zentrale Rollen: der Umfang des CMS und eventuell

62 Vgl. Hüffer 2010, § 76 Rn. 9a.
63 Für Anregungen hierzu vgl. Hans-Böckler-Stiftung 2011a.
64 Zur Effizienzprüfung mit ausführlichem Leitfaden siehe Sick 2011c.
65 Ausführlich zu Aufsichtsratsausschüssen vgl. Köster u. a. 2009, Rn. 394 ff.; Sick/Köstler 2009, S. 25 ff.
66 Köstler u. a. 2009, Rn. 394.

aufzuarbeitende Verstöße, die Besetzung des Aufsichtsrats und dessen Größe, die Branche, Internationalität und Börsennotierung sowie die Größe des Unternehmens. Wurde ein (Prüfungs-)Ausschuss eingerichtet, der sich mit Compliance befasst, muss dieser nach § 107 Abs. 3 S. 4 AktG regelmäßig dem gesamten Aufsichtsrat über seine Arbeit Bericht erstatten. Der Aufsichtsrat wiederum muss sich – da er die Überwachung des CMS delegiert – regelmäßig vergewissern, ob der Ausschuss seiner übertragenen Aufgabe gerecht wird.[67]

3 Verhältnis von Aufsichtsrat zu Betriebsrat

In vielen Fällen legt die Geschäftsleitung dem Aufsichtsrat das gesamte CMS oder Bestandteile dessen, z. B. einen Verhaltenskodex, vor. Dies kann sinnvoll sein, um zu zeigen, dass die Regelungen „von ganz oben" getragen werden. Die Arbeitnehmervertreter im Aufsichtsrat sollten jedoch stets berücksichtigen, dass die von ihnen beschlossenen Maßnahmen oder Regelungen Mitbestimmungsrechte des Betriebsrats betreffen können (z. B. § 87 BetrVG). Nur wenn zuvor eine Klärung mit den Betriebsräten herbeigeführt wurde, sollten die Arbeitnehmervertreter im Aufsichtsrat zustimmen. Ein unkoordiniertes Verhalten führt im schlimmsten Fall dazu, dass eine präjudizierende Wirkung eintritt und die Verhandlungen der Betriebsräte bei notwendigen Betriebsvereinbarungen erschwert werden. Der Aufsichtsrat kontrolliert insofern die Angemessenheit des CMS und der zentralen Vorgänge. Die Betriebsräte sind dagegen unmittelbar von den konkreten Compliance-Maßnahmen betroffen, die im Rahmen dieses Systems getroffen werden.

4 Haftung von Aufsichtsratsmitgliedern im Rahmen von Compliance

Nicht jede Pflichtverletzung des Aufsichtsrats führt dazu, dass das Aufsichtsratsmitglied haften muss. Dazu bedarf es weiterer Voraussetzungen, insbesondere eines Schadens, der auf diese Pflichtverletzung kausal zurückgeführt werden kann. Da die Pflichterfüllung im persönlichen Verhalten des Einzelnen begründet ist, stellt sie die wichtigste Stellschraube dar, um Haftung zu vermeiden.

Existiert kein förmliches CMS, muss das per se noch keine Pflichtverletzung darstellen. Entscheidend ist, dass risikoangemessene Vorkehrungen gegen Regelverstöße bestehen. Für Aktiengesellschaften ist lediglich die Einrichtung eines

67 Fissenewert/Lehr 2011, S. 356f.

Risikofrüherkennungssystems (§ 91 Abs. 2 AktG) und für Wertpapierdienstleistungsunternehmen die Einrichtung einer Compliance-Funktion vorgeschrieben (§ 33 Abs. 1 Nr. 1 WpHG). Gleichwohl können jedoch Mängel der Compliance und des CMS, die bei einer sorgfältigen Systemkontrolle hätten erkannt werden können, eine Haftung des Aufsichtsrats für im System angelegte Compliance-Verstöße begründen. Der Aufsichtsrat muss ein CMS nicht nur überprüfen, sondern er muss auch auf erkannte Mängel und Schwächen des CMS hinweisen. Falls notwendig, sollte dies durch einen formellen Empfehlungsbeschluss erfolgen. Zur genaueren Überwachung kann der Aufsichtsrat besondere Berichtspflichten oder Zustimmungsvorbehalte vorsehen. Das einzelne Aufsichtsratsmitglied kann von seinem individuellen Fragerecht gebrauch machen. Letztlich dürfen dem Aufsichtsrat jedoch keine überzogenen Aufsichtspflichten überantwortet werden. Solange keine anderslautenden Anhaltspunkte bestehen, darf er grundsätzlich auf die Vollständigkeit und Richtigkeit der Berichte der Geschäftsleitung vertrauen.[68]

Um eine Haftung zu vermeiden, muss der Aufsichtsrat bei der Überwachung eines CMS seine entsprechende Kontrollpflicht sorgfältig wahrnehmen. Insofern besteht hier keinerlei Unterschied zu sonstigen Aufsichtsratsthemen. Stets liegt die Beweislast, dass das Aufsichtsratsmitglied sorgfältig gearbeitet hat, bei diesem selbst. Daher sollten alle Schritte gründlich im Protokoll dokumentiert werden.

Aufsichtsrat und Geschäftsleitung haben einen breiten Beurteilungsspielraum bei unternehmerischen Entscheidungen und somit auch bei der Ausgestaltung eines CMS. Daher ist es keine Pflichtverletzung, wenn Aufsichtsratsmitglieder bei einer Entscheidung diesbezüglich annehmen durften, auf der Grundlage angemessener Information zum Wohle der Gesellschaft zu handeln.[69] (Business Judgement Rule). Nicht jede Fehleinschätzung und nicht jede Verwirklichung eines unternehmerischen Risikos führt zur Haftung.

Die absolute Grenze allerdings bilden Gesetzes- und Satzungsverstöße.[70] Der Aufsichtsrat ist verpflichtet einzuschreiten, wenn sich rechtswidrige Maßnahmen der Geschäftsleitung abzeichnen. Er muss einen Bericht fordern und einschreiten, sobald sich Zweifel an der Recht- und Zweckmäßigkeit der Geschäftsführung ergeben: z. B. beim Verdacht auf Unregelmäßigkeiten im Unternehmen oder betrügerischem Verhalten der Geschäftsführung.[71] Dies gilt insbesondere, wenn der Compliance Officer sich mit der Vermutung, ein Mitglied der Geschäftsführung

68 Vgl. Fissenewert/Lehr, 2011, S. 357f..

69 § 116 i. V. m. § 93 AktG (gelten über Verweisungen auch für die mitbestimmte und drittelbeteiligte GmbH).

70 OLG Düsseldorf Beschluss v. 9.12.2009 – I-6 W 45/09 (IKB) = AG 2010, 126, 128.

71 OLG Düsseldorf Urteil v. 23.6.2008 – I-9 U 22/08 = AG 2008, 666.

habe gegen Compliance verstoßen, an den Aufsichtsrat wendet. Erhält ein einzelnes Aufsichtsratsmitglied Sonderwissen über Missstände im Unternehmen, kann es sich bereits haftbar machen, wenn es dies dem Gesamtgremium vorenthält. Es gilt gründlich abzuwägen, wann ein Vorgang eine Bedeutung erlangt, die für den Aufsichtsrat relevant ist. Für eventuelle Nachweiszwecke kann es dabei sinnvoll sein, den Ablauf und Zeitpunkt der Kenntniserlangung in den persönlichen Aufzeichnungen zu dokumentieren.

Auch wenn bereits eine Pflichtverletzung seitens der Geschäftsleitung stattgefunden hat, muss der Aufsichtsrat einschreiten: Er ist verpflichtet, bei Erfolgsaussicht gegen den Vorstand vorzugehen und Schadensersatz zu fordern, sofern nicht Belange zum Wohl des Unternehmens entgegenstehen. Unterlässt er dies, haftet er selbst.[72]

Hinsichtlich der Haftung von Aufsichtsratsmitgliedern aufgrund von Compliance-Verstößen von Beschäftigten ist zunächst festzuhalten: Weder den Aufsichtsrat noch seine Mitglieder trifft eine unmittelbare Verantwortlichkeit für ein Compliance-konformes Verhalten seitens der Beschäftigten. Dies sicherzustellen ist zunächst Aufgabe der Geschäftsleitung. Der Aufsichtsrat haftet nicht unmittelbar für individuelle Regelverstöße einzelner Beschäftigter oder der Geschäftsführung, sofern er seine generelle Überwachungspflicht erfüllt.

Zur Haftungsvermeidung im Rahmen von Compliance gehört auch, dass der Aufsichtsrat selbst die für ihn geltenden Regeln einhält. Eine Möglichkeit, dies zu überprüfen, besteht in der erwähnten Effizienzprüfung (Selbstevaluation) des Aufsichtsrats. Bei börsennotierten Unternehmen gehört dazu auch die ordnungs- und wahrheitsgemäße Abgabe einer Entsprechenserklärung zum DCGK.[73]

72 ARAG/Garmenbeck-Entscheidung, BGH Urteil v. 21.04.1997 – II ZR 175/95 = ZIP 1997, 883 = DB 1997, 1088.

73 Vgl. § 161 AktG; dazu z. B. BGH Urteil v. 16.2.2009 – II ZR 185/07 = DB 2009, 500.

5 Fazit: Wichtige Rolle der Arbeitnehmervertreter

Bereits bevor der Begriff Compliance im deutschen Sprach- und Rechtskreis bekannt war, gehörte es zu den grundlegenden Interessen der Geschäftsleitung und des Aufsichtsrates, Schaden vom Unternehmen abzuwenden. Die neuerdings aufkommenden CMS vermögen dies zu unterstützen. Letztlich kann ein angemessenes CMS dazu beitragen, sowohl die Geschäftsleitung als auch den Aufsichtsrat vor übermäßigen Haftungsrisiken zu bewahren.

Darüber hinaus ist es wichtig, bei der Implementierung und Durchführung eines CMS die Rolle der Arbeitnehmer und ihrer Vertreter im Betriebs- sowie Aufsichtsrat angemessen zu berücksichtigen. Sie sollten bei der Einrichtung eines CMS eine aktive Rolle übernehmen und ihre Erfahrungen und Kompetenzen einbringen. Ein gutes CMS ist auch immer ein Schritt zu mehr Transparenz und Beteiligung.

Für die effektive Aufsichtsratsarbeit ist gerade beim Thema Compliance die Vernetzung der Arbeitnehmervertreter im Konzern auf allen Ebenen wichtig. Die unterschiedlichen Elemente der Mitbestimmung im Aufsichtsrat und im Betrieb sollten hier ergänzend ineinander greifen. Während der Aufsichtsrat die Zweckmäßigkeit des CMS als Ganzes kontrolliert, gilt es auf betrieblicher Ebene, sich bei der Einführung einzelner Compliance-Maßnahmen einzuschalten. Dass dazu Gelegenheit besteht, muss auch im Aufsichtsrat eingefordert werden. Die interne Kenntnis des Unternehmens gibt Arbeitnehmervertretern einen Wissensvorsprung gegenüber Anteilseignervertretern. Das sollten sie im Aufsichtsrat einbringen und nutzen.

Literatur

Fissenewert, Peter/Lehr, Susanne: Die Rolle des Aufsichtsrats im Compliance Management. In: Behringer (Hrsg.): Compliance kompakt, 2. Auflage, Berlin, 2011.

Grüninger, Stephan: Compliance-Prüfung nach dem IDW EPS 980. In: Der Aufsichtsrat, 2010, Heft 10, S. 141–142.

Köstler, Roland: Übersicht über Aufsichtsratsrechte im Bereich Mitbestimmungsgesetz ´76, Hans-Böckler-Stiftung (Hrsg.), Arbeitshilfe für Aufsichtsräte Nr. 2, Düsseldorf, 2009a, Download unter www.boeckler.de.

Köstler, Roland: Übersicht über Aufsichtsratsrechte im Bereich Drittelbeteiligungsgesetz 2004, Hans-Böckler-Stiftung (Hrsg.), Arbeitshilfe für Aufsichtsräte Nr. 3, Düsseldorf, 2009b, Download unter www.boeckler.de.

Hans-Böckler-Stiftung (Hrsg.): Grundsätze ordnungsmäßiger Aufsichtsratstätigkeit, Arbeitshilfe für Aufsichtsräte Nr. 10, Düsseldorf, 2011, Download unter www.boeckler.de.

Pütz, Lasse: Compliance – Eine Einführung in die Thematik, Hans-Böckler-Stiftung (Hrsg.):Arbeitshilfe für Aufsichtsräte Nr. 15, Düsseldorf, 2011, Download unter www.boeckler.de.

Sick, Sebastian: Die Effizienzprüfung des Aufsichtsrats, Hans-Böckler-Stiftung (Hrsg.), Arbeitshilfe für Aufsichtsräte Nr. 16, Düsseldorf, 2011, Download unter www.boeckler.de.

Sick, Sebastian/Köstler, Roland: Die Geschäftsordnung des Aufsichtsrats. Hans-Böckler-Stiftung (Hrsg.), Arbeitshilfe für Aufsichtsräte Nr. 1, Düsseldorf, 2009 , Download unter www.boeckler.de.

Hüffer, Uwe: AktG, 9. Auflage, München, 2010.

Köstler, Roland/Zachert, Ulrich/Müller, Matthias: Aufsichtsratspraxis, 9. Auflage, Frankfurt am Main, 2009.

Winter, Martin: Die Verantwortlichkeit des Aufsichtsrats für Corporate Compliance. In: Kindler, Peter u. a. (Hrsg.): Festschrift für Uwe Hüffer, München, 2010, S. 1103-1128.

III Compliance – Was ein Betriebsrat wissen sollte

von Andreas Priebe

1 Einleitung

Compliance ist für viele Betriebsräte ein Buch mit sieben Siegeln. „Compliance hat doch was mit Wertpapier- und Aktienhandel zu tun. Das ist was für Vorstände, betrifft aber nicht unsere Arbeit", hört man gelegentlich von den betrieblichen Praktikern in den Betriebsräten. Das stimmt – und stimmt auch wieder nicht, denn Compliance ist viel mehr als der Versuch, durch organisatorische Maßnahmen in den Betrieben Korruption zu verhindern. Compliance ist eigentlich nichts wirklich Neues: Schon immer waren sowohl Arbeitgeber als auch Betriebsrat und Arbeitnehmer in den Unternehmen verpflichtet, gesetzliche Vorschriften einzuhalten. Und auch bisher schon mussten Arbeitgeber geeignete Maßnahmen ergreifen, um Verstöße zu verhindern.

Für die Betriebsratsarbeit ist Compliance somit eigentlich ein bekanntes Themenfeld. Gemäß § 80 Abs. 1 Nr. 1 BetrVG ist der Betriebsrat beispielsweise verpflichtet darüber zu wachen, „dass die zugunsten der Arbeitnehmer geltenden Gesetze, Verordnungen, Unfallverhütungsvorschriften, Tarifverträge und Betriebsvereinbarungen eingehalten werden."

Daher keine Panik, wenn der Arbeitgeber plötzlich Compliance-Regeln – hier als Oberbegriff für Verhaltenskodizes oder Ethikrichtlinien verwendet – im Betrieb einführen will: Die Themen sind den Betriebsräten meistens wohlbekannt. Neu sind ggf. die Mechanismen, die gewährleisten sollen, dass die Einhaltung der Regeln kontrolliert werden kann. Diesbezüglich verfügt der Betriebsrat oft über ein Mitbestimmungsrecht.

2 Einführung von Compliance-Regeln

Der Arbeitgeber kann Compliance-Regeln grundsätzlich auf verschiedene Art und Weise einführen. Zum einem kann er sein arbeitgeberseitiges Direktionsrecht nutzen, um Arbeitnehmer dazu zu veranlassen, Regeln sowie Ge- und Verbote einzuhalten. Zum anderen ist dies möglich mittels entsprechend verpflichtenden

Klauseln im Arbeitsvertrag bzw. durch Individualvereinbarung. Besteht im Betrieb ein Betriebsrat, kommt der Abschluss einer entsprechenden Betriebsvereinbarung in Betracht, denn viele Compliance-Regeln unterliegen den Mitbestimmungsrechten z. B. aus § 87 Abs. 1 BetrVG.

Inwieweit sich Beschäftigte an die vom Arbeitgeber durch Compliance-Regeln erlassenen Verhaltensgrundsätze halten müssen, hängt im Wesentlichen davon ab, ob der Arbeitgeber sie rechtsverbindlich für den Arbeitnehmer eingeführt hat. Je nach Intensität des Regelungsinhaltes variieren die Voraussetzungen. Betriebsräte sollten stets streng prüfen, ob nicht der Abschluss einer Betriebsvereinbarung die Vorraussetzung für die rechtsverbindliche Einführung ist.

2.1 Direktionsrecht

Das arbeitgeberseitige Direktionsrecht hat seine Rechtsgrundlage in § 106 GewO: „Der Arbeitgeber kann Inhalt, Ort und Zeit der Arbeitsleistung nach billigem Ermessen näher bestimmen, soweit diese Arbeitsbedingungen nicht durch Arbeitsvertrag, Bestimmungen einer Betriebsvereinbarung, eines anwendbaren Tarifvertrages oder gesetzliche Vorschriften festgelegt sind. Dies gilt auch hinsichtlich der Ordnung und des Verhaltens der Arbeitnehmer im Betrieb. Bei der Ausübung des Ermessens hat der Arbeitgeber auch auf Behinderungen des Arbeitnehmers Rücksicht zu nehmen.“

Das arbeitgeberseitige Direktionsrecht ist für den Arbeitgeber attraktiv, da er sich aufgrund dessen nicht mit dem Betriebsrat beraten und einigen muss. Jedoch ist das Direktionsrecht eng begrenzt: Es kann nur dort angewendet werden, wo bestehende vertragliche oder gesetzliche Haupt- bzw. Nebenpflichten konkretisiert werden sollen. Es kann jedoch keine neuen Verhaltenspflichten begründen. Somit ist zumindest in der Praxis die Grenze des Direktionsrechts schnell erreicht.

2.2 Arbeitsvertrag und Individualvereinbarung

Will der Arbeitgeber die engen Grenzen des Direktionsrechts überschreiten, kann er grundsätzlich Verhaltensvorgaben durch Regelungen im Arbeitsvertrag bestimmen bzw. durch eine Ergänzung des Arbeitsvertrages oder durch eine separate Individualvereinbarung mit den Arbeitnehmern nachträglich einführen. Jedoch müssen solche Vereinbarungen gesetzeskonform sein und dürfen den Arbeitnehmer nicht unangemessen benachteiligen. Außerdem wird es in der Praxis an Grenzen stoßen, komplexe Verhaltensregelungen per Arbeitsvertrag bzw. Individualvereinbarung ins Arbeitsverhältnis einzuführen, von Zeit zu Zeit zu modifi-

zieren und veränderten Bedingungen anzupassen. Denn: Stimmt ein Arbeitnehmer veränderten Verhaltensvorschriften nicht zu, etwa wenn sie zu stark in sein Privatleben eingreifen, bleibt dem Arbeitgeber nur der problematische Weg über Änderungskündigungen. Allerdings muss vor jeder Kündigung, auch vor Änderungskündigungen, gemäß § 102 Abs. 1 BetrVG der Betriebsrat angehört werden.

Darüber hinaus kann sich der betroffene Arbeitnehmer gemäß § 84 BetrVG selbst beschweren, wenn er sich vom Arbeitgeber ungerecht behandelt fühlt. Alternativ kann er sich mit seiner Beschwerde gemäß § 85 BetrVG an den Betriebsrat wenden, der – wenn er sie als berechtigt erachtet – beim Arbeitgeber auf Abhilfe dringt. Der Inhalt der Beschwerde könnte in beiden Fällen wie folgt lauten: Der Arbeitgeber fordert von einem Arbeitnehmer ein bestimmtes Verhalten, das er von anderen Beschäftigten nicht fordert, ohne dass diese Unterscheidung sachlich gerechtfertigt wäre.

Vor einer in letzter Konsequenz denkbaren Änderungskündigung steht schließlich noch das Kündigungsschutzgesetz (KSchG). Auch Änderungskündigungen sind gemäß § 2 KSchG arbeitsgerichtlich überprüfbar. Greift ein Arbeitgeber tatsächlich zu diesem Mittel, sollten die Betroffenen unverzüglich gewerkschaftliche oder anwaltliche Hilfe in Anspruch nehmen. Denn im Arbeitsgerichtsverfahren müssen zahlreiche Formalitäten beachtet werden.

Alles in allem sind Versuche des Arbeitgebers, über Arbeitsverträge und Individualvereinbarungen Compliance-Regeln einzuführen, oftmals schwierig und, wenn Beschäftigte und Betriebsrat sich einig sind, meist zum Scheitern verurteilt.

2.3 Betriebsvereinbarungen

Möchte der Arbeitgeber durch die Einführung von Compliance-Regeln das Verhalten der Arbeitnehmer im Betrieb und darüber hinaus umfassend regeln, bleibt ihm in der Praxis eigentlich nur der Weg, mit dem Betriebsrat entsprechende Betriebsvereinbarungen abzuschließen. Dieser Weg stellt aus Perspektive des Betriebsrats fast immer den Königsweg dar, um Compliance-Regeln einzuführen. Denn anders als bei der Einführung auf anderem Wege kann der Betriebsrat hier seine betriebsverfassungsrechtlichen Mitbestimmungsrechte voll geltend machen und notfalls über die Einigungsstelle oder im Arbeitsgerichtsverfahren durchsetzen bzw. den Arbeitgeber zu Zugeständnissen im Interesse der Arbeitnehmer bewegen (vgl. Kap. IV).

Der Arbeitgeber könnte bei der Gestaltung von Compliance-Regeln versuchen, mitbestimmungsfreie Regelungen per Direktionsrecht umzusetzen und nur zwingend mitbestimmungspflichtige Regelungen mit dem Betriebsrat zu verhandeln und in einer Betriebsvereinbarung zu regeln. Hier sollte der Betriebsrat auf dem Verhandlungsweg versuchen, ein Gesamtwerk mit dem Arbeitgeber auszuhandeln, das auch nicht mitbestimmungspflichtige Regelungsaspekte enthält und nur eine einheitliche Kündigung zulässt. Ein Verhandlungsargument gegenüber dem Arbeitgeber könnte lauten: Die Akzeptanz bei den Beschäftigten ist größer, wenn Arbeitgeber und Betriebsrat ein gemeinsames Regelwerk beschließen. Lässt sich der Arbeitgeber nicht darauf ein, muss der Betriebsrat erwägen, wie er die Verhandlungen über die mitbestimmungspflichtigen Regelungsaspekte führen möchte.

3 Mitbestimmungsrechte des BR bei der Einführung von Compliance-Regeln

Viele Compliance-Regeln unterliegen den Mitbestimmungsrechten des Betriebsrats, die sich aus § 87 Abs. 1 BetrVG ergeben. Beispielsweise sind Torkontrollen, die der Zugangskontrolle zum Betriebsgelände dienen, mitbestimmungspflichtig nach § 87 Abs. 1 Nr. 1 BetrVG (Fragen der Ordnung des Betriebs und des Verhaltens der Arbeitnehmer im Betrieb). Ob der Arbeitgeber diese Zugangskontrolle im Rahmen von Compliance-Regeln (Zugangskontrolle für Unbefugte z. B. zum Schutz sensibler Daten) oder aus anderen Gründen (Verhinderung von Diebstählen durch Beschäftigte) einführen möchte, ist für den Betriebsrat letztendlich zweitrangig. Wichtig ist es, dass er seine gesetzlichen Mitbestimmungsrechte wahrnimmt.

Gelegentlich tritt ein Arbeitgeber an den Betriebsrat mit der Forderung heran, Compliance-Regeln zuzustimmen, da diese von einer Muttergesellschaft oder von ausländischen Geschäftspartnern verlangt würden, die ausländischem Recht unterliegen. Hier habe der Betriebsrat keinen Handlungs- und Mitbestimmungsspielraum. Diese Auffassung ist falsch, da das BAG eindeutig festlegt:

„Die Mitbestimmungsrechte nach dem Betriebsverfassungsgesetz werden nicht dadurch ausgeschlossen oder eingeschränkt, dass ausländische Bestimmungen in Deutschland tätigen Unternehmen bestimmte Pflichten auferlegen. Ausländische Vorschriften sind jedenfalls dann keine die Mitbestimmung nach § 87 Abs. 1 Eingangshalbsatz BetrVG ausschließenden gesetzlichen Regelungen,

wenn es an einer wirksamen völkerrechtlichen Transformation in das deutsche Arbeitsrecht fehlt. Die Mitbestimmungsrechte der Arbeitnehmervertretungen in Betrieben, die in Deutschland liegen, richten sich auch dann nach dem deutschen Recht, wenn der Arbeitgeber seinen Sitz im Ausland hat".[74]

Bei jeder einzelnen vom Arbeitgeber gewünschten Compliance-Regel sollte der Betriebsrat also strickt darauf achten, ob diese den Mitbestimmungsrechten aus dem BetrVG, insbesondere aus § 87 Abs. 1 BetrVG, unterliegt.

4 Ausgewählte mitbestimmungsrelevante Compliance-Regeln

Dieses Kapitel bietet einen kurzen Überblick über Compliance-relevante Themen und Aspekte, die sich zudem als besonders praxisnah erweisen.

4.1 Betriebsverfassungsgesetz

Vor einiger Zeit sorgten arbeitgeberfinanzierte Luxusreisen von Betriebsratsmitgliedern ins ferne Brasilien für Schlagzeilen und beschädigten das Image der Beteiligten in der Öffentlichkeit. Dieses Beispiel zeigt deutlich, wie wichtig es ist, betriebsverfassungsrechtliche Regeln zu beachten. Von solchen extremen Einzelfällen abgesehen: In der täglichen Praxis der Betriebsratsarbeit kommt es immer wieder vor, dass Arbeitgeber ihrerseits die betriebsverfassungsrechtlichen Beteiligungsrechte des Betriebsrats missachten. Um die Betriebsratsrechte zu schützen, enthalten die §§ 119–121 BetrVG zahlreiche Straf- und Bußgeldtatbestände.[75] Beispielsweise können Arbeitgeber, die die Betriebsratstätigkeit behindern, mit Geld- oder Freiheitsstrafen bis zu einem Jahr bestraft werden. Weiterhin sind bekanntermaßen Kündigungen, die ohne Anhörung des Betriebsrats erfolgen, gemäß § 102 Abs. 1 BetrVG unwirksam. In diesem Kontext muss beachtet werden: Mitbestimmungspflichtige Maßnahmen, die vom Arbeitgeber ohne Zustimmung des Betriebsrates durchgeführt werden und die deshalb unwirksam sind, können nicht durch nachträgliche Zustimmung des Betriebsrats legalisiert werden.[76]

Betriebsrat und Arbeitgeber tun demnach gut daran, Vereinbarungen und Regelungsabläufe zu beschließen, die ein Vorgehen gewährleisten, das den Regelungen des BetrVG entspricht. Dies kann auch in Compliance-Regeln zum Ausdruck kommen: Darin kann der Arbeitgeber etwa leitende Angestellte verpflichten, die

74 BAG vom 22.07.2008 – 1 ABR 40/07 – Nr. 60.
75 Priebe 2009.
76 BAG vom 20.01.1998 – 9 AZR 698/96, DB 1998, 2530 (2531).

Rechte des Betriebsrats zu beachten und hierfür Verfahrensgrundsätze aufstellen: z. B. Ablaufpläne zur Beteiligung des Betriebsrats bei personellen Einzelmaßnahmen gemäß § 99 BetrVG.

4.2 Datenschutz und Telekommunikation

Die Bedeutung des Datenschutzes in den Betrieben hat in den letzten Jahren enorm zugenommen. Die tägliche E-Mail- und Internetnutzung gehört inzwischen an vielen Arbeitsplätzen zum Alltag. Auch in den Personalverwaltungen werden inzwischen nahezu ausschließlich personenbezogene Daten der Arbeitnehmer per EDV verwaltet und bearbeitet. Zahlreiche Skandale der letzten Jahre, in denen Arbeitgeber (Telekom, Lidl, Deutsche Bahn etc.) Daten ihrer Beschäftigten unbefugt und entgegen gesetzlichen Bestimmungen auswerteten, sind noch gut in Erinnerung. Sie haben die Diskussion um einen wirksamen Arbeitnehmerdatenschutz neu entfacht.

Auch dem internationalen Datentransfer kommt eine wachsende Bedeutung zu: Sind Unternehmen international tätig, sind Datentransfers über Ländergrenzen hinweg oftmals an der Tagesordnung. Hier muss sichergestellt werden, dass die übermittelten Daten im Ausland nach gewissen Mindeststandards geschützt sind – denn relativ umfassende gesetzliche Regelungen, wie das Bundesdatenschutzgesetz (BDSG) sie enthält, finden sich in ausländischen Rechtsordnungen selten. Gerade der Datentransfer in „unsichere Drittstaaten" außerhalb der EU erweist sich als problematisch – hierzu zählen auch die USA.[77]

Ein weiteres Regelungsfeld entsteht, wenn der Arbeitgeber den Beschäftigten gestattet, die betrieblichen Kommunikationseinrichtungen zu privaten Zwecken zu nutzen. Dann müssen neben den Regelungen des BDSG auch die Vorschriften des Telekommunikationsgesetzes (TKG) beachtet werden. Hierzu gilt es beispielsweise zu regeln, wie mit privaten E-Mails verfahren wird, die auf den PCs gespeichert sind: Wer darf im Vertretungsfall die eingehenden E-Mails des Mitarbeiters lesen? Wie wird die Vertretung geregelt? Wie lange werden Surfprotokolle in der EDV gespeichert? All das stellt ein Betätigungsfeld für den Betriebsrat dar.

Nachdem die Skandale um die Überwachung und Ausspionierung von Beschäftigten bei Telekom, Bahn, Lidl & Co. in den Fokus der Öffentlichkeit gerückt waren, sah sich der Gesetzgeber veranlasst, politisch aktiv zu werden. Denn die bestehenden Regelungen des BDSG reichen offensichtlich nicht aus, um Arbeitnehmerinnen und Arbeitnehmer wirksam zu schützen. § 32 (Datenerhebung,

77 Vgl. Wecker/van Laak 2008, S.226.

-verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses) regelt derzeit primär, was ein Arbeitgeber darf und was nicht.

Der DGB und weitere Datenschutzexperten favorisieren ein eigenständiges Beschäftigtendatenschutzgesetz. Dieses soll den speziellen Anforderungen der Arbeitswelt Rechnung tragen[78] und Beschäftigte wirksam schützen. Der Gesetzgeber entschied sich für einen anderen Weg: Mittels einer Ergänzung des bestehenden BDSG durch die §§ 32 bis 32l will er den Datenschutzbedürfnissen der Arbeitnehmer entsprechen. Die Kritik seitens der Gewerkschaften und der Datenschutzexperten am vorgelegten Gesetzesentwurf ist verheerend: „Der Entwurf zum Beschäftigtendatenschutzgesetz schützt nicht die Daten der Beschäftigten, sondern legalisiert die Überwachung von Arbeitnehmerinnen und Arbeitnehmern. Er erlaubt dem Arbeitgeber, Gesundheitsdaten im laufenden Beschäftigtenverhältnis zu ermitteln, Screenings auch ohne konkreten Tatverdacht durchzuführen und Videoüberwachung erheblich auszudehnen. Dieser Entwurf schützt ausschließlich die Interessen der Arbeitgeber an Überwachung und Bespitzelung von Beschäftigten am Arbeitsplatz“.[79]

Aktuell ist offen, ob die geplante Novellierung des BDSG in der laufenden Legislaturperiode noch verabschiedet wird. Bislang (Dezember 2012) hat der Bundestag den Gesetzentwurf zum Beschäftigtendatenschutzgesetz noch nicht abschließend behandelt.[80]

4.3 AGG und Diskriminierungsschutz

Der Arbeitgeber ist gemäß § 12 Gleichbehandlungsgesetz (AGG) verpflichtet, vorbeugende Maßnahmen zu ergreifen, um die Beschäftigten vor Diskriminierung zu schützen. Laut § 1 AGG ist es „Ziel des Gesetzes […], Benachteiligung aus Gründen der Rasse oder wegen der ethischen Herkunft, des Geschlechts, der Religion oder Weltanschauung, einer Behinderung, des Alters oder der sexuellen Identität zu verhindern oder zu beseitigen.“

In Compliance-Regeln kann der Arbeitgeber beispielsweise für die Personalabteilung Prozeduren festlegen, die eine diskriminierungsfreie Auswahl von Bewerberinnen und Bewerbern im Einstellungsverfahren sicherstellen. Trifft der Arbeitgeber keine vorbeugenden Maßnahmen gegen Diskriminierungen im Sinne des AGG, kann der Betriebsrat gemäß den §§ 23 Abs. 3 BetrVG, 17 Abs. 2 AGG beim Arbeitsgericht beantragen, den Arbeitgeber zu verpflichten, entsprechende

78 Vgl. den DGB-Entwurf zu einem Arbeitnehmerdatenschutzgesetz, www.dgb.de.

79 DGB-Vorsitzender Michael Sommer, in der Pressemitteilung des DGB 086 – 22.05.2011.

80 Weitere Details siehe z. B. im „Info Recht“ des DGB vom 13.10.2011 (www.dgb.de).

Maßnahmen zu ergreifen. Notfalls kann das Arbeitsgericht auch Ordnungs- und Zwangsgelder in Höhe von bis zu 10.000 € gegen den Arbeitgeber verhängen.

4.4 Ethik-Richtlinien

Wal-Mart sei „Dank" waren vor einigen Jahren Ethik-Richtlinien in aller Munde. Der US-amerikanische Einzelhandelskonzern untersagte in einem Verhaltenskodex seinen Mitarbeiterinnen und Mitarbeitern, miteinander privaten Umgang zu pflegen, zusammen auszugehen oder gar eine (Liebes-)Beziehung einzugehen, wenn zwischen den Beteiligten ein berufliches hierarchisches Abhängigkeits- bzw. Weisungsverhältnis bestand. Wenngleich uns solche Klauseln und Ethik-Richtlinien in Deutschland, Europa und auch darüber hinaus weitgehend fremd sind und puritanisch anmuten, hatten sich die Wal-Mart-Verantwortlichen durchaus etwas dabei gedacht: Man wollte sexuelle Belästigungen am Arbeitsplatz unterbinden und hohen Schadensersatzforderungen, die nach US-Recht oftmals geltend gemacht werden, einen Riegel vorschieben. Relativ schnell machten die deutschen Arbeitsgerichte klar: Derartige Ethik-Richtlinien verstoßen gegen verfassungsrechtliche Grundrechte der Beschäftigten (Allgemeines Persönlichkeitsrecht) aus Art. 2 Abs. 1 i. V. m. Art. 1 GG und sind daher unwirksam.

Dennoch stellt sich für Betriebsräte die Frage: Wie weit darf der Arbeitgeber bei der Gestaltung von Ethik-Richtlinien gehen? Regelungen, die das Verhalten der Beschäftigten und die betriebliche Ordnung regeln, sind nach § 87 Abs. 1 Nr. 1 BetrVG mitbestimmungspflichtig. Mitbestimmungsfrei sind Regelungen, die die arbeitsvertraglich geschuldete Arbeitsleistung konkretisieren oder Bereiche, für die gesetzliche Regelungen bestehen. Im Einzelfall wird es gelegentlich schwierig sein, zwischen beidem zu unterscheiden. Schon aus diesem Grund bietet es sich aus Betriebsratsperspektive an möglichst zu versuchen, mit dem Arbeitgeber ein umfassendes Regelungswerk zu vereinbaren, das den Persönlichkeitsrechten der Beschäftigten Rechnung trägt und der Verpflichtung aus § 75 Abs. 2 BetrVG nachkommt.

4.5 Whistleblowing-Regeln

Whistleblowing lässt sich in etwa mit „Alarm schlagen" übersetzen.[81] Bisher ist allgemein anerkannt, dass Beschäftigte verpflichtet sind, den Arbeitgeber über wesentliche Ereignisse im Betrieb zu unterrichten, insbesondere dann, wenn dem Arbeitgeber Schaden droht. Dabei handelt es sich um eine arbeitsvertragliche

81 Zum Thema Whistleblowing vgl. Kap. IV.

Nebenpflicht[82] bzw. Unterrichtungspflicht, die der Arbeitgeber grundsätzlich per Direktionsrecht konkretisieren kann. In diesem Zusammenhang stellen sich aus Sicht des Betriebsrats vor allem zwei Fragen: Wie weit reicht das Direktionsrecht des Arbeitgebers? Und: Wie lassen sich Denunzierungen im Betrieb verhindern?

Das arbeitgeberseitige Direktionsrecht kann keine neuen Pflichten für die Beschäftigten begründen, sondern nur vorhandene konkretisieren. Der Arbeitgeber kann also verlangen, dass Beschäftigte Verstöße gegen betriebliche Regeln melden – jedenfalls dann, wenn dem Arbeitgeber Schaden droht. Fraglich ist diese Meldepflicht dann, wenn auch geringfügige Verstöße, durch die dem Arbeitgeber keine größeren Schäden oder Nachteile drohen, von Arbeitskollegen gemeldet werden sollen. Eine generelle Pflicht, alle Verstöße – unabhängig von Schwere und Folgen – zu melden, ist nicht verhältnismäßig und kann nicht durch das Direktionsrecht eingeführt werden. Idealerweise werden diese Aspekte in einer Betriebsvereinbarung geregelt. Betriebsräte sollten dabei insbesondere darauf achten, dass Meldepflichten bezüglich kleinerer Verstöße von der Meldepflicht ausgenommen sind. Weiterhin müssen folgende Fragen geregelt werden: Sollen anonyme Meldungen möglich sein? Oder sind nur Anzeigen unter Nennung des eigenen Namens statthaft? Wie soll gemeldet werden (Whistleblowing-Hotline, interne oder externe Ansprechpartner etc.)? Wie ist das Prüfungsverfahren gestaltet? Wie wird festgestellt, ob ein Verstoß vorliegt (Stichwort: Unschuldsvermutung etc.)? Und: Wie kann verhindert werden, dass Whistleblowing nicht zur Denunzierung unliebsamer Kolleginnen und Kollegen missbraucht wird?

Wenngleich bisher keine empirischen Kenntnisse vorliegen, besteht sicherlich die Gefahr, dass die Möglichkeit des Whistleblowings hin und wieder missbraucht wird, um unliebsamen Kolleginnen und Kollegen zu schaden. Whistleblowing-Regeln sollten daher so gestaltet sein, dass sich das Denunziantentum gegenüber berechtigten Meldungen in Grenzen hält. Auf jeden Fall muss für einen Beschuldigten bzw. eine Beschuldigte stets die Unschuldsvermutung gelten, bis im Rahmen einer Untersuchung unter Hinzuziehung des Betriebsrats festgestellt wird, ob der erhobene Vorwurf berechtigt ist oder nicht. Ansonsten drohen neben ungerechtfertigten Verdächtigungen und persönlichen Folgen für die Betroffenen auch eine erhebliche Störung des Betriebsfriedens sowie eine Atmosphäre des Misstrauens zwischen den Beschäftigten.

Am 21.07.2011 hat der Europäische Gerichtshof für Menschenrechte (EGMR) die Bundesrepublik Deutschland gemäß Art. 10 EMRK wegen der Verletzung des

82 Vgl. Holzhauser/Sutter 2011, S. 77.

Menschenrechts auf Freiheit der Meinungsäußerung verurteilt.[83] Eine Mitarbeiterin in einer kommunalen Altenpflegeeinrichtung hatte zunächst über längere Zeit versucht, massive Missstände bei ihrem Arbeitgeber auf dem Beschwerdeweg abzustellen. Als sie damit keinen Erfolg hatte, erstattete sie schließlich Strafanzeige. Nachdem die Staatsanwaltschaft die Ermittlungen eingestellt hatte, kündigte der Arbeitgeber der Mitarbeiterin wegen der Verletzung ihrer Loyalitätspflichten. Zwar gab das Arbeitsgericht der Klägerin Recht, das Landesarbeitsgericht gab jedoch dem Arbeitgeber Recht und auch das Bundesarbeitsgericht wies den Fall zurück. Somit wurde die Kündigung rechtskräftig. Erst der EGMR gab der Arbeitnehmerin Recht und verurteilte die Bundesrepublik Deutschland zu Schadensersatz. Er stellte klar, dass eine angemessene Abwägung zwischen dem Schutz der Reputation des Unternehmens und dem Recht auf freie Meinungsäußerung gefunden werden müsse. So müssten Beschäftigte zumindest das Recht haben, die staatlichen Organe zu informieren, wenn Versuche scheiterten, Missstände abzustellen. Das sei auch durch Art. 10 der EMRK gedeckt. Im Ergebnis bleibt deshalb zu hoffen, dass deutsche Arbeitsgerichte zukünftig in vergleichbaren Fällen die EMRK beachten. So könnte es couragierten Beschäftigten mehr als bisher gelingen, in letzter Konsequenz auch Missstände wie Korruption und andere Straftaten bei ihren Arbeitgebern notfalls öffentlich zu machen, ohne dafür durch Kündigungen sanktioniert zu werden.

5 Fazit

Dieser Beitrag bietet einen Überblick über das Themenfeld Compliance und Betriebsrat. Festzuhalten bleibt: In der Praxis geht es darum, dass die Betriebsräte ihre gesetzlichen Mitbestimmungsrechte geltend machen, wenn der Arbeitgeber seinen Beschäftigten neue Handlungs-, Überwachungs- und Meldepflichten auferlegen will. Compliance-Regeln können – wenn sie richtig gestaltet und eingehalten werden – sowohl Arbeitgebern als auch Beschäftigten nützen. Hier muss der Betriebsrat darauf achten, dass die Interessen des Arbeitgebers nicht die der Arbeitnehmer überwiegen. Die arbeitsrechtliche Implementierung sollte – soweit durchsetzbar – über Betriebsvereinbarungen erfolgen. Denn nur so kann der Betriebsrat mitbestimmen und notfalls die Einigungsstelle oder das Arbeitsgericht anrufen.

83 EGMR, Urteil vom 21.07.2011, Beschwerdenummer 28274/08.

Literatur

Holzhauser, Guido/Sutter, Carolin: Interdisziplinäre Aspekte von Compliance, Baden-Baden, 2011.

Priebe, Andreas: Straf- und Bußgeldvorschriften im Betriebsverfassungsgesetz, 2009, Online-Veröffentlichung: http://www.boeckler.de/37836.htm (Zugriff am 16.11.2011).

Schneider, Uwe: Compliance als Aufgabe der Unternehmensleitung, in: Zeitschrift für Wirtschaftsrecht (ZIP), 2003. Seite 645

Wecker, Gregor/van Laak, Hendrik: Compliance in der Unternehmenspraxis: Grundlagen, Organisation und Umsetzung, Wiesbaden, 2008.

IV Whistleblowing: Den Umgang mit Hinweisen und Meldungen im Unternehmen gestalten

Eine Auswertung betrieblicher Regelungen

von Manuela Maschke und dem Whistleblower-Netzwerk e.V.

1 Worum geht es?

Wer in die Trillerpfeife bläst (engl. whistleblowing), sorgt zunächst für Aufmerksamkeit, prangert womöglich einen Missstand an oder schlägt sogar Alarm. Werden Strukturen im Unternehmen eingerichtet, die solche Meldungen von Verstößen ermöglichen, spricht man von einem Whistleblowing-System. Da Skandale um Korruption oder Datenmissbrauch in jüngerer Zeit zunehmen, ist es gut, wenn Unternehmen ein Hinweisgebersystem einrichten, um aus eigenem Antrieb heraus gegen Missstände vorzugehen. Dabei kann sich die Einrichtung eines Whistleblowing-Systems als Gratwanderung herausstellen. Whistleblowing hat nicht von vornherein ein positives Image, vielfach wird es als Denunziantentum oder Spitzelei eingeordnet. Ob ein Whistleblowing-System dazu beiträgt, falsche Verdächtigungen gezielt zu platzieren (was letztlich auch ohne CMS möglich ist), unbeliebte Beschäftigte zu diskreditieren oder ob es auch positive Wirkungen mit sich bringt, hängt nicht zuletzt von der Unternehmenskultur ab. In diesem Zusammenhang dürfte es auch relevant sein, welche Arten von Verstößen gemeldet werden sollen (vgl. Kap. III).

Der Whistleblower kann z. B. ein Beschäftigter im Unternehmen sein. Er geht persönliche und arbeitsrechtliche Risiken ein, wenn er auf einen Missstand, gesetzwidriges oder unethisches Verhalten in der Organisation, aufmerksam macht. Adressaten der Hinweise und Informationen können z. B. Vorgesetzte sein, Fachabteilungen, vom Unternehmen Beauftragte etc. Auch die Option, Vorgesetzte gerade nicht in den Informationsfluss einzubinden, wird ermöglicht, z.B. wenn diese selbst verdächtigt werden. Richten sich Hinweise an Dritte außerhalb des Unternehmens, z. B. an Aufsichtsbehörden oder die Öffentlichkeit, spricht man von externem Whistleblowing.

In einigen Bereichen bestehen seit längerem Meldemöglichkeiten oder -pflichten. Einige umfassendere Whistleblowing-Regelungen gehen vom US-Börsenrecht aus (vgl. Kap. I). Sie verstehen sich als Instrument zur Überwachung von rechtskonformen Handeln sowie als innerbetriebliches Frühwarnsystem zur Vorsorge gegen Risiken. Vor allem international tätige Konzerne sehen sich daher häufig

in der Pflicht, entsprechende Richtlinien einzuführen. Unternehmen führen Hinweisgebersysteme z. B. auch als Reaktion auf Korruptionsskandale ein.

Bei der Einführung von Hinweisgeber-Systemen kann der Betriebsrat mitbestimmen (vgl. Kap. III).

Im Rahmen einer Analyse des Archivs Betriebliche Vereinbarungen der Hans-Böckler-Stiftung wurden erstmals 32 Richtlinien und Vereinbarungen der Jahre 2008 bis 2011 ausgewertet. Die Auswertung zeigt, dass kollektive betriebliche Vereinbarungen zu diesem Thema bislang eher selten sind. Häufiger bestimmen einseitig getroffene Unternehmensrichtlinien und Verhaltenskodizes Wege, wie mit Hinweisen und Meldungen umgegangen werden soll. Sie legen fest, welche Arten von Missständen von wem und an wen intern gemeldet werden dürfen, können oder sollen und wie mit diesen Meldungen umgegangen wird.

Über die konkrete Praxis, wie mit Hinweisen umgegangen wird, sind Unternehmen mit Informationen meist äußerst zurückhaltend. Wenn Unternehmen mit der Aufdeckung von Korruption Schlagzeilen machen, wird befürchtet, dass eher der Begriff Korruption als jener der Aufklärung hängen bleibt. Ohne Transparenz bezogen auf die praktische Anwendung, ist andererseits kaum zu beurteilen, ob Meldesysteme nur auf dem Papier gut aussehen, ob sie in der Praxis als „Spitzelsysteme“ gegen unliebsame Beschäftigte oder als reinigendes Instrument auch gegen rechtswidriges und unmoralisches Verhalten genutzt werden.

2 Regelungsrahmen und Regelungsaspekte

Die meisten ausgewerteten Vereinbarungen sind allgemeine Verhaltensrichtlinien, die von Unternehmensleitungen vorgegeben werden. Dabei stellen Whistleblowing-Regelungen nur einen Teilaspekt dar.

Verhaltensrichtlinien beschreiben, welches Verhalten ein Unternehmen allgemein von seinen Organen und Beschäftigten erwartet und welches Verhalten aus Sicht des Unternehmens unerwünscht oder untersagt ist. Dies soll einerseits ein Verhalten fördern, das den vorgegebenen staatlichen Rechtsrahmen respektiert. Andererseits wird häufig auch versucht, eine Unternehmenskultur zu etablieren für den Umgang miteinander und mit Kunden. Im Einzelnen finden sich hierfür vielfältige Bezeichnungen, z. B.: Code of Conduct, Verhaltensrichtlinie, Verhaltenskodex, Grundsätze integren Verhaltens, Ethik-Charta, Corporate Compliance Policy etc. Auch die genauen Regelungsinhalte und ihre Formulierungen variieren stark. In umfassenden Richtlinien finden sich häufig folgende Regelungsthemen:

- Verhalten und Respekt im Umgang miteinander
- Gesetzestreue und redliche Führung der Geschäfte
- Vertraulichkeit – Interessenskonflikte, Trennung von Privat- und Konzerninteressen
- Korruption oder Bestechung
- Prävention von Geldwäsche
- Keine gesetzeswidrigen Aktivitäten
- Wettbewerbs- und Kartellrecht
- Schutz natürlicher Ressourcen und des […]-Vermögens
- Annahme und Gewährung von Geschenken und anderen Vergünstigungen
- Periodenabschlüsse und Finanzkommunikation
- Insiderregeln
- Datenschutz und IT Sicherheit
- Umsetzung der Compliance Rules.

Vereinzelt werden solche Richtlinien mit dem Betriebsrat kommuniziert. Hin und wieder gibt es auch Betriebsvereinbarungen, die allgemein eine Art Verhaltenskodex definieren. Die meisten Betriebsvereinbarungen werden jedoch zu enger eingegrenzten Fragestellungen geschlossen, z. B. Korruptionsprävention oder dezidiert zum Whistleblowing-System.

Die Einhaltung von Gesetzen und Regeln im Unternehmen ist keine neue Pflicht für Arbeitgeber und Beschäftigte und auch kein neues Thema für Betriebsräte. Neben den gesetzlichen Vorschriften, dient das Direktionsrecht des Arbeitgebers, der individuelle Arbeitsvertrag und z.B. auch die Betriebsordnung dazu, das allgemeine Verhalten aller Beschäftigten im Betrieb zu regeln. Die Betriebsordnung schafft im besten Fall einen einheitlichen und verbindlichen Standard, um einen reibungslosen Arbeitsablauf zu gewährleisten. Auch Regeln zum Umgang miteinander sind insofern Bestandteile der Betriebsordnung. Wird gegen die Betriebsordnung verstoßen, kann das arbeitsrechtliche Konsequenzen nach sich ziehen.

Der Betriebsrat hat ein Mitbestimmungsrecht über den Inhalt der Betriebsordnung gemäß § 87 Abs. 1 Nr. 1 BetrVG. Die Betriebsordnung wird dann als Betriebsvereinbarung schriftlich fixiert. Außerdem haben Beschäftigte gem. §§ 84 und 85 BetrVG Beschwerderechte, die sie mit Unterstützung des Betriebsrates vorbringen und durchsetzen können.

Beim Thema Whistleblowing geht es aber nicht nur um Regelungen zum Verstoß gegen Richtlinien und Gesetze, sondern auch um den Schutz der Hinweisgeber. Beschäftigte mit Zivilcourage müssen vor arbeitsrechtlichen und an-

deren Nachteilen (z.B. Mobbing) geschützt werden, wenn sie auf Missstände aufmerksam machen.

Ziele der Regelungen

Als allgemeines Ziel wird häufig moralisches, an Werten orientiertes, integres Handeln der Beschäftigten in den Mittelpunkt gestellt und mit den ökonomischen Zielen in Verbindung gebracht:

> „Das Handeln [der Firma] und ihrer Mitarbeiter ist bestimmt durch Eigenverantwortung, Aufrichtigkeit, Loyalität sowie den Respekt gegenüber den Mitmenschen und der Umwelt. Die Führungskräfte tragen dabei eine besondere Verantwortung. Wesentliche Unternehmensziele sind die Versorgung der Kunden mit den erwünschten Leistungen und der dementsprechende unternehmerische Erfolg. Eine marktgerechte Rendite für die Aktionäre […] kann nachhaltig nur erzielt werden, wenn das Unternehmen nach einer stetig verbesserten Erfüllung der Qualitäts- und Leistungsansprüche strebt." (Energiedienstleister, 080600/28/2008)[84]

Whistleblowing-Regelungen enthalten vereinzelt explizite Anknüpfungen an Vorgaben des US-Rechts:

> „Gemäß dem Sarbanes Oxley Act aus 2002 dient der Whistleblower Prozess dazu, so früh wie möglich schwerwiegende Betrügereien und Fehlverhalten im Prüfungs- und Rechnungswesen sowie in Bank- und Bestechungsangelegenheiten aufzuweisen und zu erkennen." (Metallerzeugung und -bearbeitung, 080600/51/2010)

Zudem finden sich eng eingrenzende, auf Wirtschaftskriminalität fokussierende Zielbestimmungen:

> „Maßnahmen zum Schutz vor Unternehmensschädigendem Verhalten und zur Vorbeugung vor Wirtschaftskriminalität." (Gastgewerbe, 080600/56/2010)

84 Die Branchenangaben und Nummern beschreiben den Standort der Vereinbarung im Archiv Betriebliche Vereinbarungen der Hans-Böckler-Stiftung, www.boeckler.de/betriebsvereinbarungen.

In anderen Fällen werden auch offene Formulierungen gewählt:

> „Zweck dieser Vereinbarung ist die Schaffung eines betriebsinternen Hinweismanagementsystems, das der Aufdeckung und Aufklärung betrieblicher Missstände und dem Schutz der Beschäftigten dienen soll." (Anonym, 80600/63/2010)

Beschrieben werden vielfältige Momente, die einen Hinweis auslösen können: Verstöße gegen unternehmensspezifische Normen, Bezugnahme auf Gesetze (AGG, Datenschutz etc.). Teilweise werden Hinweisgebersysteme eingesetzt, um Arbeitsschutz und Arbeitssicherheit zu verbessern:

> „[…] etwaige Unfälle, Betriebsstörungen oder sonstige gefährliche Bedingungen, […] so dass so schnell und effizient wie möglich Gefahren abgewehrt und Schäden begrenzt werden können." (Chemische Industrie, 080600/21/2008)

Meldeberechtigter Personenkreis

Ausgangspunkt jedes Hinweisgebersystems sind die meldenden Personen. Ob durch unverbindliche Appelle oder verbindliche Vorschriften – stets geht es darum, potenzielle Whistleblower zu motivieren, Hinweise zu geben. Man unterscheidet zwei Systeme:

a) Das interne bzw. geschlossene System beschränkt sich auf alle Beschäftigten oder einzelne Abteilungen bzw. Bereiche.
b) Das nach außen – z. B. für Lieferanten und/oder Kunden – geöffnete System.

Darüber hinaus kann der Anwendungsbereich in regionaler und betrieblicher Hinsicht abgesteckt werden. Hinweisgebersysteme, die letztlich jedem offen stehen, bilden bisher die Ausnahme. Einige Unternehmen lassen jedoch in bestimmten Bereichen, z. B. im (Kunden-)Beschwerdemanagement, Meldungen von außen zu.

In Betriebsvereinbarungen sind leitende Angestellte gemäß § 5 Abs. 3 BetrVG von den vereinbarten Regelungen ausgeschlossen. Speziell bei Compliance-Regelungen werden sie teilweise eingeschlossen bzw. berücksichtigt.

> „Diese Betriebsvereinbarung gilt für alle Arbeitnehmer des Unternehmens im Sinne von § 5 BetrVG. Sie gilt nicht für leitende Angestellte. Das Unternehmen wird jedoch mit den ihm zur Verfügung stehenden rechtlichen Mitteln dafür Sorge tragen, dass die sich aus dem […]-Verhaltenskodex ergebenden Rechte und Pflichten Gegenstand der arbeitsvertraglichen

Beziehungen mit den leitenden Angestellten werden." (Versicherungsgewerbe, 080600/64/2011)

Schutz vor Benachteiligung

Regelungen zum Whistleblowing basieren im Prinzip auf einem Versprechen: Meldende sollen vor Nachteilen geschützt sein. Dieses Versprechen wird im Einzelnen sehr unterschiedlich gestaltet und gewährleistet: Beispielsweise wird Vertraulichkeit garantiert sowie der Schutz der Anonymität. Häufig werden Benachteiligungen ausgeschlossen:

> „Wegen der Erhebung einer Beschwerde werden dem/der Mitarbeiter/-in keine Nachteile entstehen." (Kreditgewerbe, 080600/25/2008)

Seltener finden sich Vereinbarungen, die umfassender formuliert sind und Zuständigkeiten intern regeln. Durch sie sichert der Arbeitgeber aktiven Schutz gegen Benachteiligungen durch Dritte zu:

> „Die zuständigen Mitarbeiter von Compliance stellen sicher, dass ein in redlicher Absicht Meldender vor negativen Auswirkungen seitens des Arbeitgebers, der Kollegen oder Dritter geschützt ist." (Versicherungsgewerbe, 080600/65/2011)

Anonymität bedeutet, dass der Meldende unbekannt und somit vor Benachteiligungen effektiv geschützt ist. Wenn die Angelegenheit hingegen vertraulich ist, dann kennt eine weitere Person die Identität des Meldenden. Diese darf sie jedoch gegenüber Dritten nicht oder nur unter besonderen Voraussetzungen offenbaren. Auch dies dient dem Schutz des Meldenden. Von den dargestellten Meldewegen sollen vor allem internetbasierte Systeme, anonyme Meldungen ermöglichen. Andere Meldewege setzen eher auf Vertraulichkeit, obwohl per Telefon, Post oder anonyme E-Mail-Dienste ebenfalls anonyme Kontakte möglich sind.

Der Schutz durch Anonymität und Vertraulichkeit betrifft vor allem den Kommunikationsweg und die Rückverfolgbarkeit zum Meldenden. Eine Identifizierbarkeit aufgrund des Inhalts der Meldung, des Kontexts oder anderer Äußerungen des Meldenden ist dadurch aber nicht ausgeschlossen. Hier zeigt sich ein gewisser Vorteil von Ombudsleuten und anderen Vertraulichkeitsmittlern: Sie berücksichtigen auch dieses Problem, indem sie die weiterzuleitende Nachricht entsprechend abfassen und den Meldenden beraten. Einige Regelungen verfahren jedoch mit Anonymität und Vertraulichkeit recht undifferenziert.

Die meisten Regelungen, die eine anonyme Meldung ermöglichen, folgen den Empfehlungen der Europäischen Datenschutzrichtlinie (Richtlinie 95/46/EG).[85] Sie weisen darauf hin, dass anonyme Meldungen zwar möglich sind, das Unternehmen aber Meldungen unter Angabe des Namens bevorzugen:

> „Meldungen über den Whistleblower-Channel können anonym oder unter Angabe des Namens des einreichenden Mitarbeiters erfolgen. In der Regel sollten Mitarbeiter ihren Namen bei der Einreichung von Beschwerden oder der Mitteilung von Besorgnissen angeben. Dies ermöglicht eine effizientere Bearbeitung des Vorgangs und erhöht normalerweise die Chancen, eine schnelle Lösung zu finden. Zudem können die einreichenden Mitarbeiter nur so eine direkte Rückmeldung über das Ergebnis des Prozesses erhalten. In Ausnahmefällen können sich Mitarbeiter aber für das anonyme Einreichen von Meldungen entscheiden. Alle anonymen Beschwerden und Besorgnisse werden ebenfalls in professioneller Weise bearbeitet." (Metallerzeugung und -bearbeitung, 080600/62/2008)

Andere Regelungen verfolgen die gleiche Grundlinie, sie gewährleisten jedoch zudem trotz anonymer Meldung einen Rückkanal zum Whistleblower: entweder über internetbasierte Systeme oder über die Vergabe von Identifikationsnummern. So können Ermittler weitere wichtige Informationen vom Hinweisgeber gezielt erfragen und ihm eine Rückmeldung zu Stand und Ergebnis der Bearbeitung geben:

> „Hinweise sollen grundsätzlich unter Nennung des Namens erfolgen. Sie können jedoch auf Wunsch ausnahmsweise auch anonym abgeben werden. Alle Hinweisgeber erhalten für ihren Hinweis eine Hinweis-ID und können eine persönliche PIN wählen. Dadurch können auch an anonyme Hinweisgeber nachträglich Fragen gestellt oder Feedback gegeben werden, sofern diese sich noch einmal mit der Hinweis-ID und ihrer persönlichen PIN melden. Bei anonymen Hinweisen ist insbesondere darauf zu achten, dass offensichtlich missbräuchliche oder unsubstantiierte Hinweise nicht weiterverfolgt werden." (Informationstechnikhersteller, 080600/49/2010)

85 Die Europäischen Datenschutzrichtlinie (Richtlinie 95/46/EG) sieht in Art. 29 die Einrichtung einer beratenden Datenschutzgruppe aus Vertretern der Mitgliedstaaten vor. Diese hat am 1. Februar 2006 eine „Stellungnahme 1/2006 zur Anwendung der EU-Datenschutzvorschriften auf interne Verfahren zur Meldung mutmaßlicher Missstände in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität" angenommen. Die Stellungnahme ist verfügbar unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_de.pdf.

Was muss gemeldet werden?

Inwieweit Mitarbeiter rechtlich verpflichtet sind, Missstände zu melden, ist in der Rechtsprechung bisher nicht eindeutig geklärt und in der juristischen Fachliteratur umstritten. Es spricht vieles dafür, dass eine umfassende innerbetriebliche Anzeigepflicht rechtlich zweifelhaft ist, insbesondere wenn sie eine Selbstanzeige erfordert. Dennoch finden sich derart weite, generell verpflichtende Formulierungen in den analysierten Vereinbarungen häufig:

> „Bei Kenntnis von Verstößen gegen den […] Verhaltenskodex hat jeder Konzernmitarbeiter seine(n) Vorgesetzte(n) oder den Compliance Officer zu unterrichten." (Chemische Industrie, 080600/14/2008)

Teilweise werden die Beschäftigten zusätzlich verpflichtet, bei Ermittlungen zu kooperieren:

> „Ein Verstoß gegen diesen Verhaltenskodex besteht auch darin, die Meldung eines dem Beschäftigten bekannten, vermuteten oder tatsächlichen Verstoßes zu unterlassen oder bei Ermittlungen einer Zuwiderhandlung die Kooperation zu verweigern." (Maschinenbau, 080600/12/2008)

Etwas abgeschwächter sind Soll-Vorschriften formuliert. Kann-Formulierungen machen deutlich, dass das Unternehmen Meldungen begrüßt. Die Entscheidung liegt jedoch letztlich bei den Beschäftigten:

> „Alle Mitarbeiter […] werden ermutigt, Verstöße gegen die Ethik-Charta bei einer der folgenden Personen zu melden […]." (Unternehmensbezogene Dienstleistungen, 080600/18/2008)

Mitunter stellen Erklärungen zum Ziel des Systems klar, dass dessen Nutzung freiwillig ist:

> „[Die Firma] wünscht sich die Anregung offener Diskussionen über verantwortungsvolles Verhalten in einer verbesserungsorientierten und unbürokratischen Ausrichtung. Alle Mitarbeiter sollen daher konzernweit die Möglichkeit erhalten, durch Bereitstellung eines Whistleblower Channels Verstöße gegen rechtliche oder unternehmensinterne Regelungen oder Verhaltensanweisungen an das Unternehmen – anonymisiert oder personalisiert – zu melden. […] Kein Mitarbeiter ist verpflichtet, Fehlverhalten über den Whistleblower Channel zu melden. Es hat für ihn keine Folgen, wenn er diesen Weg nicht benutzt." (Metallerzeugung und -bearbeitung, 080600/62/2008)

Anforderungen an den Meldenden

Hinweisgebersysteme können auch dazu missbraucht werden, falsche Verdächtigungen zu platzieren oder missliebigen Kolleginnen und Kollegen zu schaden. Um solchen Umtrieben vorzubeugen, werden verschiedene Maßnahmen ergriffen: Vorwürfe werden zügig und unter Beachtung des Datenschutzes aufgeklärt, Missbrauch wird ausdrücklich verboten, schützende Ausnahmen werden festgelegt. Eine typische Formulierung lautet, dass der Meldende „[…] nach bestem Wissen und in gutem Glauben" zu handeln habe. Mitunter wird die Absicht des Meldenden hinterfragt. Unklar bleibt letztlich, ob ein Hinweisgeber, der einen zutreffenden Sachverhalt aus niedrigen Beweggründen meldet, Whistleblower-Schutz erfahren soll oder nicht:

> „Die zuständigen Mitarbeiter von Compliance stellen sicher, dass ein in redlicher Absicht Meldender vor negativen Auswirkungen seitens des Arbeitgebers, der Kollegen oder Dritter geschützt ist." (Versicherungsgewerbe, 080600/65/2011)

Folgen bei Fehlverhalten oder Missbrauch

Die meisten untersuchten Vereinbarungen verweisen auf die Folgen bei Fehlverhalten und Missbrauch aller Art. Überwiegend beziehen sie sich auf alle Verstöße gegen aufgestellte Regeln. Bisweilen werden zudem Sanktionen angedroht: z. B. wenn a) trotz Pflicht Verstöße nicht gemeldet werden, b) Meldungen zu Unrecht bzw. böswillig erfolgen, c) Hinweisgeber benachteiligt werden, d) unrechtmäßig in die Untersuchung von Hinweisen eingegriffen wird. Angedroht werden disziplinar- und arbeitsrechtliche Konsequenzen bis hin zur Kündigung. Auch ein zivil- und strafrechtliches Vorgehen wird nicht ausgeschlossen:

> „Wenn ein Fehlverhalten festgestellt wird, werden die zuständigen Personen zur Verantwortung gezogen und gegebenenfalls disziplinarisch bestraft, unter Umständen bis hin zu einer Beendigung des Arbeitsverhältnisses und zu zivilrechtlichen Klagen oder strafrechtlichen Anzeigen. Eine vorsätzliche falsche Anschuldigung wird als Fehlverhalten betrachtet. […] Das Unternehmen wird jeden Fall von möglicher Vergeltung untersuchen und Mitarbeiter, die gegen jemanden, der mögliches Fehlverhalten gemeldet hat, Vergeltung geübt haben, disziplinarisch bestrafen." (Chemische Industrie, 080600/59/2010)

Meldewege

In Unternehmen sind Berichtswege üblicherweise vorgeschrieben, häufig zunächst zur jeweils übergeordneten Hierarchiestufe. Ein typisches Kennzeichen von Whistleblowing-Systemen ist, dass die starre Bindung des Berichts an Vorgesetzte durchbrochen werden soll. Mitunter gelten gerade Vorgesetzte als befangen oder vermissen aus anderen Gründen das Vertrauen der Meldenden. Für diese Fälle sollen alternative Meldewege bereitstehen, damit die Unternehmensleitung über den Missstand informiert werden und hierauf reagieren kann.

Dennoch entspricht es den Empfehlungen z. B. des Britischen Instituts für Normung,[86] auch die unmittelbaren Vorgesetzten als mögliche, wenn nicht sogar als bevorzugte Hinweisempfänger zu benennen und ein möglichst niedrigschwelliges Hinweissystem bereitzustellen. Dem entspricht auch ein Großteil der untersuchten Regelungen.

Neben Vorgesetzten werden regelmäßig weitere potenzielle Adressaten für Hinweise benannt, z. B. bestimmte Abteilungen des Unternehmens. Darüber hinaus finden sich in einem Teil der Regelungen spezielle Meldewege, die extra eingerichtet sind, um Hinweise entgegenzunehmen. Im Wesentlichen werden vier Grundformen unterschieden: ein spezielles Call-Center, ein spezielles Internetangebot, interne und/oder externe Ombudsleute. Zum Teil werden diese vier Grundformen kombiniert oder nebeneinander eingesetzt.

Das Call-Center wird meist von externen Dienstleistern betrieben, die oft im Ausland, insbesondere in den USA, angesiedelt sind. Es erfasst die eingehenden Informationen strukturiert und leitet sie an die jeweils zuständigen Stellen in Unternehmen weiter:

> „[…] hat [die Firma] eine so genannte [service line] eingerichtet, über die Sie mögliche Verstöße gegen den Verhaltenskodex und andere Vorfälle melden können. Sie können sich Ihrer Muttersprache bedienen und, wenn Sie das möchten, anonym bleiben. Die [service line] ist rund um die Uhr erreichbar. Wir haben in jedem Land eine gebührenfreie Rufnummer eingerichtet, die an den jeweiligen Standorten bekannt gegeben wird." (Chemische Industrie, 080600/47/2010)

86 Das Britische Institut für Normung (British Standards Institution, BSI) veröffentlichte pünktlich zum zehnten Jahrestag des britischen Whistleblower-Schutzgesetzes (Public Interest Disclosure Act – PIDA) 2008 einen rechtlich unverbindlichen Code of Practice (PAS 1998:2008). Er dient dem praktischen Umgang mit Whistleblowing und seiner Förderung. Der Code of Practice wendet sich an Unternehmen und andere Organisationen. Er geht von der britischen Rechtslage aus. Viele Konzepte sind auf Deutschland übertragbar.

Internetbasierte Systeme verzichten auf eine direkte Kommunikation. Sie setzen auf technische Anonymisierung. Kennzeichnend sind folgende Bestandteile:

> „[…] ein webbasiertes Meldesystem, das Hinweisgebern ermöglicht, absolut anonym Meldungen abzugeben. Hierbei ist über eine Postfachlösung eine anonyme Kommunikation möglich, um auch Rückfragen an den Hinweisgeber zu richten." (Telekommunikationsdienstleister, 080600/15/20082)

Interne Ombudsleute bzw. Ombudsstellen werden in den vorliegenden Regelungen nur vereinzelt beschrieben:

> „Geschäftsleitung und Betriebsrat verpflichten sich, eine Ombudsstellen zu errichten. Hierbei soll es sich um eine unbefangene Instanz handeln, an die sich Whistleblower vertraulich wenden können. Eine solche Stelle ist erforderlich, um Beschäftigten die Furcht zu nehmen, Unregelmäßigkeiten bei Vorgesetzten anzeigen zu müssen. Die Ombudsstelle besteht aus drei Mitgliedern. Jeweils ein Mitglied kommt aus dem Betriebsrat und der Geschäftsleitung. Die Belegschaft soll zu diesem Zweck aus ihrer Mitte ein weiteres Mitglied wählen." (Anonym, 080600/63/2010)

Teils wird Compliance-Officern eine Beraterfunktion übertragen, und sie werden zu absoluter Verschwiegenheit verpflichtet. Allerdings wird der Begriff Ombudsleute nicht verwendet:

> „Der Compliance Officer steht allen Beschäftigten als Ansprechpartner sowohl zur Beantwortung von Fragen als auch als Berater im Zusammenhang mit den Compliance Rules zur Verfügung. Die Mitarbeiter des Compliance Officers sind zur absoluten Verschwiegenheit verpflichtet." (Chemische Industrie, 080600/14/2008)

Das entspricht der Grundidee des Ombudsleute-Systems: Dem Hinweisgeber soll ein Ansprechpartner zur Verfügung stehen, der die rechtlich abgesicherte Möglichkeit hat, seine Hinweise bzw. die beschuldigte Person nur mit seinem Einverständnis dem Unternehmen zu offenbaren. Man greift für diese Aufgabe in der Regel auf externe Rechtsanwälte zurück. Allerdings ist es rechtlich keineswegs gesichert, dass sich diese in einer derartigen Konstellation wirksam auf ihre Zeugnisverweigerungsrechte berufen können:

> „Die Ombudsleute sind generell erfahrene externe Rechtsanwälte. Die personenbezogenen Daten und sonstigen Informationen, die der Ombudsmann vom Hinweisgeber erhält, werden streng vertraulich behandelt, solange der Hinweisgeber dem Ombudsmann nicht deren vollständige oder teilweise Weitergabe gestattet." (Energiedienstleister, 080600/54/2010)

Zu beachten ist schließlich auch, dass es sich bei Hinweisen an externe Meldeeinrichtungen oder Ombudsleute nicht um externes Whistleblowing handelt. Diese Stellen sind regelmäßig dazu verpflichtet, ihre Informationen nur an das betreffende Unternehmen und gerade nicht an externe Dritte oder an Behörden weiterzugeben.

Neben den unmittelbaren Vorgesetzten und den vier dargestellten besonderen Meldewegen nennen die meisten Regelungen eine Vielzahl anderer Adressaten von Meldungen:

> „[…] Die Führungskräfte im Geschäfts- oder Funktionsbereich oder am Standort des Mitarbeiters
> – Der für den Mitarbeiter zuständige Corporate Compliance Officer
> – Die Rechts- oder die Finanzabteilung
> – Die Personalabteilung, insbesondere bei Fragen, die den Arbeitsplatz betreffen, und bei Richtlinien wie Diskriminierungsverbot, Belästigungsverbot und Privatsphäre der Mitarbeiter." (Chemische Industrie, 080600/59/2010)

Zum Teil wird noch stärker je nach Gegenstand der Meldung differenziert.

Insbesondere in Betriebsvereinbarungen wird häufiger auch die Möglichkeit angesprochen, die (eigene) Meldung auch an den Betriebsrat zu richten:

> „Die Parteien dieser Betriebsvereinbarung stimmen überein, dass der Mitarbeiter auch ein Betriebsratsmitglied seines Vertrauens ansprechen kann." (Versicherungsgewerbe, 080600/64/2011)

Überprüfung der Meldung

Bisweilen wird eine Ermittlung in der Regelung pauschal zugesagt. Mitunter werden Zuständigkeiten und Abläufe differenzierter geregelt: vom Eingang der Meldung über (Vor-)Ermittlungen bis hin zur Zuständigkeit für Sanktionen. Diese Regelungen hängen stark von der jeweiligen Unternehmensstruktur ab. Teils variieren sie je nach Gegenstand der Meldung. Aufgrund ihres Umfanges können sie an dieser Stelle nicht im Detail dargestellt werden. Kennzeichnend ist ein gewisser Spagat: Einerseits darf aus datenschutzrechtlichen und ermittlungstaktischen Gründen nur ein möglichst kleiner Personen- bzw. Ermittlerkreis informiert werden. Dennoch muss die notwendige Expertise eingeholt werden. Zudem müssen betroffene Querschnitts- und Fachabteilungen eingebunden werden. Auch die Information bzw. Einbindung der Leitungsebene und des zuständigen Aufsichtsratsausschusses muss geregelt sein. Soweit vorhanden spielen Compliance-Beauftragte bzw. -Abteilungen eine Schlüsselrolle:

„Im zuständigen Bereich […] wird diese Meldung beantwortet und entschieden, ob die eingegebenen Hinweise durch zuständige Fachseiten bearbeitet werden können oder – bei Hinweisen mit strafrechtlich relevanten Sachverhalten – eine Weitergabe an die Sicherheitsabteilung erfolgt. Handelt es sich um Hinweise, die eine bestimmte ‚Brisanz' in sich bergen oder nicht einer bestimmten Fachseite zugeordnet werden können, werden die Hinweise […] weitergeleitet. […] Es besteht aus Mitgliedern der Bereiche […] Control […], […]revision […], […]sicherheit […], Recht […], Human Resources […], […]kommunikation […] und […] Management. Im […] Compliance wird entschieden, ob Fälle doch von einer Fachseite bearbeitet werden können oder ob aufgrund der Wichtigkeit des Hinweises der Fall vom Committee beraten werden muss. Außerdem wird entschieden, ob Fälle relevant sind für das ‚Hinweisverfahren zur Rechnungslegung und Abschlussprüfung' (Whistleblower). Diese Hinweise werden dann an die Geschäftsstelle Aufsichtsrat weitergeleitet." (Telekommunikationsdienstleister, 080600/15/2008)

Der Datenschutz wird regelmäßig besonders thematisiert. Die Vorgaben bleiben meist grundsätzlich. Mitunter werden konkrete Begrenzungen formuliert, auch Löschungsvorgaben werden geregelt. Gelegentlich werden Verwertungsverbote vereinbart. Die Problematik der Unabhängigkeit der Ermittler wird meist nicht aufgegriffen. Das folgende Beispiel bildet insoweit eine Ausnahme:

„Angezeigte Verstöße werden umgehend untersucht. Dabei ist es unerlässlich, dass eine andere Person den Verstoß untersucht als diejenige, die angezeigt wurde." (Unternehmensbezogene Dienstleistungen, 080600/9/2008)

Des Öfteren thematisiert werden mögliche Folgen von Ermittlungen:

„Sollten Sachverhalte festgestellt werden, die aus arbeitsrechtlicher Sicht Auswirkungen auf Inhalt oder Bestand von Arbeitsverhältnissen rechtfertigen können, wie zum Beispiel schwerwiegende oder laufende Verstöße gegen die Leitsätze, so wird Compliance den festgestellten Sachverhalt schriftlich dokumentieren und die Geschäftsleitung informieren." (Kreditgewerbe, 080600/25/2008)

Die Folgen reichen bis hin zur Einschaltung von Behörden:

„Falls gerechtfertigt, meldet […] mutmaßliche Verstöße den zuständigen Behörden." (Elektro, 080600/52/2010)

Überaus selten wird die Frage der Evaluation ausdrücklich angesprochen:

„Funktionsweise und Effektivität werden regelmäßig überprüft. Ein permanentes Monitoring mit ständiger Bewertung und Berichterstattung soll die fortlaufende Verbesserung dieser Corporate Compliance Policy gewährleisten. Zusätzlich wird die Konzern-Revision […] in regelmäßigen Abständen die Wirksamkeit dieser Corporate Compliance Policy überprüfen." (Chemische Industrie, 080600/57/2010)

Rechte des Beschuldigten

Der datenschutzrechtliche Schwerpunkt liegt bei Hinweisgebersystemen meist auf dem Schutz des Beschuldigten. Hier spielen die genannten Elemente Begrenzung der Informationen auf einen möglichst kleinen Ermittlerkreis, Verknüpfungs- und Verwertungsverbote sowie Löschungsauflagen eine entscheidende Rolle. Ein weiterer wichtiger Aspekt ist die Frage, wann der Beschuldigte über die gegen ihn erhobenen Vorwürfe informiert wird. Hierzu finden sich eher allgemeine Formulierungen:

„Der Angezeigte wird umgehend und nach Maßgabe der datenschutzrechtlichen Vorgaben über ihn betreffende Hinweise benachrichtigt". (Informationstechnikhersteller, 080600/49/2010)

Laut einigen Regelungen sollen Beschuldigte so frühzeitig wie ohne Gefährdung der Ermittlungen möglich, informiert werden:

„Sollte sich eine Meldung nicht von vornherein als haltlos erweisen, ist dem betroffenen Mitarbeiter möglichst frühzeitig Gelegenheit zur Stellungnahme zu geben, soweit die Aufklärung des Falles dadurch nicht gefährdet wird". (Fahrzeughersteller von Kraftwagenteilen, 080600/29/2009)

Zum Teil wird noch konkreter vorgeschrieben, welche Informationen der Beschuldigte erhalten muss:

„[…] die beschuldigte Person darüber informieren, dass ein Bericht unter Registrierung personenbezogener Daten gegen sie eingereicht wurde. Die Information hat wichtige Informationen wie:

- über den Whistleblower und den verbundenen Prozess
- die Einzelheiten, die eingereicht wurden
- die Abteilungen, die über den Bericht informiert sein könnten
- die Berechtigungen zum Zugriff auf die Daten

zu enthalten." (Metallerzeugung und -bearbeitung, 080600/62/2008)

Das Recht auf Einsichtnahme und Richtigstellung basiert auf dem Bundesdatenschutzgesetz:

„Jeder Mitarbeiter hat das Recht auf Einsichtnahme und Richtigstellung seiner persönlichen Daten. Dies gilt ebenfalls für alle in den Meldungsakten verfügbaren Angaben." (Metallerzeugung und -bearbeitung, 080600/51/2010)

Auch das Verbot der Benachteiligung zunächst Beschuldigter wird explizit formuliert – für den Fall, dass sich Verstöße nicht hinreichend belegen lassen:

„Können solche Meldungen hingegen nicht ausreichend mit Fakten belegt werden, dürfen für den beschuldigten Mitarbeiter keine Konsequenzen entstehen, insbesondere wird der Vorgang nicht in der Personalakte dokumentiert." (Fahrzeughersteller von Kraftwagenteilen, 080600/29/2009)

Einschaltung externer Stellen

Alle ausgewerteten Vereinbarungen behandeln ausschließlich internes Whistleblowing. An keiner Stelle finden sich Regelungen, die Meldungen an Behörden oder Hinweise an die Öffentlichkeit ausdrücklich zulassen. Dies wäre nach der Rechtsprechung des Bundesarbeitsgerichts in Ausnahmefällen durchaus zulässig. Stattdessen werden Behördenkontakte streng reguliert:

„Im Kontakt mit Behörden, die, wie beispielsweise die Polizei oder die Staatsanwaltschaft, auch die Aufgabe haben, Verstöße gegen geltendes Recht zu untersuchen und gegebenenfalls zu ahnden, ist sofort die Rechtsabteilung einzubeziehen. Insbesondere die Erteilung von Auskünften und die Vorlage von Akten sollen in derartigen Fällen nur nach Rücksprache mit der Rechtsabteilung erfolgen." (Chemische Industrie, 080600/57/2010)

Fast alle Regelungen enthalten zum Teil sehr weitgehende Verschwiegenheitsverpflichtungen hinsichtlich der Weitergabe von Informationen:

„Alle Mitarbeiterinnen und Mitarbeiter sind verpflichtet, über sämtliche internen Angelegenheiten von […] Stillschweigen zu bewahren, die nicht ausdrücklich von den dafür zuständigen Stellen für die Öffentlichkeit freigegeben worden sind." (Chemische Industrie, 080600/21/2008)

Auch die freie Meinungsäußerung der Beschäftigten wird eingeschränkt:

„Jeder Beschäftigte hat das Recht zur freien Meinungsäußerung. Dennoch muss sichergestellt werden, dass sowohl Zeitpunkt, Rahmen und Inhalt jeder Aussage in der Öffentlichkeit mit den Interessen und Zielen des Unternehmens übereinstimmen und mit den zuständigen Vorgesetzten und dem Bereich [Kommunikation] abgestimmt sind." (Fahrzeughersteller Kraftwagen, 080600/17/20089

Wenn Hinweisgebersysteme sehr restriktiv gehandhabt werden, kann die teilweise beabsichtigte „offene Diskussion“ durchaus am Werkstor enden.

Kommunikation der Regelungen

Der Umgang mit Hinweisen und Meldungen muss mit der Belegschaft kommuniziert werden, damit die Beschäftigten wissen, was ihnen angeboten bzw. was von ihnen erwartet wird. Hierzu finden sich unterschiedliche Detailregelungen, die auf die Selbstverantwortung der Beschäftigten setzen:

> „Jeder Mitarbeiter ist verpflichtet, sich selbst über die bestehenden internen und externen Regelungen zu informieren, um sicherzustellen, dass er in Übereinstimmung mit diesen handelt.“ (Datenverarbeitung und Softwareentwicklung, 080600/46/2010)

Andere Regelungen betonen die Verantwortung der Vorgesetzten oder der Spezialabteilungen (insbesondere Compliance). Hinweise auf die Einbindung der Arbeitnehmervertretung finden sich bisher eher selten:

> „Diese Grundsätze werden allen Beschäftigten und ihren Interessenvertretungen in geeigneter Form zugänglich gemacht. Die Kommunikationsmaßnahmen werden zuvor mit den Arbeitnehmervertretungen beraten.“ (Fahrzeughersteller Kraftwagen, 080600/60/2010)

Zum Teil müssen Beschäftigte explizit bestätigen, dass sie die Regelungen zur Kenntnis genommen haben.

Einige Unternehmen bieten ihren Beschäftigten spezielle Schulungen an:

> „Zur Schulung der Mitarbeiter werden Schulungsprogramme bereitgestellt, die über die Online-Schulung hinausgehende, für die jeweilige Funktion relevante Themen behandeln.“ (Informationstechnikhersteller, 080600/49/2010)

In einigen Fällen ist die Teilnahme an entsprechenden Schulungen sogar ausdrücklich vorgeschrieben.

3 Mitbestimmung und Umgang mit Konflikten

Rolle des Betriebsrats

Laut § 84 BetrVG steht jedem Arbeitnehmer das Recht zu, sich bei seinem Arbeitgeber zu beschweren – nach dem Wortlaut der Vorschrift allerdings nur „soweit er sich von Arbeitgeber oder von Arbeitnehmern des Betriebs benachteiligt oder ungerecht behandelt oder in sonstiger Weise beeinträchtigt fühlt.“ Zwar kann er

ein Mitglied des Betriebsrats „zur Unterstützung oder Vermittlung“ hinzuziehen; Voraussetzung ist demnach aber immer die Geltendmachung eigener Rechte, also gerade nicht der typische Fall des Whistleblowings.

Gleiches nimmt die herrschende Meinung für § 86 BetrVG an. Auch § 86a BetrVG spielt in der Diskussion um Whistleblowing bisher kaum eine Rolle. Dennoch bieten all diese Vorschriften Betriebsräten Spielräume: Sie können umso stärker genutzt werden, je mehr Vertrauen potenzielle Whistleblower dem Betriebsrat entgegenbringen und je mehr dieser die (Nicht-)Beachtung öffentlicher Interessen und deren Auswirkungen auf den Betrieb erkennbar thematisiert. Einschlägig formuliert sind die §§ 84, 85 BetrVG, soweit es darum geht, Benachteiligungen von Whistleblowern aber auch von Beschuldigten zu verhindern.

Betriebliche Regelungen zum Whistleblowing berühren regelmäßig Fragen der Ordnung des Betriebs und des Verhaltens der Arbeitnehmer im Betrieb – vorausgesetzt, sie gehen über den bloßen Verweis auf gesetzliche Beschwerderechte hinaus und haben nicht rein deklaratorischen Charakter. Es bestehen demnach Mitbestimmungsrechte nach § 87 Abs. 1 Nr. 1 BetrVG. Soweit technische Einrichtungen (z. B. Call-Center, Internetportale, Compliance-Datenbanken u. a.) geschaffen werden, greift § 87 Abs. 1 Nr. 6 BetrVG. Je nach Anwendungsbereich können darüber hinaus weitere Tatbestände des § 87 Abs. 1 BetrVG (z. B. Nr. 7 und 12) relevant werden. Generell gilt laut Rechtsprechung des Bundesarbeitsgerichts, dass Whistleblower-Regelungen nicht insgesamt zu betrachten sind: Die Mitbestimmungspflichtigkeit muss hinsichtlich jedes einzelnen Elements der Regelung gesondert geprüft werden.

Auch die Personalvertretung hat nach § 68 BPersVG die Aufgabe, „Anregungen und Beschwerden von Beschäftigten entgegenzunehmen und, falls sie berechtigt erscheinen, durch Verhandlung mit dem Leiter der Dienststelle auf ihre Erledigung hinzuwirken.“

Innerhalb der ausgewerteten Regelungen sind es naturgemäß vor allem Betriebsvereinbarungen, die dem Betriebsrat teilweise eine aktive Rolle im Hinweisgebersystem zuweisen oder zumindest ermöglichen. Einige beziehen sich auf die §§ 84, 85 BetrVG und weiten sie auf alle Compliance-Belange aus:

> „In allen Belangen von Compliance kann der/die Mitarbeiter/-in von seinem/ihrem Beschwerderecht gemäß §§ 84, 85 BetrVG Gebrauch machen und bei allen diesbezüglich geführten Gesprächen den örtlichen Betriebsrat hinzuziehen.“ (Kreditgewerbe, 080600/25/2008)

Nachstehend wird der Betriebsrat ausdrücklich als mögliche Meldestelle genannt:

„Bei Beschwerden oder Hinweisen auf eine mögliche Verletzung dieser gemeinsamen Erklärung kann sich jeder Mitarbeiter direkt an seinen Vorgesetzten oder an die jeweilige lokale Arbeitnehmervertretung sowie auch an die […] benannten externen Ombudsleute wenden." (Fahrzeughersteller von Kraftwagenteilen, 080600/55/2010)

Mitunter werden lediglich grundsätzliche Bekenntnisse zum Hinweisgebersystem formuliert:

„[…] und der Konzernbetriebsrat halten diese Maßnahme im Interesse der Mitarbeiter und des Unternehmens für sinnvoll und wirken daher bei der konzernweiten Einführung durch diese Konzernbetriebsvereinbarung mit." (Metallerzeugung und -bearbeitung, 080600/62/2008)

Im folgenden Beispiel werden Informations- und Berichtspflichten zugunsten des Betriebsrats formuliert. Sie beziehen sich auf das gesamte Hinweisgebersystem:

„Die Geschäftsleitung informiert den Gesamtbetriebsausschuss im Rahmen der regelmäßigen Sitzungen über die Anzahl der Anzeigen (nach Regionen), die Art des Schädigungsvorwurfs, sowie über das Verhältnis von bestätigten Vorwürfen zu offensichtlich unbegründeten Vorwürfen und solchen, die nicht abschließend aufgeklärt werden konnten. Die Geschäftsleitung informiert des Weiteren über die damit verbundenen eingeleiteten personellen Maßnahmen gegen Anzeigende/Beschuldigte sowie über Maßnahmen zum Schutz des Unternehmens bei begründeten Vorwürfen." (Gastgewerbe, 080600/56/2010)

Eine Mustervereinbarung enthält folgenden weitergehenden Vorschlag zur Einbindung des Betriebsrates:

„Geschäftsleitung und Betriebsrat verpflichten sich, eine Ombudsstelle zu errichten. Hierbei soll es sich um eine unbefangene Instanz handeln, an die sich Whistleblower vertraulich wenden können. […] Die Ombudsstelle besteht aus drei Mitgliedern. Jeweils ein Mitglied kommt aus dem Betriebsrat und der Geschäftsleitung. Die Belegschaft soll zu diesem Zweck aus ihrer Mitte ein weiteres Mitglied wählen. […] Die Ombudsstelle leitet den Hinweis an den Betriebsrat und die Geschäftsleitung weiter." (Anonym, 080600/63/2010)

Bisweilen werden Betriebsräte in Schulungsmaßnahmen zum Thema Whistleblowing eingebunden und informiert.

Behandlung von Konflikten

Soweit Betriebsvereinbarungen zu Whistleblowing Konflikte zwischen den Vertragsparteien regeln, sehen sie meist strukturierte und gestufte Einigungsversuche und notfalls das Anrufen der Einigungsstelle gemäß § 76 BetrVG vor:

> „Auftretende Meinungsverschiedenheiten und Interpretationsschwierigkeiten aus dieser Vereinbarung werden zwischen Geschäftsleitung und dem Gesamtbetriebsrat behandelt. Erweist sich diese Vereinbarung als auslegungs- und ergänzungsbedürftig oder treten nicht ausräumbare Meinungsverschiedenheiten zwischen Mitarbeiterin/Mitarbeiter und Geschäftsleitung auf, so werden Geschäftsleitung und Gesamtbetriebsrat in einer paritätisch aus mindestens je zwei Mitgliedern gebildeten Kommission im Sinne einer vertrauensvollen Zusammenarbeit gemeinsam nach Lösungen suchen. Ist Einvernehmen nicht zu erzielen, entscheidet die Einigungsstelle gem. § 76 BetrVG." (Kreditgewerbe, 080600/25/2008)

Transparenz sowie die Einbindung der Beschäftigten und ihrer Interessenvertretungen sollten das Leitmotiv darstellen für die Entwicklung, Anwendung bis hin zur Evaluation und Anpassung von Compliance-Richtlinien und CMS. Ein solches Verständnis verbessert die Akzeptanz und unterstützt Maßnahmen. Hierin liegt auch ein Vorteil von kollektiven Vereinbarungen gegenüber einseitigen Vorgaben durch die Unternehmensleitung: gemeinsame Vereinbarungen erhöhen die Verbindlichkeit. Die Beteiligung von Beschäftigten, die Beachtung von Mitbestimmungsrechten der Interessenvertretungen gehören dazu. Compliance beginnt an diesem Punkt im Unternehmen: Die Gretchenfrage lautet daher: Wie hältst du es mit dem Betriebsrat?

4 Zum Schluss

Vor dem Hintergrund des Urteils des EGMR vom 21.07.2011 und einer Selbstverpflichtungserklärung der G20-Staaten bis Ende 2012 gesetzliche Regelungen zum bestmöglichen Schutz von Whistleblowern zu schaffen, ist auch in Deutschland eine Diskussion um Gesetzesänderungen in Gang gekommen. Alle Oppositionsfraktionen haben hierzu eigene Anträge in den Bundestag eingebracht. Am 05.03.2012 fand im Ausschuss für Arbeit und Soziales auch eine Anhörung zum Thema statt (http://dbtg.tv/cvid/1590010). Die Koalitionsfraktionen sahen jedoch keinen Bedarf für neue gesetzliche Regelungen.

Download der Auswertung und weiterer Informationen zum Abschluss einer betrieblichen Vereinbarung unter: www.boeckler.de/betriebsvereinbarungen, Auswertungen: Kompass, Unternehmenskultur oder www.boeckler.de/6299.htm?produkt=HBS-005053

Literatur

Brandt, Jochen: Compliance und Datenschutz. In: Arbeitsrecht im Betrieb (AiB), 2009, Heft 5, S. 288–291.

Briegel, Torsten: Einrichtung und Ausgestaltung unternehmensinterner Whistleblowing-Systeme, Wiesbaden, 2009.

Donato, Jessica: Whistleblowing – Handlungsempfehlungen für eine nutzenstiftende Umsetzung in deutschen börsennotierten Unternehmen, Frankfurt am Main, 2009.

Düsel, Jens: Gespaltene Loyalität – Whistleblowing und Kündigungsschutz in Deutschland, Großbritannien und Frankreich, Baden-Baden, 2010.

Fahrig, Thomas: Die Einführung eines Verhaltenskodexes und das Whistleblowing, Baden-Baden, 2010.

Goers, Matthias: Der Ombudsmann als Instrument unternehmensinterner Kriminalprävention, Frankfurt am Main, 2010.

Leisinger, Klaus M.: Whistleblowing und Corporate Reputation Management, Mering, 2003.

Neumann, Anneli: Whistleblowing und die Frage nach dem rechtspolitischen Erfordernis einer gesetzlichen Schutzregelung, Berlin, 2010.

Pittroff, Esther: Whistle-Blowing-Systeme in deutschen Unternehmen, Wiesbaden, 2011.

Rohde-Liebenau, Björn: Whistleblowing, edition der Hans-Böckler-Stiftung, Nr. 159, Düsseldorf, 2005.

Schulz, Mike: Ethikrichtlinien und Whistleblowing – Arbeitsrechtliche Aspekte der Einführung eines Compliance-Systems, Frankfurt am Main, 2010.

Triskatis, Claudiana: Ethikrichtlinien im Arbeitsrecht, Frankfurt am Main, 2008.

Wagner, Andreas: Ethikrichtlinien – Implementierung und Mitbestimmung, Baden-Baden, 2008.

Zander, Ulrike: Ethik- und Verhaltensrichtlinien im Betrieb, Berlin, 2010.

Internethinweise

Der Code of Practice on Whistleblowing (PAS 1998:2008) der British Standards Institution kann kostenlos bezogen werden über www.pcaw.co.uk/bsi/

Die Mitgliederzeitschrift „Scheinwerfer“ von Transparency Deutschland hat sich in Ausgabe 44/2009, mit dem Schwerpunkt Hinweisgeber beschäftigt. Das Heft ist verfügbar unter:
http://www.transparency.de/fileadmin/pdfs/Rundbriefe/Scheinwerfer_44_III_2009_Hinweisgeber.pdf
Vielfältige weitere Informationen rund um das Thema Whistleblowing und weiterführende Links bieten die Seiten des Whistleblower-Netzwerks: www.whistleblower-net.de
Europäischer Gerichtshof für Menschenrechte 5. Sektion, Heinisch versus Germany, Application no. 28274/08, Urteil vom 21.07.2011. Eine ausführlichere Darstellung findet sich z. B. unter: www.whistleblower-net.de/blog/2011/07/21/urteil-des-egmr-whistleblowing-von-meinungsfreiheit-geschuetzt/

V Compliance-Management-Systeme von DAX-Unternehmen – ein Vergleich

von Lasse Pütz und Maximilian Waclawczyk

1 Übersicht

Haftungsfälle von Vorständen sowie Rücktritte von Managern und Aufsichtsräten aufgrund von Regelverstößen trugen in letzter Zeit zur Verunsicherung der Wirtschaft, der Unternehmen und der Öffentlichkeit bei. Immer mehr Unternehmen beschäftigen sich aus diesem Grund mit dem Thema Compliance. Wie jedoch die vorhergehenden Ausführungen zeigen, ist weder der Begriff Compliance abschließend definiert, noch können die Bestandteile eines CMS abschließend benannt werden. Letztlich ist jedes CMS individuell auf das jeweilige Unternehmen anzupassen. Die Risiken eines Unternehmens, seine Organisationsstruktur sowie seine Unternehmenskultur geben maßgeblich vor, welche Maßnahmen hinter einem CMS stehen sollten (vgl. Kap. I und Pütz 2011, S. 17 ff.).

Dennoch kann ein vergleichender Blick in die Praxis der Unternehmen Anregungen geben, wie ein Compliance-System aussehen kann oder ob das bestehende System den Anforderungen der heutigen Zeit gerecht wird. Einige Elemente kamen häufig vor, so dass zumindest von Good-Practice-Maßstäben gesprochen werden kann. Für einen vergleichenden Blick eignen sich besonders die DAX-Unternehmen. Zum einen müssen sich diese Unternehmen nach § 161 AktG erklären, ob sie dem Deutschen Corporate Governance Kodex folgen,[87] der wiederum Compliance als eine Pflicht des Vorstandes hervorhebt.[88] Zum anderen sind sie wegen ihrer Größe und Internationalität oftmals Vorreiter von neueren Entwicklungen.

87 Der Deutsche Corporate Governance Kodex (DCGK) richtet sich an börsennotierte Gesellschaften und gibt diesen Empfehlungen (keine gesetzlich zwingenden Vorgaben), deren Nichtbeachtung offengelegt und begründet werden muss (vgl. § 161 AktG).

88 Ziff. 3.4 Abs. 2 S. 1 DCGK; vgl. auch: Hans-Böckler-Stiftung 2011b, S. 7 und 11 ff.; zur rechtlichen Verbindlichkeit des DCGK: Schmidt 2010, S. 44 ff.

2 Untersuchungsmethode

Die nachfolgenden Ausführungen versuchen, einige Good-Practice-Maßstäbe soweit möglich zu identifizieren. Hierfür wurden die Internetpräsenzen sowie die dort veröffentlichten Geschäfts- und Nachhaltigkeitsberichte der 30 DAX-Unternehmen betrachtet und ausgewertet. Stichtag der Untersuchung war der 31.08.2011. Alle Angaben der Unternehmen wurden, soweit möglich, auf ihre Plausibilität überprüft.

Ein Vorteil der gewählten Herangehensweise ist, dass – anders als bei einer Befragung – nicht mit einem abgeschlossenen Kriterienkatalog gearbeitet wurde. Vielmehr war eine offene Herangehensweise möglich, bei der im Laufe der Untersuchung der Fokus erweitert und angepasst werden konnte. Ein Nachteil dieser Herangehensweise ist jedoch, dass eine mögliche Diskrepanz zwischen der Eigendarstellung im Internet und der tatsächlichen im Unternehmen anzutreffenden Praxis nicht ausgeschlossen werden kann. So ist es möglich, dass ein Unternehmen bestimmte Compliance-Maßnahmen anwendet, ohne diese im Internet oder ihrem Geschäftsbericht zu benennen. Zuletzt kann, trotz größter Sorgfalt, nicht vollständig ausgeschlossen werden, dass bestimmte Inhalte der Webpräsenzen nicht aufgefunden wurden, da einige Unternehmen mittlerweile über weit verzweigte Internetseiten mit vielfachen Verlinkungen verfügen. Trotz dieser Defizite, die aus der Art der Untersuchung resultieren, zeichnen sich in den gefundenen Ergebnissen Tendenzen ab, welche Compliance-Maßnahmen zumindest bei großen Unternehmen regelmäßig verwendet werden.

3 Ergebnisse der Untersuchungen

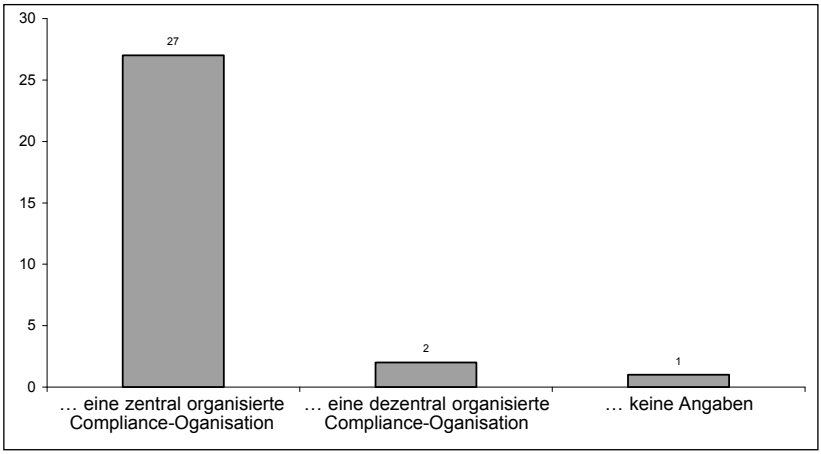
Die Darstellungen der Unternehmen unterscheiden sich teilweise erheblich. Zwar lassen sich bei den meisten Unternehmen die Compliance-relevanten Inhalte und Aussagen schnell ausfindig machen. Einem einheitlichen Darstellungsmuster folgen sie indes nicht. Da es auch kein einheitliches CMS geben kann (Pütz 2011, S. 17), werden gleiche oder ähnliche Sachverhalte oft in anderem Kontext dargestellt.

In nachfolgenden Darstellungen wird versucht soweit möglich, die Compliance-Organisation und einzelne Maßnahmen zu vergleichen. Weitere Aspekte die behandelt werden, betreffen Fragen der Berichterstattungen an den Aufsichtsrat, die Bedeutung von Verhaltenskodize, Risikoanalysen, die Rolle des Betriebsrats sowie Zertifizierungen von CMS.

3.1 Compliance-Organisation

Ein homogenes Bild ergibt sich zunächst hinsichtlich der Ausgestaltung der Compliance-Organisation (vgl. Abb. 1). In 27 Fällen geben die Unternehmen an, dass die Leitung der Compliance-Maßnahmen unterhalb des Vorstandes zentral in einer Person oder Abteilung zusammengefasst sind (Chief Compliance Officer, Group Compliance Officer etc.). In zwei Fällen werden die Aufgaben dezentral wahrgenommen. Ein Unternehmen macht keine Angaben hinsichtlich des Aufbaus der Compliance-Organisation.

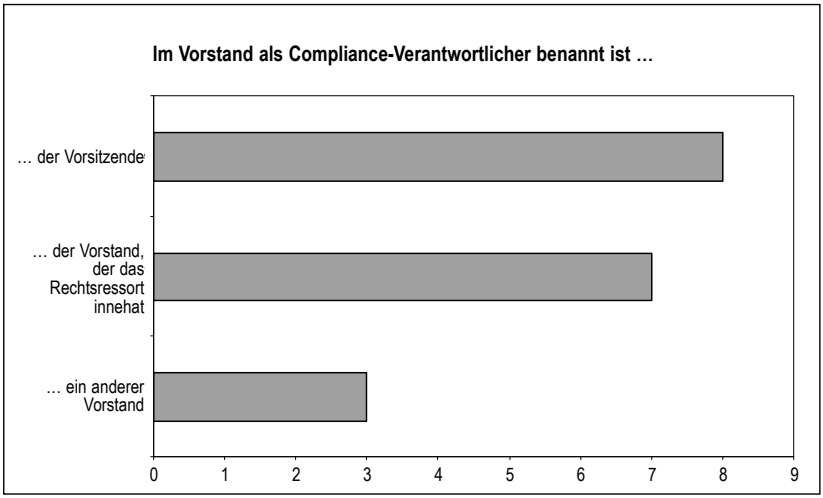
Abb. 1: Compliance-Organisation, eigene Berechnungen, n = 30 DAX-Unternehmen



Von den 30 Unternehmen heben 24 Unternehmen hervor, dass sie regionale oder nach Geschäftsbereichen unterteilte Compliance Officer beschäftigen. Ob diese ausschließlich für den Bereich Compliance tätig oder auch operativ ins Unternehmensgeschäft eingebunden sind, lässt sich aus den Darstellungen nicht entnehmen.

In 18 Unternehmen folgt aus den Ressortbeschreibungen der Vorstände, dass die Compliance-Funktion explizit einem Mitglied des Vorstands übertragen wurde (vgl. Abb. 2). In acht Fällen handelt es sich hierbei um den Vorstandsvorsitzenden selbst. In sieben Fällen wird die Compliance-Funktion an einen Vorstand übertragen, dessen Ressort sich u. a. mit rechtlichen Aspekten der Unternehmensführung beschäftigt.

Abb. 2: Verantwortung für Compliance im Vorstand, eigene Berechnungen, n = 18 DAX-Unternehmen



3.2 Berichterstattung gegenüber dem Aufsichtsrat

Wichtiger Bestandteil einer Compliance-Organisation sind die Berichtslinien im Unternehmen hinsichtlich Compliance-Verstößen (Pütz 2011, S. 23 ff.). Die nach § 161 AktG für die DAX-Unternehmen geltenden Empfehlungen des Deutsche Corporate Governance Kodex sehen unter Ziffer 3.4 Abs. 2 S. 1 vor, dass der Vorstand den Aufsichtsrat regelmäßig, zeitnah und umfassend über alle für das Unternehmen relevanten Fragen der Compliance informiert. Daneben soll der Aufsichtsrat gemäß Ziffer 5.3.2 einen Prüfungsausschuss einrichten, „der sich insbesondere mit Fragen […] der Compliance […] befasst." Entsprechend dieser Empfehlung des Kodex erwähnt jeder Geschäftsbericht, dass der Prüfungsausschuss sich vom Vorstand hinsichtlich der Compliance-Fragen informieren ließ.

Unterschiede machen die Unternehmen jedoch bei der Frage, ob dem Compliance Officer explizit das Recht eingeräumt wird, auch am Vorstand vorbei an den Aufsichtsrat zu berichten. Sechs Unternehmen geben an, dass die Compliance-Leitung, d. h. die unterhalb des Vorstandes angesiedelten Compliance-Verantwortlichen, allein dem Prüfungsausschuss Bericht erstatten. Ein Unternehmen etabliert im Aufsichtsrat ein eigenes so genanntes Compliance Committee, dem Bericht erstattet wird. Zwölf Unternehmen erstatten an Vorstand und Aufsichtsrat

gemeinsam Bericht. In neun Fällen wird hierbei nur der Prüfungsausschuss, in zwei Fällen nur der Finanzvorstand erwähnt. In acht Unternehmen wird allein dem Vorstand Bericht erstattet. Dabei wird in zwei Fällen nur der Vorstandsvorsitzende erwähnt, in einem Fall nur der Finanzvorstand. Drei Unternehmen geben keine Auskunft über die Berichterstattung.

3.3 Verhaltenskodex und Risikoanalyse

Homogen ist das Bild erneut hinsichtlich der Frage, ob die jeweiligen Compliance-Systeme auch Verhaltenskodizes berücksichtigen. 29 der 30 DAX-Unternehmen geben an, dass Bestandteil ihres CMS ein Verhaltenskodex ist, der oft als Code of Conduct bezeichnet wird. In keinem Unternehmen beschränkt sich die Definition von Compliance auf die bloße Befolgung gesetzlicher Vorgaben (Legalitätsprinzip). Vielmehr umfassen alle CMS auch immer die Einhaltung unternehmenseigener Richtlinien. Die Unternehmen folgen somit erwartungsgemäß der Definition des DCGK in Ziffer 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).“

Eine nähere inhaltliche Betrachtung der Verhaltenskodizes zeigte darüber hinaus, dass diese oftmals besonderes Augenmerk auf den Bereich der personenbezogenen Daten legen. Bei 20 der 30 untersuchten Unternehmen werden personenbezogene Daten in den Verhaltenskodizes besonders berücksichtigt. Dies mag u. a. in den Datenskandalen deutscher Konzernen während der letzten Jahre begründet sein (vgl. Manager Magazin 9/2011, S. 110).

Bei der Einhaltung des Verhaltenskodex durch die Mitarbeiter kommt den Vorgesetzten eine besondere Vorbildfunktion zu (vgl. Kap. I; Pütz 2011, S. 12). Dementsprechend betonen 17 Unternehmen die notwendige Vorbildfunktion leitender Angestellter („Tone from the Top“).

Vor der Implementierung eines CMS sollte eine Risikoanalyse, die die unternehmensspezifischen Risiken ermittelt, durchgeführt werden. Nur so können alle weiteren Maßnahmen genau auf das Unternehmen abgestimmt werden. 16 Unternehmen geben an, eine solche Analyse vorgenommen haben: 5 davon führten eine eigenständige Compliance-Risikoanalyse durch; 11 Unternehmen integrierten die Analyse in die konzernweite (allgemeine) Risikoanalyse (vgl. Kap. VI). Sinnvollerweise fließt die Risikoanalyse auch in die Erstellung des jeweiligen Verhaltenskodex mit ein.

Dass die untersuchten Verhaltenskodizes auf die jeweiligen Unternehmen und eine vorab erfolgte Risikoanalyse abgestimmt sind, konnte indes nur bei weni-

gen Unternehmen eindeutig ausgemacht werden. Zwar betonten beispielsweise Unternehmen im Bereich des Banken- und Kreditwesens spezielle Anti-Geldwäsche-Richtlinien,[89] während Chemie- und Pharmaunternehmen hohen Wert darauf legen, dass bestimmte Umweltstandards befolgt werden. Der überwiegende Teil der Unternehmen verfügt jedoch über einen sehr austauschbaren und allgemein gehaltenen Richtlinienkatalog, aus dem die Compliance-relevanten Risiken des Geschäftsbereiches nicht herauszulesen sind.

3.4 Einzelne Bestandteile eines CMS

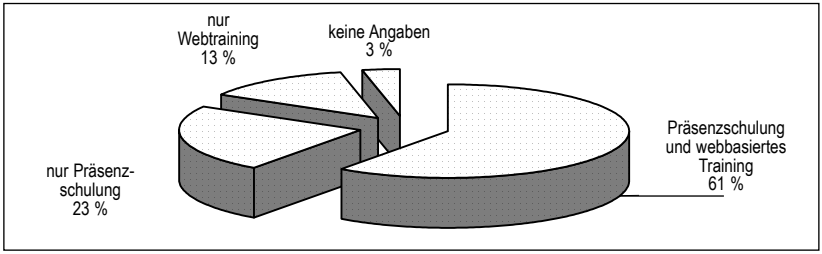
Ein CMS unterteilt sich stets in einzelne Bestandteile. Diese sollten jeweils auf das Unternehmen abgestimmt sein.

3.4.1 Mitarbeiterschulungen

Schulungen für Beschäftigte stellen sich als wichtiger Bestandteil eines CMS heraus. Laut Angaben der 30 DAX-Unternehmen bieten Unternehmen sowohl Präsenzschulungen als auch webbasierte Trainings für ihre Beschäftigten an; 7 Unternehmen führen nur Präsenzschulungen und 4 Unternehmen nur Webtrainings durch (vgl. Abb. 3). Nur ein Unternehmen gibt nicht an, seine Beschäftigten hinsichtlich nationaler Gesetzgebung und unternehmensinterner Richtlinien zu schulen.

89 Vgl. z.B. §§ 31 ff. WpHG, wobei sich die konkrete Ausgestaltung des Compliance-Management-Systems sich aus den Rundschreiben der Bundesanstalt für Finanzdienstleistungsaufsicht MaRisk und MaComp ergibt.

Abb. 3: Art der Qualifizierung, eigene Berechnungen, n = 30 DAX-Unternehmen

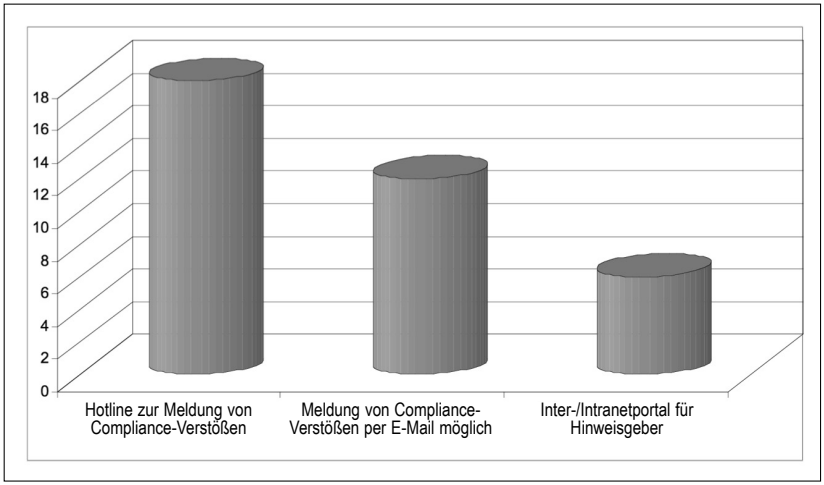


3.4.2 Hinweisgebersystem und Whistleblowing

Neben den Mitarbeiterschulungen als Maßnahmen, um Compliance-Verfehlungen vorzubeugen, umfasst ein CMS einen weiteren Bestandteil: das Erkennen und Aufdecken bereits begangener Verstöße (Pütz 2011, S. 26 f.). In der Praxis nehmen – neben unternehmensinternen Untersuchungen – Hinweisgebersysteme hierbei eine zentrale Rolle ein (vgl. Kap. IV). Dabei sind die Möglichkeiten, Verstöße zu melden, vielfältig: Neben den Meldewegen über den Vorgesetzten oder einen Compliance Officer reicht die Spanne vom Meldeformular im Internet bzw. Intranet („Tell us"-Seiten) über die Einsetzung eines Ombudsmannes, die Nutzung von E-Mail und Post bis zur bekannten Whistleblower-Hotline. Viele Unternehmen nutzen dabei gleich mehrere mögliche Hinweisgebersysteme. Beispielsweise bietet Siemens seinen Beschäftigten an, Compliance-Verstöße alternativ über eine „Tell us"-Seite, einen Ombudsmann, eine interne Bilanzbeschwerdestelle, per E-Mail oder eine Hotline zu melden.

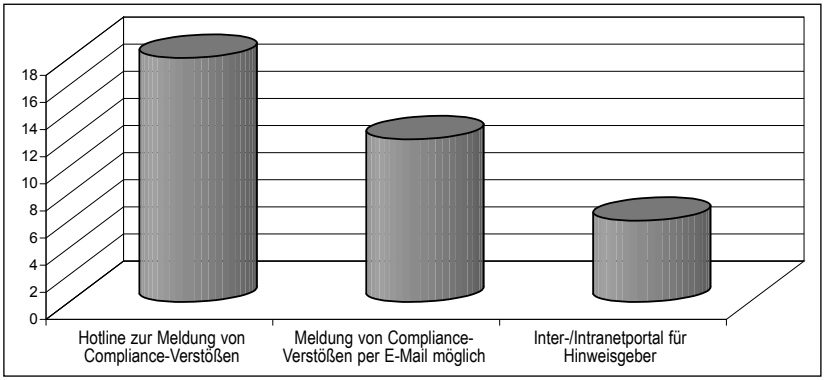
Insbesondere die Möglichkeit, Compliance-Verstöße über eine Hotline zu melden, wird vermehrt angeboten. Eigenen Angaben zufolge stellen 18 Unternehmen eine Hotline für Hinweisgeber zur Verfügung (vgl. Kap. IV). Diese wird in zwei Fällen von externen Anbietern betrieben. 9 Unternehmen verweisen auf die Möglichkeit der Meldung per E-Mail. 6 Unternehmen geben an, ein Internetportal für Hinweisgeber eingerichtet zu haben. Lediglich 2 Unternehmen thematisieren soweit erkennbar kein Hinweisgebersystem (vgl. Abb. 4).

Abb. 4: Möglichkeiten, Verstöße zu melden, eigene Berechnungen, n = 30 DAX-Unternehmen



Bei fast allen Unternehmen ist es möglich, Compliance-Verstöße sanktionsfrei zu melden. Entweder wird die Sanktionsfreiheit durch das Unternehmen garantiert oder das jeweilige Hinweisgebersystem trägt die Voraussetzungen sanktionsfreier Meldungen schon in sich. In 24 Unternehmen ist sichergestellt, dass Beschäftigte sowie Dritte anonym Compliance-Verstöße melden können, indem anonyme und externe Meldewege eingerichtet wurden (vgl. Abb. 5). Bei 13 der genannten 24 Unternehmen besteht mindestens ein Meldeweg über eine externe Stelle. Oftmals fungiert dabei ein externer Rechtsanwalt als Ombudsmann mit Verschwiegenheitspflicht.

Abb. 5: Anonyme Meldung bzw. Meldung an externe Stellen, eigene Berechnungen n = 30 DAX-Unternehmen



Nur 3 Unternehmen formulieren die ausdrückliche Verpflichtung zur Meldung auf ihrer jeweiligen Internetseite. In 5 Unternehmen besteht eine solche Verpflichtung ausdrücklich nicht. Zwei von ihnen schließen ihre Führungskräfte davon wiederum aus und verpflichten sie zur Meldung. Die Möglichkeit, dass auch Externe (Lieferanten, Kunden etc.) einen Compliance-Verstoß melden, besteht lediglich bei 8 Unternehmen.

3.4.3 Unternehmensinterne Untersuchungen

Ernstzunehmenden Meldungen folgen in der Regel entsprechende Untersuchungen. Hierzu nehmen nur 14 Unternehmen überhaupt Stellung: In 9 Unternehmen erfolgen unternehmensinterne Untersuchungen auch präventiv. Sie werden überwiegend von der eigenen Compliance-Abteilung im Unternehmen durchgeführt oder durch eine Zusammenarbeit der Compliance-Abteilung mit der internen Revision. Lediglich zwei Unternehmen ziehen dafür (ausschließlich) ihre Revisionsabteilung heran.

3.4.4 Unternehmensübergreifende Maßnahmen

13 Unternehmen führen nicht nur interne Maßnahmen durch, die sich rein auf das Unternehmen oder den Konzern beziehen. Sie weiten ihre Compliance-Maßnahmen auch auf Geschäftspartner aus. In 7 Fällen wird den Geschäftspartnern zugesichert, dass sie unternehmenseigenen oder internationalen Standards unterliegen. In 6 Fällen werden Kontrollen verschiedener Art durchgeführt.

3.5 Die Rolle des Betriebsrats

Nur drei Unternehmen erwähnen den Betriebsrat im Zusammenhang mit den getroffenen Compliance-Maßnahmen. Ein Unternehmen garantiert, hinsichtlich Compliance-relevanter Untersuchungen die Mitbestimmungsrechte des Betriebsrats zu berücksichtigen. Die beiden anderen Unternehmen geben an, den Betriebsrat in die Erstellung gemeinsamer Grundsätze einzubinden. Im Rahmen der vorliegenden Untersuchung bleibt unklar, worauf dieses Ergebnis zurückzuführen ist: Sind sich die Unternehmen der Rolle des Betriebsrats in einem Compliance-Management-System nicht hinreichend bewusst? Oder gilt seine Einbindung als (rechtliche) Selbstverständlichkeit (vgl. Kap. III)?

3.6 Zertifikate und internationale Standards

Nur 3 Unternehmen betonen ausdrücklich, dass ihr Compliance-Programm zertifiziert wurde. Zweimal wird auf eine Zertifizierung durch Wirtschaftsprüfer hingewiesen, einmal allgemein auf standardisierte Bewertungsverfahren. Auf welche Zertifikate sich die Unternehmen dabei beziehen (DIW, TÜV), ist an keiner Stelle ersichtlich. Da die Zertifizierung von Compliance-Management-Systemen jedoch erst neuerdings möglich ist (vgl. Kap. VII), bleibt abzuwarten, wie sich dieser Bereich entwickelt.

Neben dem eigenen Verhaltenskodex unterwerfen sich die meisten Unternehmen freiwillig den Standards internationaler Organisationen. Laut eigenen Angaben sind 23 Unternehmen Mitglied des Global Compact,[90] der Vereinten Nationen. Acht Unternehmen sind auch Mitglied bei Transparency International. Sieben Unternehmen geben keine Mitgliedschaft in einer der beiden Organisationen an.

90 Global Compact ist eine Initiative der Vereinten Nationen für Unternehmen, die sich verpflichten, ihre Geschäftstätigkeiten und Strategien an zehn universell anerkannten Prinzipien aus den Bereichen Menschenrechte, Arbeitsnormen, Umweltschutz und Korruptionsbekämpfung auszurichten.

4 Fazit

Die DAX-Unternehmen haben ihre Compliance-Management-Systeme unterschiedlich organisiert. Compliance hat interdisziplinäre Funktion und stellt damit auch eine ebensolche Aufgabe dar. Daher liegen die Schwerpunkte in unterschiedlichen Bereichen. Ein einheitliches CMS für alle Unternehmen existiert nicht. Gleichwohl konnte die Untersuchung gewisse Tendenzen ausmachen: Beispielsweise kann ein regelmäßiger Erfahrungsaustausch zwischen Aufsichts- bzw. Betriebsräten aber auch zwischen Managern unterschiedlicher Unternehmen dazu beitragen, ein CMS kontinuierlich zu verbessern.[91]

Die Untersuchungen zeigen auch, dass CMS in Deutschland noch am Anfang steht. Vorausgesetzt, dass der Umfang und die Komplexität der Internet-Darstellungen des CMS dem in der Praxis anzutreffenden System entsprechen, unterscheiden sich die Unternehmen teils erheblich voneinander: In einigen Unternehmen – insbesondere wenn diese in der Vergangenheit schon wegen Compliance-Verstößen negativ auffielen – wird viel Wert auf die Darstellung des vorhandenen Compliance-Systems gelegt. Andere belassen es bei einer Darstellung, die vermutlich dem DCGK geschuldet ist. Gerade weil sich die Compliance von Unternehmen noch entwickelt, werden die Erfahrungen und Entwicklungen der nächsten Zeit, z. B. die zunehmenden Zertifizierungsmöglichkeiten, die CMS verändern. Betriebs- und Aufsichtsräten sollten sich daher kontinuierlich mit dem Thema auseinanderzusetzen.

91 Für die Vertreter der Arbeitnehmer im Aufsichtsrat sei auf die vom Arbeitskreis Mitbestimmung des DGB-Bundesvorstandes verfassten „Grundsätze ordnungsmäßiger Aufsichtsratstätigkeit“ verwiesen: Hans-Böckler-Stiftung, 2011.

Literatur

Hans-Böckler-Stiftung (Hrsg.): Arbeitshilfe für Aufsichtsräte Nr. 10; Grundsätze ordnungsmäßiger Aufsichtsratstätigkeit, Düsseldorf, 2011.

Pütz, Lasse: Compliance – Eine Einführung in die Thematik, Hans-Böckler-Stiftung (Hrsg.), Arbeitshilfe für Aufsichtsräte Nr. 15, Düsseldorf, 2011, www.boeckler.de.

Manager Magazin 9/2011: Der gläserne Kandidat, S. 108-112

Schmidt, Bernd: Compliance in Kapitalgesellschaften, Baden-Baden 2010

Internethinweise

Mehr zu Transparency International, einer weltweit agierende nichtstaatliche Organisation mit Sitz in Berlin, die sich in der nationalen und internationalen volks- und betriebswirtschaftlichen Korruptionsbekämpfung engagiert:
http://www.transparency.de/
www.globalcompact.de
http://www.unglobalcompact.org/docs/languages/german/de-gc-flyer-05.pdf
Zu den rechtlichen Grundlagen des Global Compact im deutschen Recht: http://www.globalcompact.de/fileadmin/PDFs/GC/Rechtliche_Grundlagen_Global_Compact_Prinzipien.pdf

VI Compliance und Risiko-Management – Das geht alle Aufsichtsräte an!

von Alexandra Krieger

1 Trügerische Sicherheit – darum benötigen Unternehmen ein Risikomanagement

Vor 100 Jahren sank die Titanic. Sie kollidierte auf ihrer Jungfernfahrt in der Nacht des 14. April 1912 mit einem Eisberg. Entsetzen löste die Katastrophe nicht nur deshalb aus, weil dabei mehr als 1.400 der rund 2.200 Menschen an Board starben, sondern auch, weil das damals größte Schiff der Welt bis zu seinem Untergang als unsinkbar galt. Das Beispiel zeigt, dass Sicherheit trügerisch ist. Zum einen, weil auch als unwahrscheinlich eingeschätzte Risiken eintreten können. Zum anderen, weil Risiken unterschätzt oder ignoriert werden – im Falle der Titanic starben zahlreiche Passagiere, weil nicht genügend Rettungsboote für eine Evakuierung des Schiffes an Bord waren.

Die meisten Risiken, denen Unternehmen heute ausgesetzt sind, schlagen sich glücklicherweise „nur" in einem finanziellen Schaden nieder. Dabei versteht man unter einem Risiko allgemein die Gefahr einer negativen Abweichung von einem gewünschten oder geplanten Ergebnis.[92] In der Statistik, die Instrumente zur Messung von Risiken zur Verfügung stellt, wird ein Risiko als „die mögliche Schwankungsbreite der Ergebnisse einer unternehmerischen Entscheidung oder unternehmerischen Aktivität" definiert.[93] Je größer diese Schwankungsbreite – also das Risiko –, desto höher ist der mit der Aktivität verknüpfte Vergütungsanspruch dessen, der das Risiko eingeht.[94] Warum die Schwankungsbreite von erwarteten Ergebnissen für das Risiko eine Rolle spielt, veranschaulichen wir an einem einfachen Beispiel aus der Praxis der Aufsichtsratsarbeit.

92 Vgl. Krumnow/Ruhwedel, 2002.
93 Degen u. a., 2011.
94 Ebd.

Beispiel

Dem Aufsichtsrat werden alternativ zwei Projekte mit identischer Investitionssumme zur Zustimmung vorgeschlagen: Investition in einen Staudamm am Amazonas (Projekt 1) oder in einen Staudamm an der Ruhr (Projekt 2). Gewählt werden soll das Projekt mit dem niedrigeren Risiko, also der geringeren Schwankungsbreite der erwarteten Projektergebnisse (Ausschüttungen).

Das Unternehmen ermittelt für beide Projekte jeweils zwei Entwicklungs-Szenarien mit den erwarteten Ergebnissen: ein positives bzw. Best Case-Szenario und ein negatives bzw. Worst Case-Szenario. Man geht davon aus, dass die Eintrittswahrscheinlichkeiten der Best- und Worst Case-Szenarien in beiden Projekten gleich hoch sind und jeweils 50 % betragen. Daraus ermittelt das Unternehmen einen Ergebnis-Erwartungswert, der ebenfalls für beide Projekte gleich hoch ist und 50 TEUR beträgt.

Projekt 1 – Investition in einen Staudamm am Amazonas (in TEUR)

Worst Case-Szenario	Best Case-Szenario	Ergebnis-Erwartungswert
– 100 (Verlust)	+ 200 (Gewinn)	(–100 x 50 %) + (200 x 50 %) = – 50 + 100 = 50

Projekt 2 – Investition in einen Staudamm an der Ruhr (in TEUR)

Worst Case-Szenario	Best Case-Szenario	Ergebnis-Erwartungswert
40 (Gewinn)	60 (Gewinn)	(40 x 50 %) + (60 x 50 %) = 20 + 30 = 50

Die Projekte unterscheiden sich allerdings deutlich in der Schwankungsbreite der erwarteten Ergebnisse, also dem Ergebnisrisiko:

Projekt 1 – Investition in einen Staudamm am Amazonas

Worst Case-Szenario	Best Case-Szenario	Schwankungsbreite Ergebnisse
-100 TEUR (Verlust)	+ 200 TEUR (Gewinn)	300 TEUR

Projekt 2 – Investition in einen Staudamm an der Ruhr

Worst Case-Szenario	Best Case-Szenario	Schwankungsbreite Ergebnisse
40 TEUR	60 TEUR	20 TEUR

Fazit: Unter der Vorgabe, dass der Aufsichtsrat das Projekt mit dem niedrigeren Risiko wählen soll, muss er sich für das Projekt Ruhr entscheiden: Zwar winken beim Amazonas-Projekt größere Ertragschancen (im Best Case-Szenario 200 TEUR Gewinn statt nur 60 TEUR Gewinn im Ruhr-Projekt). Allerdings besteht hier auch das Risiko erheblicher Verluste von 100 TEUR,

während für das Ruhr-Projekt auch im schlechtesten Fall noch ein Gewinn von 40 TEUR vorhergesagt wird. Bei gleichem erwartetem Gesamtergebnis schwanken die Einzelergebnisse im Projekt Amazonas deutlich stärker (300 TEUR im Vergleich zu nur 20 TEUR), was dieses Projekt riskanter macht.

Im Unternehmen werden in der Risikobetrachtung wie im Beispiel neben möglichen Ertragschancen insbesondere potenziell vermögensschädigende Ereignisse betrachtet.[95] Oft sind eingetretene Risiken auch mit einem Image-Schaden verbunden, der sich in der Folge wiederum in finanziellen Einbußen bemerkbar macht.[96] Ein Beispiel aus jüngerer Zeit ist die Explosion auf der Deepwater Horizon im April 2010, einer im Auftrag des Mineralölkonzerns BP betriebenen Ölplattform: Der Unfall führte zu einer schweren Ölpest im Golf von Mexiko, elf Arbeiter starben. BP geriet wegen fehlender Sicherheitsvorkehrungen, vor allem aber wegen seines unprofessionellen Krisenmanagements in die Kritik. Der Aktienkurs brach ein; die Kosten für den Konzern werden auf 40 Mrd. US-$ geschätzt.[97]

Angesichts solcher Erfahrungen versuchen Unternehmen, vor allem existenzbedrohende Risiken mit Hilfe von Risiko-Management-Systemen zu verhindern, bevor die Entwicklung außer Kontrolle geraten kann. Unter einem Risiko-Management-System versteht man Prozesse und Maßnahmen zur Aufdeckung, Bewertung und Steuerung von Risiken.[98] Es soll so genannte Frühwarnindikatoren liefern, wann und wo sich Fehlentwicklungen im Unternehmen andeuten, und damit den Eintritt vor allem bestandsgefährdender Risiken möglichst verhindern.

2 Was ist Compliance-Management? Was ist Risiko-Management?

2.1 Gemeinsamkeiten und Unterschiede

Seit einigen Jahren lässt sich ein Trend beobachten, wonach Unternehmen u. a. aufgrund gewachsener gesetzlicher Anforderungen ihr Risiko-Management differenziert und im Zuge dessen eigenständige Teilsysteme innerhalb des Risiko-Ma-

95 Vgl. Arbeitskreis Externe und Interne Überwachung der Unternehmung (AKEIÜ) der Schmalenbach-Gesellschaft für Betriebswirtschaft e. V., 2010.

96 Vgl. Menzies u. a., 2008.

97 Vgl. o. V., http://www.n-tv.de/wirtschaft/BP-erhaelt-Milliarden-Zahlung-article4543731.html [Zugriff 29.1.2012].

98 Vgl. Romeike, 2004.

nagements entwickelt haben.[99] Ein solches Teilsystem ist das Compliance-Management-System. Compliance übt eine Querschnittsfunktion aus zwischen Revision, Controlling, Rechtsberatung – und eben auch dem Risiko-Management.[100] Wie diese Systeme am effizientesten zusammenwirken können, wird derzeit noch diskutiert.[101] Compliance nimmt aber insofern eine Sonderstellung innerhalb des Risiko-Management-Systems ein, als sie dort ein gewisses autonomes Eigenleben führt. Sie geht nämlich nicht unmittelbar im Risiko-Management auf, um präventiv auch gegen Regelverstöße von Funktionsträgern des Risiko-Managements wirken zu können. Hierzu muss sie von diesen Funktionsträgern und Prozessen unabhängig sein. Im Ergebnis bedeutet das: Die Compliance-Organisation ist zwar ein Teil des Risiko-Management-Systems, bleibt zur Gewährleistung ihrer Unabhängigkeit organisatorisch aber selbständig. Sie ist daher nicht in das Risiko-Management-System eingebunden.[102]

Was konkret unter Compliance bzw. einem CMS zu verstehen ist, darüber schweigt das Gesetz. Das Wort Compliance stammt aus der anglo-amerikanischen Rechtssprache. Es umfasst in einem engen Verständnis die Pflicht, im Einklang mit dem geltenden Recht zu handeln.[103] Im weiteren Sinne geht es um Maßnahmen, mit denen die Einhaltung, Übereinstimmung und Befolgung von gesetzlichen und freiwillig aufgestellten Regeln im Unternehmen sichergestellt werden sollen.[104] Anders gesagt: „Compliant" handelt, „wer eine Gesamtheit organisatorischer Maßnahmen ergreift um sicherzustellen, dass unternehmerisches Handeln mit Gesetzen, Standards und unternehmensspezifischen Regeln – Satzung, Unterschriftenregelungen, Arbeitsanweisungen und Rundschreiben[105] – sowie ethisch-moralischen Grundsätzen übereinstimmt"[106]. Damit ist zwar nicht alles, was Recht und Anstand fordern, eine Frage der Compliance. Aber die Unbestimmtheit des Begriffes lässt den Unternehmen einen großen Ermessensspielraum für die Auslegung und Umsetzung in der Unternehmenspraxis.

Für den Aufsichtsrat lassen sich das Compliance- und das Risiko-Management-System nicht immer einfach voneinander trennen. Beide Systeme sind eng miteinander verzahnt, da – wie in Abschnitt 2 beschrieben – das Compliance-

99 http://www.pwc.de/de/strategie-organisation-prozesse-systeme/unterstutzung-bei-der-erfullung-gesetzlicher-massgaben-compliance.jhtml [Zugriff am 14.11.2011].
100 Vgl. Schefold, 2011.
101 Vgl. Hentschel, 2011.
102 Vgl. Höft, 2011.
103 Vgl. Gebauer/Kleinert, 2010.
104 Vgl. Höft, 2011.
105 Vgl. Vetter, 2008.
106 Vgl. Höft, 2011.

Management ein Teilsystem des Risiko-Management-Systems ist. Trotzdem gibt es Unterschiede: Anders als das Compliance-Management kümmert sich das Risiko-Management nicht nur um Risiken, die aus Regelverstößen entstehen können. Gegenstand des Risiko-Managements sind vielmehr alle zumindest bestandsgefährdenden Risiken, unabhängig von ihrer Entstehungsursache. Wie später noch gezeigt wird, kann das Unternehmen bei der Festlegung seiner Risikostrategie außerdem entscheiden, bestimmte Risiken bewusst in Kauf zu nehmen bzw. sie zumindest bis zu einer selbst definierten Grenze zu dulden. So gehört es zur typischen Praxis im Kreditgeschäft von Banken, das Risiko eines Kreditausfalls bis zu einer bestimmten, statistisch kalkulierten Verlustgrenze „sehenden Auges" einzugehen, sofern die Bank zu der Einschätzung gelangt ist, den Verlust bei Eintritt des Kreditausfalls aus dem Eigenkapital tragen zu können. Demgegenüber kann das Unternehmen ein Compliance-Risiko – die Gefahr eines Verstoßes gegen unternehmensinterne oder gesetzliche Vorschriften – nicht einfach bewusst in Kauf nehmen. Es muss in jedem Fall zumindest Maßnahmen ergreifen, um solche Regelverstöße zu verhindern.

2.2 Wer muss ein Risiko-Management- bzw. ein Compliance-System einrichten? Welche Mindestanforderungen werden an diese Systeme gestellt?

Unternehmerisches Handeln ist immer mit Risiken behaftet. Umso erstaunlicher, dass der Begriff Risiko-Management-(System) erst seit kurzer Zeit im Gesetz verankert ist. Erst 2009 führte ihn der Gesetzgeber mit dem Bilanzrechtsmodernisierungsgesetz (BilMoG)[107] in das Aktiengesetz ein (vgl. § 107 Abs. 3).[108] Bis dahin war dort nur die Pflicht für Aktiengesellschaften zur Einrichtung eines Risikofrüherkennungs-Systems niedergeschrieben. Diese wiederum wurde 1998 mit dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich[109] in § 91 Abs. 2 AktG verankert. Die Pflicht zur Einrichtung eines Risikofrüherkennungs-Systems bezieht sich allerdings nur auf bestandsgefährdende Risiken. Das Unternehmen bzw. die Aktiengesellschaft muss demnach nicht Vorsorge gegen jedes denkbare Risiko treffen, sondern nur gegen solche Gefahren, die das Unternehmen existenziell gefährden und z. B. zu seiner Insolvenz führen können. Anders gesagt:

107 Gesetz zur Modernisierung des Bilanzrechts (Bilanzrechtsmodernisierungsgesetz – BilMoG) vom 25.5.2009, BGBl. I 2009, S. 1.102 ff.

108 Vgl. Holzmayer/Jost, 2011.

109 Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) v. 28.1.1998, BT-Drucks. 13/9712.

Risiken zu überwachen, die nicht das Potenzial zur Bestandsgefährdung haben, liegt im freien Ermessen der Aktiengesellschaft.[110]

Auch das Risikofrüherkennungs-System ist wie das CMS Bestandteil des Risiko-Management-Prozesses und soll mit Hilfe von Frühwarnindikatoren insbesondere bestandsgefährdende Entwicklungen schon in ihrer Entstehungsphase erkennen helfen.[111] Frühwarnindikatoren zeigen negative Trends an, die sich in einer Verschlechterung der wirtschaftlichen Lage niederschlagen können, wenn das Unternehmen diesen Entwicklungen nicht rechtzeitig entgegensteuert. Welche Frühwarnindikatoren eingesetzt werden, hängt vom Unternehmen und seinen spezifischen Risiken ab. „Klassische" Beispiele für Frühwarnindikatoren sind z. B. sinkende Auftragsbestände, steigende Ausschussquoten, eine Zunahme von Kundenbeschwerden und Zahlungsengpässe.

Im April 2005 befragte der Bundesverband Deutscher Unternehmensberater 800 mittelständische Unternehmen zur Bedeutung von Risikofrühwarnindikatoren.[112] Der Verband wollte wissen: Aus welchen Bereichen im Unternehmen stammen die wichtigsten Risikofrühwarnindikatoren? Für die Mehrzahl der Befragten war das eindeutig der Bereich Finanzwirtschaft, gefolgt von der Unternehmensstrategie; auf den hinteren Plätzen lagen Personalrisiken.

Wie ein Unternehmen sein Risiko-Management-System ausgestaltet, liegt in seinem Ermessen und ist sinnvollerweise in Abhängigkeit von der Unternehmensstruktur festzulegen, z. B. von Faktoren wie Größe, Branche, Komplexität, Risikosituation, finanzieller Lage, Kapitalmarktzugang[113] und der Organisation des Unternehmens. In der Praxis vielleicht noch entscheidender: Die Ausgestaltung des Systems hängt auch ab vom „Risiko-Appetit"[114] der Geschäftsführung – davon, ob diese eher risikoscheu, risikoneutral oder risikofreudig agieren will. Diese Flexibilität ist insofern sinnvoll, als jedes Unternehmen (s)einer ganz individuellen und im Zeitablauf außerdem veränderlichen „Risiko-Umgebung" ausgesetzt ist, die u. a. vom Unternehmenszweck, der Branche, den Kunden und Produkten beeinflusst wird.[115] Auch an diesen Rahmenbedingungen muss die Geschäftsführung

110 Vgl. Arbeitskreis Externe und Interne Überwachung der Unternehmen (AKEIÜ) der Schmalenbach-Gesellschaft für Betriebswirtschaft e. V., 2010.

111 Vgl. Holzmayer/Jost, 2011.

112 Bundesverband Deutscher Unternehmensberater, 2005.

113 Vgl. Weber-Rey, 2010; vgl. außerdem Regierungsbegründung zu dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) v. 28.1.1998, BT-Drucks. 13/9712, S. 15; vgl. weiterhin Holzmayer/Jost, 2011.

114 Vgl. Arbeitskreis Externe und Interne Überwachung der Unternehmen (AKEIÜ) der Schmalenbach-Gesellschaft für Betriebswirtschaft e. V., 2010.

115 Vgl. Holzmayer/Jost, 2011.

ihre Risiko-Politik ausrichten. Und: Mit einer größeren Risikobereitschaft sind in der Regel auch größere Ertragschancen verbunden. Welche Risiken ein Unternehmen eingehen will, ist in dieser Hinsicht also auch eine Frage der Chancen-Risiko-Abwägung.

Zudem lassen sich aus dem Strafrecht Organisationspflichten der Geschäftsleitung für die Einrichtung eines Risiko-Management- bzw. Compliance-Systems ableiten. Sie ergeben sich aus dem Ordnungswidrigkeiten-Recht OWiG: Beispielsweise muss die Geschäftsführung gemäß § 130 OWiG Aufsichtsmaßnahmen ergreifen bzw. darf sie zumindest nicht vorsätzlich oder grob fahrlässig unterlassen, um Straftaten und Ordnungswidrigkeiten in seinem Unternehmen zu verhindern.

Unternehmen des Finanzsektors wie Banken, Versicherungen und Pensionsfonds müssen aufgrund ihrer besonderen Bedeutung für die Gesamtwirtschaft zusätzlich aufsichtsrechtliche Vorschriften erfüllen, da hier zu einer ordnungsgemäßen Geschäftsorganisation insbesondere ein angemessenes und wirksames Risiko-Management gehört (§ 25a KWG, § 64a VAG). Für diese Branche konkretisiert die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) als nationale Aufsichtsbehörde die genannten gesetzlichen Vorschriften in den internen Verwaltungsregeln „Mindestanforderungen an das Risiko-Management (MaRisk BA für Kreditinstitute bzw. MaRisk VA für Versicherungsunternehmen)“. D. h. Unternehmen der Finanzbranche haben kein entsprechendes freies Ermessen bezüglich der Ausgestaltung ihrer Risiko-Management-Systeme wie Unternehmen außerhalb dieses Sektors, sondern sind mit wesentlich präziseren Vorschriften der Berufsaufsicht konfrontiert. Zu den erforderlichen Bestandteilen einer „ordnungsgemäßen Geschäftsorganisation“ zählt auch eine Compliance-Organisation.

Für Unternehmen, die nicht aus dem Finanzsektor stammen, bestehen keine solchen ausdrücklichen gesetzlichen Pflichten zur Einrichtung eines Risikofrüherkennungs- bzw. Risiko-Management-Systems. Aber auch für sie lässt sich aus der allgemeinen Sorgfaltspflicht im Rahmen der Geschäftsführung ableiten, dass das Management von Risiken dazu gehört. Zumindest sollten solche Risiken überwacht werden, die den Bestand des Unternehmens gefährden können.[116] Und pragmatisch betrachtet: Ein Unternehmer tut schon in seinem eigenen Interesse gut daran, entsprechende Prozesse einzurichten.

116 Vgl. Schließmann, 2009.

2.3 Wer ist zuständig für das Risiko- und Compliance-Management im Unternehmen?

Die Einrichtung eines Risikofrüherkennungs-Systems i. S. v. § 91 Abs. 2 AktG in der Aktiengesellschaft ist Aufgabe des Vorstands.[117] Anders bei der (monistischen) europäischen Aktiengesellschaft Societas Europaea (SE): Hier trägt der Verwaltungsrat die Verantwortung für das Risikomanagement-System.[118] Für börsennotierte Aktiengesellschaften hebt zudem der Deutsche Corporate Governance Kodex (DCGK) die Einhaltung von Gesetzen und unternehmensinternen Vorschriften als zentrale Aufgabe des Vorstands hervor. In Ziff. 4.1.3 heißt es dazu: „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)". Außerdem muss er für ein angemessenes Risiko-Management und Risiko-Controlling im Unternehmen sorgen (Ziff. 4.1.4). Der Vorstand soll demnach „mit gutem Beispiel vorangehen", im Sinne des viel zitierten „Tone from the Top". Im Umgang mit Risiken und Compliance-Fragen sollte er insgesamt eine Vorbildfunktion wahrnehmen.

In der Praxis ist das Risiko-Management oft beim Chief Financial Officer (CFO) oder beim Chief Executive Officer (CEO) angesiedelt.[119] Ist kein Vorstandsmitglied explizit als Chief Compliance Officer (CCO) benannt, nimmt dessen Funktion im Unternehmen mitunter der Leiter für Controlling/Finanzen oder Risiko-Management wahr. Eine Untersuchung Mitte 2010 zum Stand des Risiko-Managements im DAX 30 ergab, dass bei allen Unternehmen in diesem Börsenindex mindestens ein ständiger zentraler Ansprechpartner für das Risiko-Management benannt ist.[120]

Der Vorstand kann auch einzelne Aufgaben zur Umsetzung und Überwachung des Risiko-Management-/Compliance-Systems an andere Funktionen im Unternehmen delegieren. Doch auch in diesem Falle bleibt er persönlich verantwortlich für die Einrichtung und grundsätzlich Funktionsfähigkeit des Risiko-Management-/Compliance-Systems.

117 Vgl. Behringer, 2011.
118 Vgl. Velte, 2010.
119 Vgl. Arbeitskreis Externe und Interne Überwachung der Unternehmen (AKEIÜ) der Schmalenbach-Gesellschaft für Betriebswirtschaft e. V., 2010.
120 Vgl. Diederichs u. a., 2011.

3 Die Rolle des Aufsichtsrats

3.1 Überwachung des Risiko- und Compliance Management-Systems als Aufgabe des Aufsichtsrats

Der Aufsichtsrat muss die Geschäftsführung überwachen (§ 111 Abs. 1 AktG). Das betrifft alle Leitungsmaßnahmen des Vorstands, d.h. Entscheidungen mit einer gewissen Tragweite für das Unternehmen.[121] Dazu zählen die grundsätzliche Funktionsfähigkeit und Wirksamkeit des Risiko-Management-Systems sowie dementsprechend auch das Compliance-Management, das – wie dargestellt – ein wichtiges Sub-System des Risiko-Management-Systems bildet.[122] Folgerichtig heißt es in Ziff. 3.4 DCGK: „Der Vorstand informiert den Aufsichtsrat regelmäßig, zeitnah und umfassend über alle für das Unternehmen relevanten Fragen der […] Risikolage, des Risiko-Managements und der Compliance. Er geht auf Abweichungen des Geschäftsverlaufs von den aufgestellten Plänen und Zielen unter Angabe von Gründen ein."

Zwar liegt die Verantwortung für die Einrichtung und Funktionsfähigkeit eines Risiko-Management-/Compliance-Systems (mit Ausnahme der monistischen SE) bei der Geschäftsführung. Dennoch haftet daneben der Aufsichtsrat für dessen ordnungsgemäße Organisation: Erkennt das Aufsichtsratsmitglied diesbezüglich Schwächen, muss es auf entsprechende Maßnahmen des Vorstands hinwirken. Es kann sich nicht auf die Verantwortung des Vorstands zurückziehen.

In der Praxis erscheint vielen Aufsichtsratsmitgliedern die Rollenverteilung zwischen Aufsichtsrat und Vorstand bezogen auf das Risiko-/Compliance-Management-System nicht eindeutig. Bei näherem Hinsehen ist sie aber klar geregelt: Der Vorstand muss die Systeme und Prozesse einrichten und – z. B. über eine angemessene interne Revision – ihre Wirksamkeit kontrollieren. Der Aufsichtsrat überwacht, ob der Vorstand diesen Pflichten nachkommt. Insbesondere muss er überprüfen, ob der Vorstand sein organisatorisches Ermessen bezüglich Umfang und Ausgestaltung der Systeme und die Wirksamkeitskontrolle über sie pflichtgemäß ausübt.[123]

Erschwert wird dem Aufsichtsrat seine Aufgabe durch die Tatsache, dass kein für alle Unternehmen einheitlicher Maßstab besteht, wie intensiv er überwachen muss: Er kann generell[124] im dargestellten Zusammenhang sowie insbesondere

121 Vgl. Behringer, 2011
122 Vgl. ebd.
123 Vgl. Probst/Becker, 2009.
124 Vgl. Hentschel, 2011.

für die Überwachung der Wirksamkeit des Compliance-/Risiko-Management-Systems nicht auf ausdrückliche gesetzliche Vorgaben und keinen verbindlichen Maßstab zurückgreifen. Etabliert hat sich aber mittlerweile die Einrichtung eines Prüfungsausschusses des Aufsichtsrats.[125] Seine Verantwortung zur Überwachung des Risiko-bzw. des Compliance-Management-Systems kann der Aufsichtsrat an den Prüfungsausschuss delegieren, jedoch ohne dass er dadurch von seiner Überwachungs-Verantwortung entbunden wäre.[126] Eine entsprechende Empfehlung formuliert auch der DCGK. Gemäß Ziff. 5.3.2. soll der Aufsichtsrat zur Verbesserung der Effizienz seiner Überwachung einen Prüfungsausschuss einrichten, „[…] der sich insbesondere mit Fragen […] des Risiko-Managements und der Compliance, […] befasst".

Seit Inkrafttreten des Bilanzrechtsmodernisierungsgesetztes (BilMoG) 2009 sind kapitalmarktorientierte Unternehmen ohne Aufsichtsrat – also Gesellschaften, die zur Beschaffung von Kapital einen öffentlichen Kapitalmarkt in Anspruch nehmen – sogar verpflichtet, einen Prüfungsausschuss einzurichten. Allerdings befreit auch der Prüfungsausschuss das „einfache" Aufsichtsratsmitglied nicht von seiner Haftung. Vielmehr muss sich das Gremium als Ganzes regelmäßig vom Ausschussvorsitzenden unterrichten lassen, inwieweit das Risiko-/Compliance-Management ordnungsmäßig funktioniert, und sich mit seinem Bericht auseinandersetzen.

Verfügt ein kapitalmarktorientiertes Unternehmen über einen Aufsichtsrat, muss dieser keinen Prüfungsausschuss bilden, um das Risiko-Management-/Compliance-System zu überwachen.[127] In diesen Fällen kann der gesamte Aufsichtsrat die Überwachung der Wirksamkeit des Risiko-Managementsystems und der Compliance wahrnehmen. Die freiwillige Einrichtung eines Prüfungsausschusses bleibt dem Unternehmen aber natürlich unbenommen und hat sich in der Praxis großer Unternehmen zwischenzeitlich als Standard etabliert.

3.2 Überwachungspflichten des Aufsichtsrates im Rahmen des Compliance- und Risiko-Management-Systems

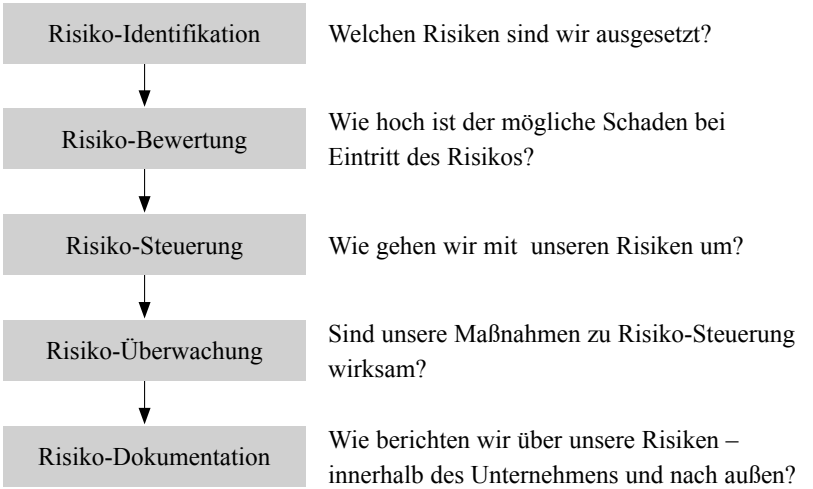
Die zentrale gemeinsame Herausforderung für das Risiko-Management bzw. die Compliance-Organisation innerhalb des Risiko-Managements im Unternehmen lautet: Wie können die Systeme so gestaltet werden, dass Risiken nicht eintreten? Wie können das Risiko- und das Compliance-Management präventiv gegen

125 Vgl. App, 2010.
126 Vgl. Behringer, 2011.
127 Vgl. Velte, 2010.

Risiken wirken – bezogen auf das Compliance-Management demnach gegen die Risiken aus Regelverstößen?

Der Prozess des Risiko-/Compliance-Managements sollte auf einer Risikostrategie fußen, die sich schlüssig aus der Unternehmensstrategie ableitet. In der Risikostrategie dokumentiert das Unternehmen seine Risikopolitik. Diesen Prozess muss die Geschäftsleitung installieren, seine grundsätzliche Funktionsfähigkeit muss der Aufsichtsrat überwachen. Er lässt sich grob in fünf Schritte einteilen:

Abb. 1: Bestandteile des Risiko-Management-Prozesses



Im ersten Schritt, der Risiko-Identifikation, muss die Geschäftsführung aus der Fülle der grundsätzlich möglichen Risiken, die das Unternehmen treffen könnten, die relevanten, folglich die als wesentlich angesehenen möglichen Schäden auswählen. Leitfragen zur Abgrenzung relevanter Risiken lauten beispielsweise wie folgt:

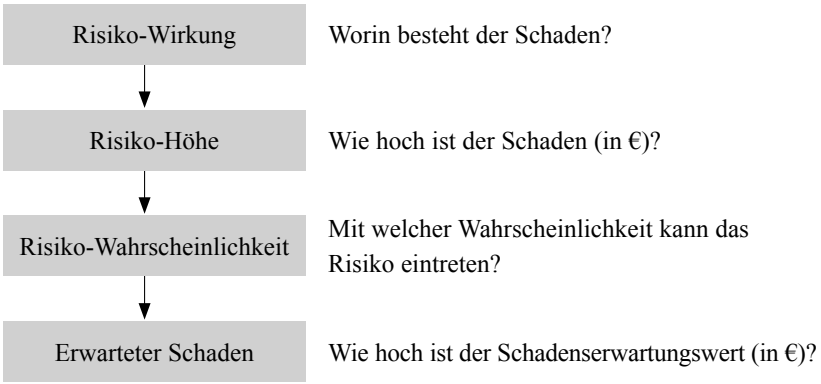
- Führt das Risiko zu einem finanziellen Schaden von mindestens xy EUR (Toleranzschwelle)? Beispiel: Fehlerhafte Softwareprogrammierung führt zu Fehlbuchungen in Höhe von x EUR.
- Führt das Risiko zu einem immateriellen Schaden? Beispiel: Verlust an Reputation wegen Falschberatung.

- Gefährdet das Risiko das Erreichen bestimmter Geschäftsziele? Beispiel: Abwanderung von zentralen Fachkräften verhindert Expansion in ausländische Märkte.
- Beeinträchtigt das Risiko Geschäftsprozesse? Beispiel: Fehlerhaftes Warenwirtschaftssystem führt zu erhöhten Kapitalkosten wegen unnötiger Lagerhaltung.
- Verletzt das Risiko die Ansprüche wichtiger Stakeholder? Beispiel: Fehlerhafte Bewertung von Derivaten im Jahresabschluss einer Bank führt zu Verlusten im Handelsergebnis.
- Verstärkt das Risiko andere Risiken? Beispiel: Führen die aufgrund von Leistungsdruck entstandenen krankheitsbedingten Fehlzeiten der Beschäftigten zu Produktionsausfällen?

In der Praxis existieren zahlreiche Instrumente, um Risiken zu identifizieren. Zu den einfachsten gehören Checklisten mit möglichen Risikoarten und -quellen, aus denen der Nutzer die für das konkrete Unternehmen relevanten auswählen kann. Komplexer sind z. B. Fehlerbaum- und Flow-Chart-Analysen, mit denen Risikoursachen und Abhängigkeiten (Korrelationen) zwischen Einzelrisiken ermittelt werden sollen.[128]

Sind die wesentlichen Risiken ausgemacht, müssen sie in einem zweiten Schritt bewertet werden.

Abb. 2: Die Bewertung von Risiken



128 Vgl. Pampel u. a., 2010.

Bei der Risiko-Bewertung geht es darum, den möglichen Schaden bei Eintritt eines Risikos zu quantifizieren, demnach einen potenziellen Schadenswert („Schadenserwartungswert“) zu ermitteln. Dabei lässt sich die Schadenshöhe im Falle quantifizierbarer Risiken als Produkt aus potenziellem Schaden und Risiko-Eintrittswahrscheinlichkeit berechnen. Hierzu ein vereinfachtes Beispiel.

Beispiel
Ein Unternehmen ermittelt, dass eine Betriebsunterbrechung aufgrund von Stromausfall an einem bestimmten ausländischen Standort mit einer Wahrscheinlichkeit von 20 % eintreten könnte. Pro Tag würde dadurch eine Produktionskapazität von 10 Tonnen wegfallen. Das entspräche einem Gesamtumsatz von 1 Mio. Euro. Der Schadenserwartungswert beträgt in diesem Fall 1 Mio. Euro x 20 % = 200.000 Euro.

Mitunter lässt sich der erwartete Schaden bzw. die Schadenseintrittswahrscheinlichkeit nicht verlässlich quantifizieren. In diesem Fall kann die damit einhergehende Unsicherheit durch pauschale Risikozu- bzw. -abschläge berücksichtigt werden. In der Praxis werden hierzu immer häufiger auch so genannte Sensitivitätsanalysen eingesetzt. Damit soll untersucht werden, wie sich die Veränderung einer Einflussgröße auf das Risiko auswirkt.[129]

Beispiel
Wie viel mehr Zinsen muss das Unternehmen für seine Kredite bezahlen, falls der Kreditzins um 1 %, 2 %, … x % steigt?

Der dritte Schritt besteht in der Risiko-Steuerung: Maßnahmen und Abläufe zum Umgang mit den identifizierten Risiken. Bei der Risikosteuerung geht es zum einen darum, Risiken aktiv zu beeinflussen. Da jedoch

- nicht alle Risiken sich vollständigen ausschließen lassen,
- die Reduzierung oder der Ausschluss von Risiken im Einzelfall für das Unternehmen mit Kosten verbunden sein kann, die aus seiner Sicht inakzeptabel hoch sind,
- das Unternehmen die mit der Übernahme eines Risikos ggf. auch verbundenen Chancen wahrnehmen möchte,

129 Vgl. Pampel/Glabe, 2010.

kann sich das Management zum anderen auch entscheiden, Risiken bewusst zu tragen.[130] Folgende Risiko-Steuerungsstrategien wenden Unternehmen in der Praxis an:

- Risiko-Vermeidung: Bestimmte, als zu riskant definierte Geschäft werden nicht abgeschlossen.
- Risiko-Verminderung: Das Unternehmen versucht, sein Risiko auf ein als tragbar eingeschätztes Maß zu verringern, z. B. durch Risikostreuung („Diversifikation") seiner Aktivitäten in verschiedenen Branchen.
- Risiko-Begrenzung/Risiko-Vorsorge: Das Unternehmen legt Obergrenzen für bestimmte Risiken fest, die im operativen Geschäft nicht überschritten werden dürfen. Werden die Obergrenzen erreicht, dürfen keine weiteren Geschäfte dieser Art abgeschlossen werden.
- Risiko-Abwälzung: Das Unternehmen überträgt Risiken auf Dritte, z. B. indem es eine Versicherung abschließt, ein Sicherungsinstrument kauft (z. B. Abschluss eines Termingeschäfts gegen Wechselkursschwankungen) oder Risiken im Konzernverbund auf mehrere Tochterunternehmen verteilt (z. B. durch Belastung von Konzernvermögen zur Besicherung von Krediten).
- Akzeptanz des Risikos: Risiken, die sich nicht ausschließen lassen oder die bewusst nicht vermieden, vermindert oder abgewälzt werden sollen, werden übernommen. Voraussetzung für eine solche Strategie ist jedoch, dass das Unternehmen über ausreichendes Vermögen verfügt, einen möglichen Schaden bei Eintritt dieser Risiken zu decken.

Die bisher genannten Maßnahmen gehören zu den geschäftsführenden Maßnahmen des Vorstands. Bei der Kontrolle, ob diese Maßnahmen wirksam sind, ist wieder der Aufsichtsrat gefragt. Dieser vierte Schritt ist die Risikoüberwachung. Einige einfache, aber zentrale Leitfragen können für ihn hilfreich sein:

- Werden alle Maßnahmen umgesetzt, und zwar pünktlich, vollständig, sorgfältig und wirtschaftlich?
- Sind die Maßnahmen wirksam, nimmt im Ergebnis das Risiko ab?
- Welchen Erfolg haben die Maßnahmen: Senken sie die Schadenshöhe, die Eintrittswahrscheinlichkeit oder beides?

Der fünfte und letzte Schritt im Risiko-Management-Prozess besteht in der Risiko-Dokumentation: Sie umfasst eine schriftliche Darstellung des Risiko-Management-Systems (oft in Form eines Risiko-Handbuchs) sowie eine Zusammenfassung der Risiko-Lage zu bestimmten Stichtagen. Ziel der Risiko-Dokumentation ist es, a) den Risiko-Verantwortlichen im Unternehmen eine Grundlage für risikobezogene

130 Vgl. Pampel/Glabe, 2010; vgl. außerdem Holzmayer/Jost, 2011.

Entscheidungen zu liefern, und b) diese Entscheidungen nach innen und – in aggregierter Form – nach außen zu dokumentieren.

Im Wesentlichen muss sich der Aufsichtsrat aufgrund dieser Berichterstattung der Geschäftsführung über Risiken ein eigenes Urteil darüber bilden, ob das Risiko-/Compliance-Management-System ordnungsmäßig aufgebaut und grundsätzlich funktionsfähig bzw. wirksam ist. Dazu muss er die Risikosteuerungsprozesse und das interne Reporting analysieren und die Angemessenheit der Bewertung und Kommunikation der wesentlichen aktuellen und künftigen Risiken einschätzen. Konkret bedeutet „Überwachung" in diesem Zusammenhang: Der Aufsichtsrat muss sich vergewissern, ob

- der Vorstand Maßnahmen zur Prävention gegen (Compliance-)Risiken getroffen und folglich einen Risiko-Management-Prozess (wie beschrieben) installiert hat,
- diese Maßnahmen greifen,
- aufgetretene Schwächen beseitigt werden.[131]

Auch hier ist die Ausgestaltung dieser Vorgaben im Einzelnen nicht gesetzlich vorgeschrieben. Dem Aufsichtsrat fehlt damit eine eindeutige Referenz: Er muss – abhängig von der Größe und Komplexität des Unternehmens, der Unternehmensstrategie und dem Risikogehalt des Geschäftsmodells – darüber nach eigenem Ermessen entscheiden, welche Überwachungsmaßnahmen diesen Rahmenbedingungen angemessen sind. Das bedeutet konkret: Der Aufsichtsrat einer Versicherung, deren Geschäftsmodell ja gerade in der Übernahme von Risiken besteht, muss höhere Ansprüche an das Compliance- und Risiko-Managementsystem stellen, als der Aufsichtsrat einer Wohnungsbaugesellschaft. In der Aufsichtspraxis der beiden Unternehmen wird sich das an verschiedenen Stellen niederschlagen: Die Identifikation und Bewertung von Risiken werden in einer Versicherung differenzierter, die inhaltliche und zeitliche Überwachung eingehender und präziser sein als in einer Wohnungsbaugesellschaft. Im Ergebnis braucht ein Aufsichtsrat in einem solchen Unternehmen eine ganz andere, vor allem fachliche Ausstattung als in weniger risikoreichen Unternehmen. Vor diesem Hintergrund sollte der Aufsichtsrat besonderen Wert auf ein aussagefähiges Berichtswesen legen und in diesem Zusammenhang regelmäßig mindestens folgende Informationen von der Geschäftsleitung anfordern:

- Risiko-Inventar: Eine Übersicht der wesentlichen Einzelrisiken des Unternehmens, gestaffelt nach deren prognostizierten Eintrittswahrscheinlichkeiten und

131 Vgl. Herzig/Probst, 2010.

Schadenshöhen samt Wirkungsanalyse (Angaben darüber, welche Erfolgsfaktoren bei Eintritt dieser Risiken bedroht wären).

- Risiko-Tragfähigkeitsrechnung: Eine Darstellung, in welchem Umfang die wesentlichen Unternehmensrisiken durch frei verfügbares Eigenkapital gedeckt sind.

3.3 Wie kann der Aufsichtsrat einschätzen, ob das Risiko-/Compliance-Management funktioniert?

Einen einfachen und in der Praxis leicht umsetzbaren Wirksamkeitstest des Compliance-/Risiko-Management-Systems kann der Aufsichtsrat durch eine Abweichungsanalyse durchführen:

- Lässt sich eine eingetretene Planabweichung auf im Vorhinein bekannte bzw. von der Geschäftsleitung an den Aufsichtsrat berichtete Risiken zurückführen?
- Auf welches der bekannten Risiken ist sie zurückzuführen?

Denn wie schon festgestellt: Ohne Risiko keine Planabweichung. Abgesehen von rechnerischen Fehlern sollten keine Planabweichungen existieren, die nicht auf im Voraus bekannte Risiken zurückgeführt werden können. Insofern stellen Planabweichungen einen wirkungsvollen Weg für den Aufsichtsrat dar Risiken aufzuspüren. Darüber hinaus bieten sie einen Anlass, über Verbesserungsmöglichkeiten bestehender Risiko-Management-/Compliance-Systeme nachzudenken.

Unterstützt wird der Aufsichtsrat bei der Überwachung der Funktionsfähigkeit des Risiko-/Compliance-Management-Systems zumindest in börsennotierten Unternehmen durch den Abschlussprüfer. Letzterer muss hier auch die grundsätzliche Funktionsfähigkeit des Risiko-Managements (und damit der Compliance-Organisation) prüfen (§ 317 Abs. 4 HGB).[132] Nach dem neuen Prüfungsstandard des IDW, EPS 980 – Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen – kann der Aufsichtsrat den Abschlussprüfer auch damit beauftragen, das Compliance-Management des Unternehmens zu prüfen. Allerdings ist das nur ausnahmsweise sinnvoll: Denn der Abschlussprüfer muss nur die formale Ordnungsmäßigkeit feststellen, prüft aber nicht die materielle Funktionsfähigkeit des Compliance-Management-Systems.[133]

In seinem Bestätigungsvermerk muss der Abschlussprüfer darauf eingehen, ob die Risiken der künftigen Entwicklung zutreffend dargestellt sind – insbesondere solche Risiken, die den Fortbestand des Unternehmens gefährden. Zudem muss

132 Vgl. Behringer, 2011.
133 Vgl. Behringer, 2011.

er in diesen Fällen erklären, ob Maßnahmen erforderlich sind, um das interne Überwachungssystem zu verbessern (§ 321 Abs. 4 HGB). Diese so genannte Redepflicht kann für den Aufsichtsrat eine große Hilfe sein, auf Schwächen im Risiko- und Compliance-Management-System aufmerksam zu werden.

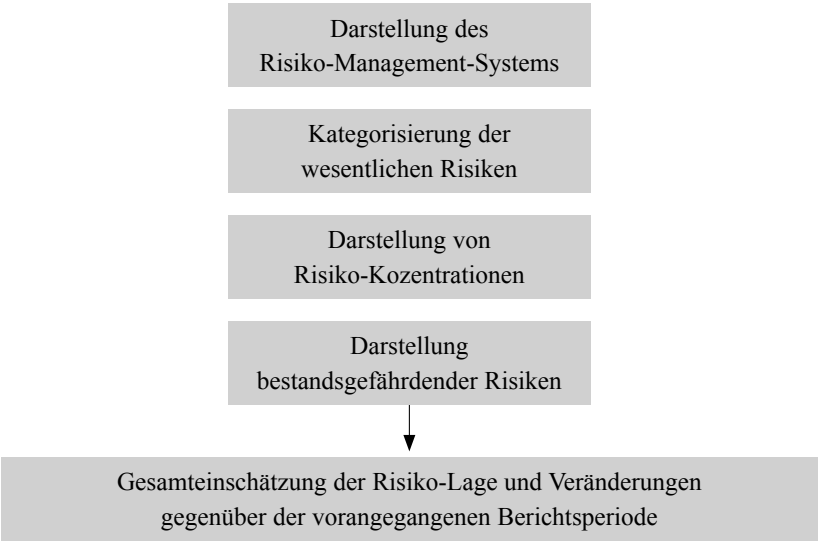
Einen weiteren Berührungspunkt mit der Überwachung des Vorstands bezogen auf das Risiko- bzw. Compliance-Management hat der Aufsichtsrat im Zusammenhang mit der Prüfung und Feststellung des Jahresabschlusses: Denn zumindest bei Kapitalgesellschaften gehört hierzu obligatorisch der Risikobericht im Lagebericht – wenngleich er nicht immer ausdrücklich als solcher bezeichnet wird. Eine weitere Neuerung des KonTraG: Alle Kapitalgesellschaften müssen im Lagebericht die voraussichtliche Entwicklung mit ihren wesentlichen Chancen und Risiken erläutern (§ 289 Abs. 1 S. 4 HGB).[134] Erstmals mussten die Unternehmen die Beschreibung ihres Risiko-Management-Systems in die Lageberichte des Berichtsjahrs 2009 aufnehmen.[135] Die Feststellung des Jahresabschlusses durch den Aufsichtsrat – auf deren Grundlage schließlich die Gewinnverteilung erfolgt – schließt den Lagebericht und damit auch den Risikobericht im Lagebericht ein.

Der Lagebericht muss die voraussichtliche Entwicklung mit ihren wesentlichen Chancen und Risiken aus der Perspektive der Geschäftsleitung beurteilen und erläutern. Dabei muss die Geschäftsleitung die Annahmen angeben, die ihrer Einschätzung zugrunde liegen.

Diese schriftliche Risikoberichterstattung – die interne Dokumentation des Risiko-Managements und die externe Dokumentation im Lagebericht – bildet das Ende der Prozesskette im Risiko-Management-System. Dabei sollte die interne Berichterstattung an den Aufsichtsrat folgende Mindestinhalte umfassen:

134 Vgl. Hoffmann-Becking, 2010.
135 Vgl. App, 2010.

Abb. 3: Mindestbestandteile eines Risikoberichtes an den Aufsichtsrat



Während die interne Risikoberichterstattung oft detailliert ausfällt, ist die Aussagekraft der externen Berichte im Jahresabschluss bzw. Lagebericht aus mehreren Gründen eher ernüchternd gering:

Der Gesetzgeber schreibt dem Unternehmen wie bei der Ausgestaltung der Compliance- und Risiko-Management-Systeme kein einheitliches Berichtsformat vor. Die Berichterstattung muss lediglich den allgemeinen handelsrechtlichen Grundsätzen genügen, u. a. dem „Grundsatz der Vollständigkeit" sowie dem „Grundsatz der Richtigkeit und Willkürfreiheit". Bezogen auf Risiken des Unternehmens bedeutet das beispielsweise: Nicht nur alle buchungspflichtigen Vorfälle müssen erfasst, sondern auch bestehende Risiken erwähnt werden, die sich noch nicht im Vermögens- und Ertragsausweis niedergeschlagen haben.[136] Vereinfacht gesagt darf der Bilanzleser also nicht über das wahre Ausmaß an Risiken getäuscht werden.

Zu berichten sind nur die für das Unternehmen wesentlichen Risiken. Dabei macht sich die Wesentlichkeit an den möglichen Auswirkungen auf die Vermögens-, Finanz- und Ertragslage fest, sofern das entsprechende Risiko eintritt. Auch hier existieren keine gesetzlichen Schwellenwerte, so dass der Aufsichtsrat im Zweifel z. B. die Einschätzung des Wirtschaftsprüfers zu Rate ziehen sollte.

136 Vgl. Coenenberg, 2009.

4 Die Praxis: Welche Risiken stecken in deutschen DAX 30-Konzernen?

Auch wissenschaftliche Untersuchungen belegen die im Durchschnitt geringe Aussagekraft der externen Risikoberichterstattung. Das bestätigt wiederum eine unter den DAX 30-Unternehmen[137] durchgeführte Untersuchung der Jahresabschlüsse des Geschäftsjahres 2002. Diese Untersuchung kommt hinsichtlich der Qualität der Aussagen im Risikobericht zu folgenden Ergebnissen:

- In der Praxis dominiert die „Controller-Perspektive“: eine eher zahlenorientierte Sichtweise mit Schwerpunkt auf leicht quantifizier- und messbaren Risiken.
- Die Unternehmen berichten kaum aussagefähige Informationen zu den Risiken der künftigen Entwicklung.
- Die Aussagen sind oft sehr allgemein gehalten bzw. wären in dieser Form auf viele Unternehmen übertragbar.

Über die Gründe stellt der Autor der Studie folgende Vermutungen an:

- Mangels Verlässlichkeit von Informationen über die potentielle Schadenshöhe und die Eintrittswahrscheinlichkeit von Risiken verzichten Unternehmen auf konkretere Angaben im Risikobericht.
- Gegenseitige Abhängigkeiten zwischen den Risiken lassen sich schwer ermitteln, was meist zu einer Unterlassung entsprechender Aussagen im Risikobericht führt.
- Unternehmen wägen ab zwischen den mit der Veröffentlichung verbundenen möglichen „Kosten“ (z. B. Wettbewerbsnachteile) und dem potentiellen Nutzen (z. B. geringere Kapitalkosten).

Diese Feststellungen treffen auch heute, rund zehn Jahre und eine schwere Finanzkrise später, auf viele Lageberichte noch zu. Aber zumindest im Handelsrecht wurden in den letzten Jahren – u. a. durch das BilMoG – Tendenzen in Richtung erweiterter Angaben mit Bezug zu den Unternehmensrisiken erkennbar.

Langfristig können sich die Unternehmen höheren Transparenzanforderungen der verschiedenen am Unternehmen beteiligten Interessengruppen bezogen auf Unternehmensrisiken nicht entziehen. Das beantwortet auch die Frage, ob Compliance eine Modeerscheinung sein wird: Eine aktuelle Studie zur Wirtschaftskriminalität in deutschen Großunternehmen der Prüfungs- und Beratungsgesellschaft PriceWaterhouseCoopers (PWC) in Kooperation mit der Universität Halle-Wittenberg kommt zu dem Schluss, dass Compliance als Präventionssystem

137 Vgl. Führing, 2004.

zunehmend einen Marktwert erhält. Der nächste Schritt liege in einer Etablierung entsprechender Standards. 40 % der befragten Unternehmen kennen bereits den neuen IDW-Prüfungsstandard PS 980 (vgl. Kap. VII).[138] Das Thema Compliance bleibt demnach mit Sicherheit ganz oben auf der Tagesordnung des Aufsichtsrats.

138 Vgl. Nestler u. a. 2011.

Literatur

App, Jürgen: Überwachung des Internen Kontrollsystems durch den Aufsichtsrat. In: Der Aufsichtsrat, 2010, Heft 10, S. 138 f.

Arbeitskreis Externe und Interne Überwachung von Unternehmen (AKEIÜ) der Schmalenbach-Gesellschaft für Betriebswirtschaft e. V.: Aktuelle Herausforderungen im Risikomanagement – Innovationen und Leitlinien. In: Der Betrieb, 2010, Heft 23, S. 1.245–1.252.

Behringer, Stefan: Aufsichtsrat und Compliance-Management. In: Zeitschrift Risc, Fraud & Compliance (ZRFC), 2011, Heft 3, S. 127–130.

Bundesverband Deutscher Unternehmensberater BDU e. V.: Frühwarnindikatoren für den Mittelstand, Bonn, 2005.

Coenenberg, Adolf G.: Jahresabschluss und Jahresabschlussanalyse, Landsberg, 2009, S. 38 f.

Degen, Beate/Ruhwedel, Peter: Der Aufsichtsrat und das Risikomanagement. In: Der Aufsichtsrat, 2011, Heft 10, S. 138 f.

Diedrichs, Marc/Fricke, Wolfgang/Macke, Sandra: Risiko-Management im DAX 30. In: Der Betrieb, 2011, Heft 26/27, S. 1.461–1.465.

Führing, Meik: Risikoberichterstattung. In: Zeitschrift für Personalforschung, 2004, Heft 2, S. 183–206.

Gebauer, Stefan/Kleinert, Ursula: Risikobereich und Haftung: Compliance in Finanzdienstleistungsunternehmen. In: Krieger/Uwe H. Schneider (Hrsg.): Handbuch Managerhaftung, Köln, 2010, S. 583–612.

Hentschel, Helge: IKS – effizientes Kontrollinstrument für Aufsichtsrat und Management. In: Der Aufsichtsrat, 2011, Heft 10, S. 140 f.

Herzig, Andreas/Probst, Uwe: Compliance, Risiko-Management und internes Kontrollsystem. In: Risikomanager, 2010, Heft 2, S. 16–19.

Höft, Kay: Verknüpfung von Risiko-Management und Compliance im mittelständischen Konzernunternehmen, Hamburg, 2011.

Hoffmann-Becking, Michael: Risiko und Risikosteuerung im Aktienrecht. In: Die Wirtschaftsprüfung, 2010, Sonderheft, S. S103–S105.

Holzmayer, Werner/Jost, Ralph: Risiko-Managementsysteme als Element professioneller Aufsichtsratsarbeit. In: Board, 2011, Heft 3, S. 116–119.

Inderst, Cornelia: Compliance-Organisation in der Praxis. In: Görling, Helmut/Inderst, Krumnow, Jürgen/Gramlich, Ludwig/Lange Thomas A./Dewner, Thomas M. (Hrsg.): Gabler Bank Lexikon, Wiesbaden, 2002, S. 123.

Menzies, Christof/Tüllner, Jörg/Alan, Martin: Compliance Management. In: Zeitschrift Führung und Organisation (zfo), 2008, Heft 3, S. 136.

Nestler, Claudia/Salvenmoser, Steffen/Bussmann, Kai-D.: Wirtschaftskriminalität 2011: Compliance im Aufwind – Zehn Jahre Forschung zur Wirtschaftskriminalität, Frankfurt/Main /Halle, 2011, S. 1–72.

O. V.: BP erhält Milliarden-Zahlung, http://www.n-tv.de [Zugriff 29.1.2012].

Pampel, Jochen R./Glabe, Dietmar: Unternehmensrisiken und Risiko-Management. In: Hauschka, Christoph E. (Hrsg.): Corporate Compliance, München, 2010, S. 84–101.

Probst, Arno/Becker, Carl Christian: Vertrauen ist gut, Kontrolle ist Pflicht: Die Überwachung des Rechnungslegungsprozesses. In: Der Aufsichtsrat, 2009, Heft 12, S. 176 f.

Romeike, Frank: Lexikon Risiko-Management, Köln, 2004, S. 119.

Schefold, Christian: Compliance-Management-Systeme nach deutschem Standard. In: Zeitschrift Risc, Fraud & Compliance (ZRFC), 2011, Heft 5, S. 221–227.

Schließmann, Christoph: Die toten Winkel des Risikomanagements und die Lösung. In: Der Aufsichtsrat, 2009, Heft, S. 140 f.

Velte, Patrick: Der deutsche Prüfungsausschuss nach dem BilMoG und dem VorstAG. In: Zeitschrift für internationale und kapitalmarktorientierte Rechnungslegung (KoR), 2010, Heft 9, S. 429–433.

Vetter, Eberhard: Compliance in der Unternehmenspraxis. In: Wecker, Gregor/van Laak, Hendrik (Hrsg.): Compliance in der Unternehmenspraxis, Wiesbaden, 2008, S. 33–47.

Weber-Rey,Daniela: Compliance und Aufsichtsrat. In: Görling, Helmut/Inderst, Cornelia/Bannenberg, Britta (Hrsg.): Compliance, Heidelberg, 2010, S. 501–640.

Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) v. 28.1.1998, BT-Drucks. 13/9712.

Gesetz zur Modernisierung des Bilanzrechts (Bilanzrechtsmodernisierungsgesetz – BilMoG) vom 25.5.2009, BGBl. I 2009.

VII Externe Prüfung von Compliance-Management-Systemen

von Oliver Emons

1 Wirtschaftskriminalität und Compliance

Das Thema Wirtschaftskriminalität rückt in den letzten Jahren mehr in den Fokus von Justizbehörden und Kartellwächtern. Immer wieder berichten Medien über neue Rechtsverstöße von global agierenden Wirtschaftsunternehmen.

Im Zusammenhang mit Rechtsverstößen haben in den USA vor allem Bilanzskandale für großes Aufsehen gesorgt. Dabei zeigte sich, dass die US-Justizbehörden durch den Rückgriff auf den Foreign Corrupt Practices Act (FCPA) wegen der Zahlung von Bestechungsgeldern[139] 2010 insgesamt 1,5 Milliarden Dollar vor allem gegen europäische Firmen verhängt haben.[140] In der EU haben Unternehmen ebenfalls vermehrt durch Rechtsverstöße auf sich aufmerksam gemacht. Jüngst verfolgten die EU-Kartellwächter Unternehmen im Bereich der Schienentechnik, darunter Tochterunternehmen von Thyssen-Krupp und Voestalpine. Dabei stand der Vorwurf im Raum, Preisabsprachen getroffen zu haben.[141]

Eine Verschärfung von Antikorruptionsgesetzen stellt vor allem der UK Bribery Act dar, ein extraterritorial wirkendes Gesetz. Das britische Gesetz wird auch auf deutsche Unternehmen weitreichende Auswirkungen haben, da es zukünftig nicht mehr nach der Nationalität des Gesetzesbrechers unterscheidet, vielmehr kommt es auf den britischen Bezug an.[142] Als Folge dieses Gesetzes und der zunehmenden Gefahr durch Rechtsverstöße belangt zu werden, stehen Unternehmen vor der Herausforderung, künftig vermehrt Maßnahmen zur Korruptionsverhinderung ergreifen zu müssen. Zur Prävention gegen solche Schäden, führen immer mehr Unternehmen CMS ein. Ein CMS umfasst im Wesentlichen „[…] die Gesamtheit aller […] unternehmerischen Strukturen und Prozesse und Maßnahmen, die darauf gerichtet sind, die rechtlichen und internen Regelungen sowie die Standards zu

139 Vgl. Handelsblatt 2011a.

140 Über den Corruption Practise Act hat die US-Justiz die Möglichkeit, Fälle außerhalb der USA zu verfolgen, auch wenn diese nicht auf dem Boden der USA stattgefunden haben.

141 Vgl. Handelsblatt 2011b.

142 UK Bribery Act: Das Gesetz betrifft neben natürlichen Personen ebenfalls juristische Personen und Personengesellschaften. Es wird somit für international agierende Unternehmen unerlässlich werden, sich Klarheit über die Reichweite des Gesetzes zu verschaffen. Sobald ein hinreichender Geschäftsbezug zu Großbritannien besteht, können aufgrund des Gesetzes auch deutsche Unternehmen von Ermittlungen britischer Strafverfolgungsbehörden betroffen sein.

erfüllen, um auf diese Weise die Geschäfte des Unternehmens, seine Ertrags- und Finanzlage sowie seine Reputation zu verbessern."[143]

Allerdings kann ein CMS keinen vollständigen Schutz gewährleisten. Vielmehr kommt es auf die Umsetzung in der Unternehmenspraxis an. Unternehmen, die sich im Zusammenhang mit dem UK Bribery Act dem Vorwurf der Korruption ausgesetzt sehen, können sich von dem Vorwurf befreien, wenn sie über ausreichende Compliance-Maßnahmen verfügen. Dies ist jedoch nur möglich, wenn die britischen Strafverfolgungsbehörden diese Maßnahmen auch als ausreichend ansehen.[144]

Um die Wirksamkeit ihres CMS zu prüfen bedienen sich Unternehmen zunehmend externer Prüfer, angeregt vom DCGK oder dem Bilanzkontrollgesetz. Es lassen sich weitere Gründe anführen, die für die Prüfung eines Compliance-Management-Systems sprechen können:

- Aufdeckung und Verfolgung von Delikten, die besonders ins Blickfeld der Behörden geraten sind,
- Ausschluss eines möglicherweise unwissentlich begangenen Gesetzesverstoßes,
- Verhinderung hoher Bußgelder, Freiheitsstrafen und Schadensersatzansprüchen,
- Vermeidung von Image- und Reputationsschäden, die im Rahmen von wirtschaftskriminellen Handlungen entstehen könnten,
- Nachweis erfolgreicher Compliance-Maßnahmen, der bei Verhandlungen mit Banken und Versicherungen hilfreich sein kann. Beispielsweise kann der Nachweis eine positive Auswirkung auf das Rating eines Unternehmens haben.

Große Wirtschaftsprüfungsunternehmen haben auf den zunehmenden Bedarf der externen Prüfungen von CMS reagiert und ihre Experten im Bereich Compliance aufgestockt. Der TÜV Rheinland bietet eine Checkliste (Compliance Assessment) an, mit deren Hilfe Manager ihr Compliance-System selber prüfen können, sowie zusätzlich eine TÜV-Zertifizierung des Systems. Darüber hinaus hat auch das Institut der Wirtschaftsprüfer (IDW)[145] im März 2011 auf den zunehmenden Bedarf von CMS-Prüfungen reagiert: Es entwickelte einen eigenen Standard, den Prüfungsstandard IDW PS 980 „Grundsätze ordnungsgemäßer Prüfung vom Compliance Management Systemen". Kernbestandteil der Standards ist eine erstmalige einheitliche Formulierung von Anforderungen an ein wirksames CMS.

143 Vgl. Wente 2011.

144 Vgl. Müller 2011.

145 Das Institut der Wirtschaftsprüfer ist ein Verein, deren Mitglieder sich aus Wirtschaftsprüfern und Wirtschaftsprüfungsgesellschaften zusammensetzen.

Im Folgenden soll Aufsichtsräten und Compliance-Verantwortlichen eine erste Orientierung im Umgang mit der Prüfung von CMS in Bezug auf IDW PS 980 und der TÜV-Zertifizierung geboten werden. Weiterhin werden Vor- und Nachteile sowie Chancen und Risiken diskutiert, die sich im Zusammenhang mit der Prüfung des CMS nach den Standards ergeben können. Die folgende Darstellung liefert zunächst einen Überblick über die Prüfung nach dem IDW-Standard PS 980. Anschließend erfolgt eine kurze Einführung in die Zertifizierung nach dem TÜV-Standard TR CMS 101:2011.

2 IDW PS 980 und TÜV Zertifizierung

2.1 Der IDW Standard PS 980

Der IDW Prüfungsstandard konkretisiert die Anforderungen an eine freiwillige CMS-Prüfung durch Wirtschaftsprüfer. Anwendung findet der Standard seit dem 30.09.2011. Die Grundlage der CMS-Prüfung nach dem Standard ist die Dokumentation des CMS.

Ein CMS umfasst nach Wente (2011) die Gesamtheit aller „[…] unternehmerischen Strukturen, Prozesse und Maßnahmen, die darauf gerichtet sind, die rechtlichen und internen Regelungen sowie Standards zu erfüllen, um auf diese Weise die Geschäfte des Unternehmens, seine Ertrags- und Finanzlage sowie seine Reputation zu wahren und zu verbessern“.[146] Das gesamte CMS wird dabei im Regelfall dokumentiert. Übliche Dokumente, die bei einer Prüfung hinzugezogen werden sollen, sind die Beschreibung des CMS, dokumentierte Compliance-Anforderungen, Rechtsquellen etc. [147] Der IDW-Standard bietet ein Rahmenwerk für die Prüfung des CMS und somit die Möglichkeit, anhand von bestimmten Kriterien die „[…] Konzeption, Implementierung und Wirksamkeit der Grundsätze und Maßnahmen [...]“ einzuschätzen. [148] Der große Vorteil des neuen IDW-Standards soll somit darin bestehen, dass erstmals einheitliche Grundelemente des CMS dem interessierten Publikum vorgestellt werden können. Diese sollten nicht isoliert nebeneinander, sondern vielmehr in wechselseitiger Beziehung miteinander stehen. Man spricht diesbezüglich auch von einer ganzheitlichen Betrachtung.

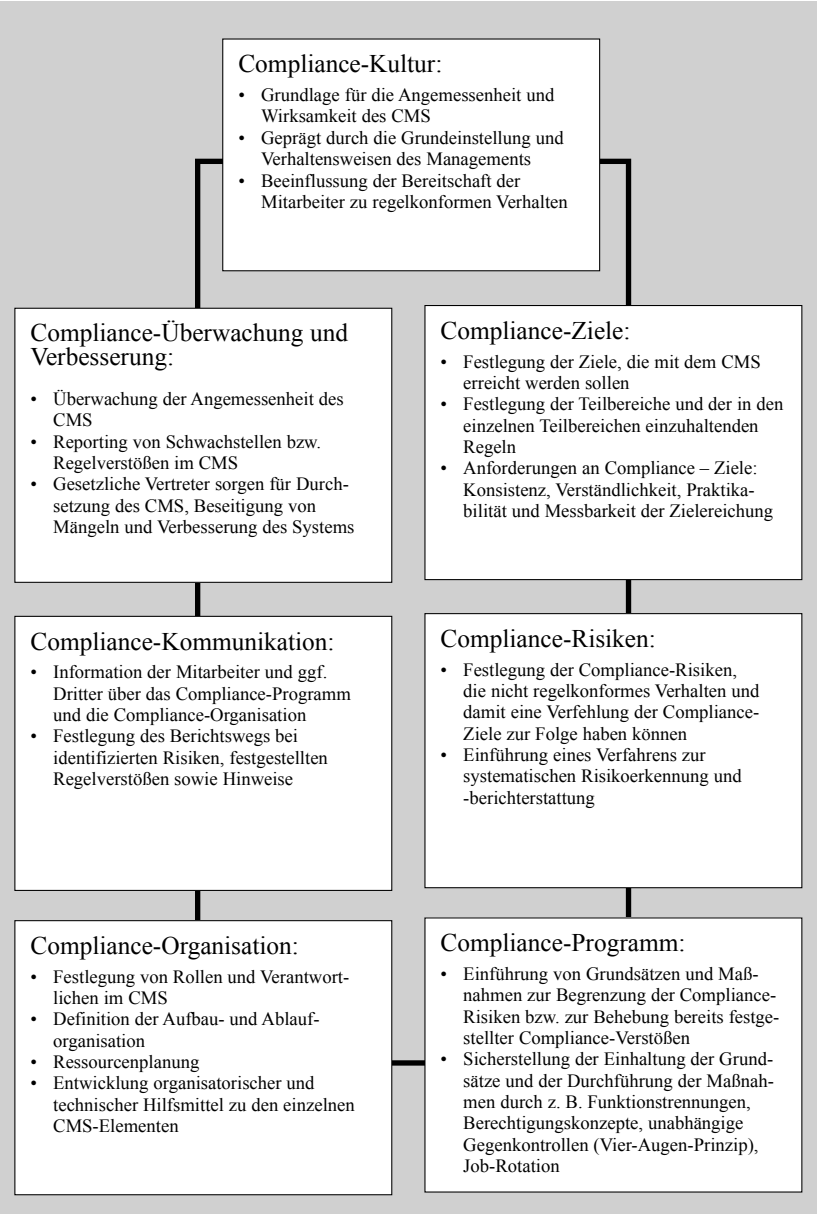
Die folgende Abbildung gibt einen Überblick über die jeweiligen Inhalte der einzelnen Elemente.

146 Vgl. Pütz 2011.

147 Eine Übersicht über die Dokumentation eines CMS findet sich beispielsweise im TÜV-Standard TR CMS 101:2011.

148 Vgl. Wente 2011, S.16

Abb. 1: Die Grundelemente eines CMS nach dem IDW PS 980

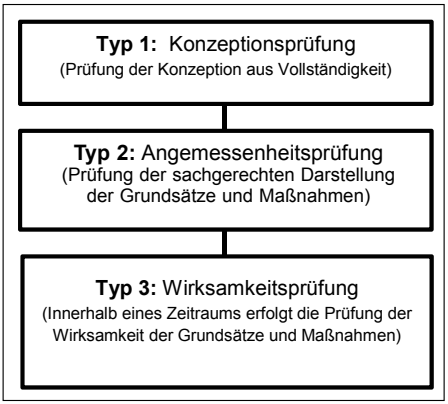


Quelle: Wente 2011, S. 605–606

Im Vorfeld der Prüfung klären die Wirtschaftsprüfer zunächst, ob das gesamte CMS oder einzelne Teilbereiche (Rechtsgebiete, Geschäftsbereiche etc.) untersucht werden sollen. Die CMS-Beschreibung des Unternehmens dient wie bereits erwähnt als Grundlage zur Prüfung nach dem IDW-Standard. Dieser unterscheidet dabei zwischen drei aufeinander aufbauenden Auftragstypen, zwischen denen der Aufsichtsrat bzw. Auftragsnehmer wählen kann. Die anschließende Prüfung erfolgt dem Standard entsprechend durch einen Wirtschaftsprüfer.

Die folgende Abbildung gibt zunächst einen Überblick über die drei Prüfungsarten nach dem IDW-Standard.

Abb. 2: Prüfungsarten nach IDW PS 980



Quelle: angelehnt an Wente (2011)

Typ1: In diesem Prüfungsteil wird insbesondere geprüft, ob auf alle Grundelemente eines CMS eingegangen wurde. Der Fokus liegt auf der Vollständigkeit der CMS-Konzeption.[149]

Typ 2: Im zweiten Auftragstyp geht es um die Prüfung der Maßnahmen und Grundsätze. Dabei soll insbesondere geprüft werden, ob „[…] die Grundsätze und Maßnahmen des CMS in allen wesentlichen Belangen zutreffend dargestellt sind, dass die dargestellten Grundsätze und Maßnahmen in Übereinstimmung mit den angewandten CMS-Grundsätzen geeignet sind, Risiken für wesentliche Regelverstöße mit hinreichender Sicherheit rechtzeitig zu erkennen und Verstöße zu verhindern und dass die Grundsätze

149 Vgl. www.Compliance.net 2011

und Maßnahmen zu einem bestimmten Zeitpunkt implementiert sind".[150] Somit handelt es sich im Wesentlichen um eine Prüfung der Angemessenheit der angewandten CMS-Grundsätze. Dabei sollen insbesondere zwei Fragen beantwortet werden: Sind die Maßnahmen zutreffend dargestellt? Können Risiken und Regelverstöße rechtzeitig erkannt werden?

Typ 3: Ein dritter Auftragstyp untersucht die Wirksamkeit der CMS-Beschreibung innerhalb eines bestimmten Zeitraums. Es handelt sich somit um eine Erweiterung des zweiten Typs, denn die Wirksamkeit eines CMS kann dem Standard nach nur innerhalb eines bestimmten Zeitraums beurteilt werden. In der weiteren Beschreibung des Standards heißt es, dass die beiden anderen Auftragstypen in die Wirksamkeitsprüfung einbezogen werden müssen.

Neben der Darstellung dieser drei Prüfungstypen führt der IDW-Standard Prüfungsanforderungen auf, die zwingend beachtet werden müssen. Dem Prüfer wird beispielsweise demonstriert, wie die Prüfung durchgeführt und dokumentiert werden muss.

2.2 TÜV-Standard TR CMS 101:2011

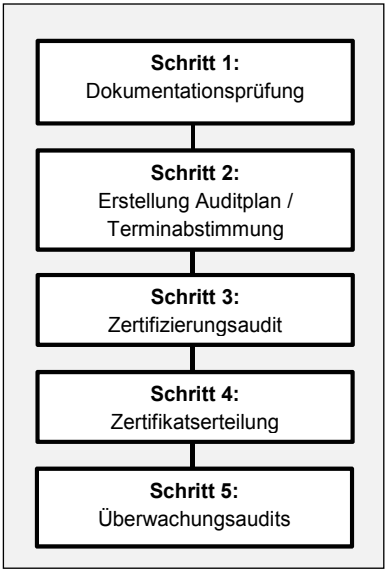
Unternehmen haben mittlerweile auch die Möglichkeit, ihr CMS zertifizieren zu lassen.

In diesem Jahr veröffentlichte der TÜV seinen „Standard für Compliance Management Systeme" (TR CMS 101:2011). Ähnlich dem IDW-Standard bietet der TÜV-Standard einen Überblick über die notwendigen Bestandteile eines CMS.

Die folgende Abbildung gibt einen Überblick über den Ablauf des Prüfungsprozesses mit einer abschließenden Zertifizierung.

150 Vgl. IDW PS 980

Abb. 3: Fünf Schritte zum TÜV-Zertifikat



Quelle: TÜV 2011

Nachdem das System-Audit erfolgreich durchgeführt wurde, kann anschließend die Ausstellung eines Zertifikats angefordert werden. Dieses soll bescheinigen, dass das Unternehmen „ein wirksames CMS aufrechterhält, die Mindestanforderungen an ein CMS erfüllt und in der Lage ist, präventive wie korrigierende Maßnahmen umzusetzen“.[151]

Der TR CMS 101:2011 geht ähnlich wie der IDW PS 980 von einer ganzheitlichen Betrachtung des CMS aus. Der TÜV greift bei seinem Audit ebenfalls auf die bestehende Dokumentation des CMS zurück und prüft, „...inwieweit die Dokumentation des Compliance Managements bereits den Anforderungen des Standards entspricht“[152]. Der TÜV weist in seinen weiteren Ausführungen jedoch deutlich darauf hin, dass die Zertifizierung des CMS keinerlei Aussagen darüber zulässt, ob „tatsächlich alle geltenden Compliance-Anforderung erfüllt“ wurden.[153]

151 Vgl. TR CMS 101:2011, S. 5.
152 Vgl. TÜV 2011: 5 Schritte zum Zertifikat.
153 Ebd.

Weiterhin heißt es dort, dass das „Zertifizierungsaudit[154] […] keine Beratung hinsichtlich der anwendbaren Regeln bzw. Rechtsberatung[…]" darstellt.

Bei der Prüfung wird auf die bestehende Dokumentation des CMS zurückgegriffen. In seinem Artikel weist Modlinger (2011) auf Stärken und Schwächen des TÜV-Standards hin. Positiv wird dort hervorgehoben, dass Compliance als ein ganzheitlicher (nicht unkoordinierter) Ansatz verstanden werden sollte. Andererseits heißt es in diesem Artikel jedoch auch, dass der TÜV-Standard viele Mängel aufweist, die es nahelegen, ihn nur als eine erste Orientierung zum Thema Compliance heranzuziehen. Zu den Mängeln zählen demnach:[155]

- Auf anerkannte internationale Rahmenwerke (wie z. B. die United States Sentencing Guidelines oder das COSO-Modell[156]) werde nicht verwiesen.
- Vorgaben im Standard werden als Muss-Vorgaben formuliert. Dem Unternehmen bliebe fast kein Spielraum für individuelle Entscheidungen.
- Bedingt durch die beabsichtigte Anwendbarkeit für nationale wie internationale Organisationen werde der Standard sehr allgemein gehalten.
- Probleme, die in der Praxis auftreten könnten, würden fast nicht angesprochen.
- Im Zusammenhang mit dem Thema Datenschutz geht der Standard auf Whistleblowing nicht ein.
- Häufig würde auf die Erfahrungen und das Ermessen des Prüfers vertraut.

3 Vor- und Nachteile, Chancen und Risiken der Prüfung bzw. Zertifizierung eines CMS

Einige Nachteile im Zusammenhang mit der Zertifizierung wurden bereits angeführt. Jedes Unternehmen sollte im Vorfeld prüfen bzw. prüfen lassen, ob es ein CMS überhaupt benötigt und ob eine vernünftige Risikoanalyse im Vorfeld durchgeführt wurde.[157] Ein daran anschließender Blick von außen auf das CMS kann auf jeden Fall sinnvoll sein. Hierbei sollten Vor- und Nachteile sowie Chancen und

154 Ein Zertifizierungsaudit ist ein Systemaudit. Dabei wird im Regelfall das gesamte CMS dahingehend geprüft, ob es die Forderungen im zugrunde liegenden Standard erfüllt. Der Ablauf wird in einem Auditplan festgelegt.

155 Modlinger 2011, S. 239–240.

156 COSO-Modell: Kontrollmodell, das der Dokumentation, Gestaltung und Analyse des internen Kontrollsystems dient. Es ist jedoch hauptsächlich auf die Finanzberichterstattung fokussiert. United States Sentencing Guidlines (USSC): Seit 1991 bestehen spezielle Richtlinien, die Sanktionen für Unternehmen im Falle kriminellem Verhalten regeln.

157 Vgl. Goette 2011.

Risiken sorgfältig gegeneinander abgewogen werden. Entscheidet sich ein Unternehmen zur Prüfung seines CMS, sollten sich die Compliance-Verantwortlichen an diesem Prüfungsprozess in jedem Fall konstruktiv beteiligen. Weiterhin ist es wichtig, die individuelle Situation des Unternehmens zu berücksichtigen.

Eine Gefahr im Zusammenhang mit einer Zertifizierung besteht vor allem darin, dass ein Unternehmen sein CMS zertifizieren lässt und keine weiterführende Anpassung vornimmt. Hierbei handelt es sich um eine trügerische Sicherheit, denn eine Erstzertifizierung kann nur der Anfang eines fortlaufenden Prozesses sein, da sich die Risiken in einem Unternehmen ständig ändern können. Eine regelmäßige Anpassung des CMS sowie die regelmäßige externe Prüfung (Audit) sind jedoch auch mit zusätzlichen und teilweise nicht unerheblichen Kosten verbunden. Auch hier müssen Kosten und Nutzen ebenfalls sinnvoll abgewogen werden.

Zu den Vorteilen im Zusammenhang mit dem CMS-Audit zählt, dass Anforderungen (Grundelemente) an ein wirksames CMS formuliert werden und bei der Umsetzung somit ein hohes Maß an Transparenz gewährleistet wird. Sinn des Audits sollte vor allem die Identifikation von Verstößen, Schwachstellen und Verbesserungspotenzialen sein sowie die Reduktion der straf- und haftungsrechtlichen Risiken für die gesetzlichen Vertreter des Unternehmens.[158] Befürworter sehen weiterhin einen Vorteil im einheitlichen Vokabular und dessen Erklärung.[159] Ein anderer Vorteil besteht darin, dass Dokumentation und Zertifizierung ein wirksames Instrument bei Verhandlungen mit Banken und Versicherungen darstellen können (Rating).

Neben Vorteilen und Chancen des CMS-Audits bestehen jedoch auch Nachteile und Risiken. Die Prüfungsgrundlage beim IDW-Standard und dem TÜV-Standard ist die Dokumentation des CMS. Die Prüfung bezieht sich somit auf ein bereits bestehendes CMS. Kritiker des IDW-Standards führen an, dass es zunächst einer Risikoanalyse bedarf und das CMS erst dann auditiert werden sollte.[160] In diesem Zusammenhang verweist der TÜV beispielsweise darauf, dass eine Zertifizierung des CMS Unternehmen nicht vor vorsätzlichem oder grob fahrlässigem Verhalten von Beschäftigten des Unternehmens schützen kann. Eine weitere Kritik richtet sich gegen die ausschließliche Prüfung von Teilbereichen des CMS: Auf diese Weise würde der geprüfte Teil aus dem Gesamtzusammenhang gerissen.[161] Man könnte somit nie wissen, ob der Geschäftspartner tatsächlich „compliant“ sei.[162]

158 Vgl. Wente, 2011, S. 605.
159 Vgl. Neuy 2011.
160 Vgl. Goette 2011.
161 Vgl. Ebd.
162 Vgl. Ebd.

Ein weiteres großes Risiko bestünde darin, dass bei einem CMS-Audit die unternehmensbezogene Individualität des CMS nicht berücksichtigt würde. Die Individualität basiert auf Faktoren wie Branche, Unternehmensgröße, Konzernstruktur, Internationalisierungsgrad oder Börsennotierung, die ebenfalls ständigen Veränderungen unterworfen sein können.[163]

4 Fazit

Vor dem Hintergrund der zunehmenden Verfolgung von Rechtsverstößen durch Strafverfolgungsbehörden und Kartellwächter stellt die Prüfung eines CMS eine sinnvolle, erste Maßnahme dar. Vor- und Nachteile sowie Chancen und Risiken einer solchen Prüfung sind jedoch sorgfältig gegeneinander abzuwägen. Erstmalige einheitliche Compliance-Standards liefert der IDW PS 980, jedoch sind diese nicht verbindlich.

Bei Böttcher (2011) wird diskutiert, wie die zivil- und strafrechtliche Haftung im Zusammenhang mit der Anwendung des IDW PS 980 gestaltet ist und ob die Unternehmensführung nach einer Prüfung von ihrer Haftung befreit ist. Die Autoren kommen zu dem Schluss: „[…] obwohl bislang keine Erfahrungswerte darüber vorliegen, wie Gerichte mit dem IDW PS 980 umgehen werden, ist eine generelle Enthaftungswirkung für die Unternehmen und ihre Geschäftsleiter nicht zu erwarten. Dem Prüfungsstandard fehlt es an juristischer Grundlage, inhaltlicher Vollständigkeit sowie rechtlicher Verbindlichkeit“.[164]

Durch eine Prüfung und Zertifizierung des CMS entfällt weder die Haftung der Geschäftsführung, noch des Aufsichtsrats. Die Kontrollfunktion des Aufsichtsrats bleibt unberührt.

Damit stellt sich für Compliance-Verantwortliche bzw. Geschäftsführer und Aufsichtsräte die Frage, warum das CMS überhaupt überprüft werden sollte, wenn sich doch dadurch die Haftung nicht reduzieren lässt. Dazu lässt sich anführen, dass die Prüfung mögliche Schwächen des eigenen CMS aufdecken soll und kann. Der kritische Blick eines externen Prüfers kann Hinweise liefern, die dem geprüften Unternehmen zumeist verschlossen sind. Somit kann es sein, dass das Unternehmen stärker für das Thema Compliance sensibilisiert wird. In diesem Zusammenhang drängt sich jedoch die Frage auf, ob eine Prüfung und Zertifizierung ausschließlich durch einen Wirtschaftsprüfer erfolgen muss oder ob nicht

163 Vgl. Pütz 2011, S. 15.
164 Vgl. Böttcher 2011.

auch andere Berufsgruppen wie z. B. Unternehmensberater für eine Prüfung des CMS in Frage kommen. In diesen Zusammenhang soll auf den Foreign Corrupt Practices Act verwiesen werden. Dort ist die Prüfung durch einen Wirtschaftsprüfer *nicht* zwingend vorgeschrieben. Das bedeutet im Umkehrschluss, dass auch Unternehmensberater hier eine Prüfung des CMS vornehmen können.

Die externe Prüfung eines CMS nach dem IDW PS 980 und die Zertifizierung z. B. durch den TÜV kann, wie dargestellt wurde, Vorteile bieten. Beispielsweise kann der Nachweis erfolgreicher Compliance-Maßnahmen Verhandlungen mit Banken und Versicherungen positiv beeinflussen. Dabei würde sich der Nachweis eines erfolgreichen und funktionierenden CMS möglicherweise auf das Rating des Unternehmens auswirken. Daneben kann ein funktionierendes CMS ebenfalls dazu beitragen, Image- und Reputationsschäden zu vermeiden, indem Risiken frühzeitig aufgedeckt würden. Compliance-Programme folgen im Regelfall einem ähnlichen System. Ein wichtiger Bestandteil dieses Systems ist die regelmäßige Verbesserung des CMS.[165] Somit kann eine Zertifizierung und Standardisierung des CMS als ein Bestandteil der regelmäßigen Überprüfung der Compliance-Struktur und -Organisation aufgefasst werden.

Da eine externe Prüfung ebenfalls mit teilweise nicht unerheblichen Kosten verbunden ist, sollte ein Unternehmen bzw. der oder die jeweilige Compliance-Verantwortliche vorsichtig Kosten und Nutzen einer solchen Zertifizierung bzw. externen Prüfung abwägen. Dieser Zusammenhang wird insbesondere dann verstärkt, wenn regelmäßige Überprüfungen des CMS erfolgen sollen. Sollten sich die Compliance-Verantwortlichen für eine Prüfung des CMS entscheiden und einen Wirtschaftsprüfer hinzuziehen, müssten die drei genannten Auftragstypen im IDW PS 980 in logischer Folge betrachtet werden. Dabei sollte sich der Konzeptionsprüfung eine Angemessenheitsprüfung anschließen und in jedem Fall durch die Wirksamkeitsprüfung ergänzt werden.

165 Vgl. Pütz 2011, S. 15.

Literatur

Böttcher, Lars: Compliance: Der IDW PS 980 – Keine Lösung für alle (Haftungs-) Fälle! In: Neue Zeitschrift für Gesellschaftsrecht (NZG), 2011, Heft 27, S. 1058.

Compliance.net (2011): Compliance Management, idW Prüfungsstandard EPS 980, www.compliance-net.de/node/89 [Zugriff am 19.01.2012].

Goette, Wulf: Zur Prüfung von Compliance-Management-Systemen, In: Die Wirtschaftsprüfung, 2011, Heft 12, Seite 12

Handelsblatt (2011a): Das Geschäft mit der Angst, 25.08.2011, S. 26.

Handelsblatt (2011b): Kartell in der Schienenbranche vermutet, www.handelsblatt.com/unternehmen/industrie/kartell-in-der-schienenbranche-vermutet/4163068.html. [Zugriff am 19.01.2012].

Pütz, Lasse (Hrsg.): Compliance – Eine Einführung in die Thematik, Hans-Böckler-Stiftung (Hrsg.), Arbeitshilfe für Aufsichtsräte Nr. 15, Düsseldorf, 2011, Download unter www.boeckler.de.

Institut der Wirtschaftsprüfer (IDW) (Hrsg.): IDW PS 980: Grundsätze ordnungsgemäßer Prüfung von Compliance Management Systemen, 2011.

Modlinger, Florian: Der Compliance-Standard des TÜV-Rheinlands. In: Zeitschrift Risk, Fraud & Compliance (ZRFC), 2011, Heft 5, S. 239–240.

Müller, Enno: Antikorruptionsgesetz. Setzt London mit dem UK Bribery Act einen weltweiten Standard? In: Anwalt Aktuell, 2011, Heft 4, S. 18.

Neuy, Michael: Standardisierung des Risikomanagements. In Zeitschrift Risk, Fraud & Compliance (ZRFC), 2011, Heft 1, S. 36–40.

TÜV Rheinland (Hrsg.): TR CMS 101:2011: Standard für Compliance Management Systeme (CMS), 2011.

WeltOnline (2011): Internet lässt Wirtschaftskriminalität explodieren; http://www.welt.de/wirtschaft/article5820627/Internet-laesst-Wirtschaftskriminalitaet-explodieren.html [Zugriff am 19.01.2012].

Wente, Martina: Anmerkungen zum Prüfungsstandard IDW PS 980: Prüfung von Compliance Management Systemen. In: Unternehmenssteuern und Bilanzen (StuB), 2011, Heft 16, S. 603–609.

TUV.com (2011): Compliance Care: Zertifizierung Compliance Management System: www.tuv.com/de/deutschland/gk/managementsysteme/nachhaltigkeit_csr/compliance_management_zertifizierung/compliance_management_zertifizierung.jsp?null [Zugriff am 19.01.2012].

Glossar

Amnestie-Programm

Die Geschäftsführung verzichtet auf mögliche Sanktionen wie z. B. Kündigung, Schadenersatzprozesse. Im Gegenzug verpflichtet sich die andere Seite (z. B. der Mitarbeiter), zur vollständigen Sachverhaltsaufklärung beizutragen.

Da die Geschäftsführung verpflichtet ist, zum Wohle der Gesellschaft zu handeln, bedarf ein Verzicht auf Sanktionen im Regelfall der Einzelfallbeurteilung. Das Aufklärungsinteresse muss das Sanktionsinteresse überwiegen.

Bilanzrechtsmodernisierungsgesetz

Artikelgesetz, durch das schwerpunktmäßig handels- und aktienrechtliche Vorschriften geändert wurden. Mit dem BilMoG wurde eine der größten Reformen des deutschen Handelsrechts umgesetzt, durch die insbesondere das deutsche Handelsgesetzbuch an internationale Rechnungslegungsvorschriften angepasst werden sollte. Das BilMoG konkretisiert bestehende Vorschriften zur Einrichtung, Besetzung und zu den Aufgaben des Prüfungsausschusses.

Business Judgement Rule

Rechtliche Konstruktion, die dem US-amerikanischen Recht entlehnt ist. Die Business Judgment Rule stellt die Geschäftsführung haftungsfrei, wenn sie bei einer Ermessensentscheidung vernünftigerweise annehmen durfte, (auf der Grundlage angemessener Informationen) zum Wohle der Gesellschaft zu handeln. Geregelt ist die Business Judgment Rule in § 93 Aktiengesetz.

Chief Compliance Officer (CCO)

Seine Aufgabe ist es, konzernweit die Einhaltung der Compliance-Regelungen durchzusetzen. Regelmäßig ist er unterhalb der Geschäftsleitung angesiedelt. Er berichtet gewöhnlich an die Geschäftsführung bzw. das zuständige Mitglied für Compliance und ggf. an den Aufsichtsrat oder den Prüfungsausschuss.

Compliance Management System (CMS)

Gesamtheit aller unternehmerischen Strukturen sowie Prozesse und Maßnahmen, die sicherstellen sollen, dass die rechtlichen und internen Regelungen sowie die Standards eingehalten werden. Ziel eines solchen Systems ist regelmäßig die Ge-

schäfte des Unternehmens, seine Ertrags- und Finanzlage sowie seine Reputation zu verbessern oder gesetzlichen Anforderungen gerecht zu werden.

Corporate Social Responsibility

Corporate Social Responsibility beschreibt die Wahrnehmung von gesellschaftlicher Verantwortung durch Unternehmen als freiwillige Beiträge zu einer nachhaltigen Entwicklung. CSR umfasst dabei ökonomische, ökologische und gesellschaftlich/soziale Aspekte. Das schließt auch die Beziehungen eines Unternehmens zu seinen Beschäftigten sowie den Austausch mit relevanten Stakeholdern ein.

COSO-Modell

Committee of Sponsoring Organisations of the Treadway Commission (COSO).

Kontrollmodell, das der Dokumentation, Gestaltung und Analyse des internen Kontrollsystems dient. Es ist jedoch hauptsächlich auf die Finanzberichterstattung fokussiert.

Deutscher Corporate Governance Kodex

Von der Regierungskommission Deutscher Corporate Governance Kodex verabschiedeter Kodex, der die Grundsätze „guter Unternehmensführung" für deutsche börsennotierte Unternehmen regelt (www.corporate-governance-code.de). Nach § 161 AktG müssen der Vorstand und der Aufsichtsrat von börsennotierten Gesellschaften jährlich eine Erklärung (Entsprechenserklärung) abgeben, inwieweit sie den Empfehlungen des Kodex folgen. Für den Fall, dass sie den Empfehlungen nicht folgen, müssen diese Abweichungen begründet werden.

Datenschutz

Schutz des Einzelnen vor dem Missbrauch personenbezogener Daten. Der Einzelne soll davor geschützt werden, dass er durch den Umgang anderer mit seinen personenbezogenen Daten in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt wird. Werden personenbezogene Daten verarbeitet, muss nach dem BDSG zwingend ein Datenschutzbeauftragter bestellt werden.

Effizienzprüfung des Aufsichtsrats

Laut Ziff. 5.6 des DCGK soll der Aufsichtsrat regelmäßig die Effizienz seiner Tätigkeit prüfen. In einer solchen Selbstevaluation sollen Aufsichtsräte die Struk-

turen, Qualität und Wirksamkeit ihrer eigenen Arbeitsweise hinterfragen und gegebenenfalls weiterentwickeln.

Frühwarnindikatoren

Zeigen negative Trends an, die sich in einer Verschlechterung der wirtschaftlichen Lage niederschlagen können, wenn das Unternehmen diesen Entwicklungen nicht rechtzeitig entgegensteuert.

IDW PS 980

Der IDW-Prüfungsstandard IDW PS 980 konkretisiert Anforderungen und Inhalte zur freiwilligen CMS-Prüfung durch Wirtschaftsprüfer. Anwendung findet der Standard seit 30.09.2011.

Insider-Geschäfte

Geschäfte mit Finanzinstrumenten wie z. B. Aktien, bei denen eine Person („Insider“) beruflich oder dienstlich der Allgemeinheit nicht zugängliche Informationen erlangt und diesen Wissensvorsprung nutzt, um sich oder einen Dritten einen Vorteil zu verschaffen.

Mindestanforderungen an das Risiko-Management

Verwaltungsanweisungen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) für die Ausgestaltung des Risikomanagements in deutschen Kreditinstituten bzw. Versicherungsunternehmen.

Prüfungsausschuss

Die Errichtung eines Prüfungsausschusses (oft fälschlicherweise auch als Audit Committee bezeichnet) wird als Teil der Corporate Governance in Ziff. 5.3.2 des DCGK für deutsche Aktiengesellschaften empfohlen. Zu seinen Aufgaben gehört u. a. die Kontrolle eines Compliance-Systems (vgl. § 107 Abs. 3 S. 2 AktG und Ziff. 5.3.2, S.1 des DCGK).

Risiko

Mögliche Schwankungsbreite eines geplanten Ergebnisses; Gefahr einer negativen Abweichung von einem gewünschten oder geplanten Ergebnis.

Risiko-Appetit
Einstellung des Risikoträgers gegenüber einem Risiko. Ausprägung: risikoscheu, risikoneutral oder risikofreudig.

Risiko-Früherkennungs-System
Ein Risiko-Früherkennungs-System ist Bestandteil des Risiko-Management-Prozesses. Es soll mit Hilfe von Frühwarnindikatoren insbesondere bestandsgefährdende Entwicklungen schon in ihrer Entstehungsphase erkennen helfen.

Risikoidentifikation
Auswahl relevanter, als wesentlich für das Unternehmen angesehener Risiken aus den grundsätzlich möglichen Risiken.

Risiko-Management-System
Prozesse und Maßnahmen zur Aufdeckung, Bewertung und Steuerung von Risiken. Ein Risiko-Management-System soll so genannte Frühwarnindikatoren liefern, wann und wo sich Fehlentwicklungen im Unternehmen andeuten, um den Eintritt vor allem bestandsgefährdender Risiken zu verhindern.

Risikostrategie
Sie definiert, wie das Unternehmen mit den für sich identifizierten Risiken umgehen will, also z. B. welche Risiken das Unternehmen zu tragen bereit ist und in welcher Höhe.

Sarbanes-Oxley Act (SOX)
US-Bundesgesetz, das als Reaktion auf Bilanzskandale die Qualität und Transparenz der Berichterstattung von Unternehmen, die den öffentlichen Kapitalmarkt der USA in Anspruch nehmen, verbessern soll. Hinsichtlich Compliance fordert das Gesetz von Unternehmen, dass diese jährlich über den Zustand der unternehmensinternen Finanzkontrolle berichten.

Tone from the Top
(engl. für „Botschaft von oben“) ist das Bekenntnis der Geschäftsführung, dass bestimmte Grundsätze einzuhalten sind. Die Grundsätze, nach denen ein Unternehmen handelt, werden unmissverständlich von den Beschäftigten eingefordert.

Hierzu gehört auch, dass die Geschäftsleitung als Vorbild Compliance im Unternehmen vorlebt und sich an die aufgestellten Regeln hält.

UK Bribery Act 2010

Im April 2010 verabschiedetes britisches und ab 01.07.2011 angewendetes Gesetz sanktioniert vor allem Korruption im Ausland, beschränkt dies aber nicht auf Amtsträger, wie z. B. der US Foreign Corrupt Practices Act. Als wirtschaftsstrafrechtliches Gesetz schafft der UK Bribery Act aktive und passive Bestechungstatbestände für natürliche und juristische Personen. Dabei hat der UK Bribery Act wie auch der US Foreign Corrupt Practices Act einen extraterritorialen Anwendungsbereich. Zu beachten ist: Unternehmen können sich strafbar machen, wenn im Zusammenhang mit ihren Geschäften eine Korruptionstat begangen wird und das jeweilige Unternehmen versäumt hat, die Tat durch adäquate Vorkehrungen zur Bekämpfung von Korruption zu verhindern (z. B. durch ein Compliance-System).

United States Sentencing Guidelines

Seit 1991 bestehen spezielle Richtlinien in den USA, die bei Vorliegen eines kriminellen Verhaltens die Bestrafungen von Unternehmen regeln.

edition der Hans-Böckler-Stiftung
Bisher erschienene Reihentitel ab Band 240

	Bestellnr.	ISBN	Preis / €
Arno Prangenberg, Martin Stahl Steuerliche Grundlagen der Umwandlung von Unternehmen	13240	978-3-86593-133-7	15,00
Samuel Greef, Viktoria Kalass, Wolfgang Schroeder (Hrsg.) Gewerkschaften und die Politik der Erneuerung – Und sie bewegen sich doch	13241	978-3-86593-134-4	28,00
Anne Ames Ursachen und Auswirkungen von Sanktionen nach § 31 SGB II	13242	978-3-86593-135-1	23,00
Ulrich Zachert Tarifeinheit durch Satzungsrecht der Gewerkschaften	13243	978-3-86593-136-8	10,00
Matthias Knuth, Gernot Mühge Von der Kurz-Arbeit zur langfristigen Sicherung von Erwerbsverläufen	13244	978-3-86593-137-5	15,00
Gertrud Hovestadt Institute zur Schulung betrieblicher Arbeitnehmervertreter	13246	978-3-86593-139-9	15,00
Godehard Neumann, Heinz Pfäfflin Metropolregionen zwischen Exzellenzanspruch und regionalem Ausgleich	13247	978-3-86593-140-5	20,00
Judith Beile, Beate Feuchte, Birte Homann Corporate Social Responsibility (CSR) Mitbestimmung	13248	978-3-86593-141-2	20,00
Felix Ekardt Soziale Gerechtigkeit in der Klimapolitik	13249	978-3-86593-142-9	15,00
Kerstin Windhövel, Claudia Funke, Jan-Christian Möller Fortentwicklung der gesetzlichen Rentenversicherung zu einer Erwerbstätigenversicherung	13250	978-3-86593-143-6	24,00
Arno Prangenberg, Martin Stahl, Julia Topp Verrechnungspreise in Konzernen	13251	978-3-86593-144-3	15,00
Martin Albrecht, Hans-Holger Bleß, Ariane Höer, Stefan Loos, Guido Schiffhorst, Carsten Scholz Ausweitung selektivvertraglicher Versorgung	13252	978-3-86593-146-7	23,00
Karl-Heinz Köpke Gesunde Arbeit für alle	13253	978-3-86593-148-1	24,00
Elisabeth Schwabe-Ruck „Zweite Chance“ des Hochschulzugangs?	13254	978-3-86593-149-8	32,00
Enno Balz Finanzmarktregulierung nach der Finanzmarktkrise	13255	978-3-86593-105-4	16,00
Johannes Kirsch, Gernot Mühge Die Organisation der Arbeitsvermittlung auf internen Arbeitsmärkten	13256	978-3-86593-151-1	12,00

	Bestellnr.	ISBN	Preis / €
Kerstin Bolm, Nadine Pieck, Anja Wartmann Betriebliches Gesundheitsmanagement fällt nicht vom Himmel	13257	978-3-86593-152-8	12,00
Christiane Lindecke Neue Arbeitszeiten für (hoch)qualifizierte Angestellte	13258	978-3-86593-153-5	12,00
Jens Ambrasat, Martin Groß, Jakob Tesch, Bernd Wegener Determinanten beruflicher Karrieren unter den Bedingungen flexibilisierter Arbeitsmärkte	13259	978-3-86593-154-2	28,00
Klaus Maack, Jakob Haves, Katrin Schmid, Stefan Stracke Entwicklung und Zukunft der Brauwirtschaft in Deutschland	13260	978-3-86593-155-9	20,00
Klaus Kost, Lienhard Lötscher, Jörg Weingarten Neue und innovative Ansätze zur Regionalentwicklung durch unternehmerische Wirtschaftsförderung	13261	978-3-86593-156-6	25,00
Reingard Zimmer (Hrsg.) Rechtsprobleme der tariflichen Unterbietungskonkurrenz	13262	978-3-86593-157-3	15,00
Uwe Jürgenhake, Cordula Sczesny, Frauke Füsers Berufslaufbahnen von Betriebsratsmitgliedern	13263	978-3-86593-159-7	20,00
Felix Ekhardt Sicherung sozial-ökologischer Standards durch Partizipation	13264	978-3-86593-175-7	15,00
Reingard Zimmer (Hrsg.) Tarifeinheit – Tarifpluralität in Europa	13265	978-3-86593-161-0	18,00
Heiko Geiling, Stephan Meise, Dennis Eversberg Die IG Metall lokal	13266	978-3-86593-162-7	32,00
Michael Gümbel, Sonja Nielbock Die Last der Stereotype	13267	978-3-86593-163-4	28,00
Günter Pochmann, Markus Sendel-Müller, Sven Kischewski, Marion Houben Internationale Bilanzpolitik	13269	978-3-86593-165-8	29,00
Thorsten Ludwig, Holger Seidel, Jochen Tholen Offshore-Windenergie: Perspektiven für den deutschen Schiffbau	13270	978-3-86593-167-2	25,00
Achim Sollanek, Pascal Hansen Bankbilanzen nach IFRS	13271	978-3-86593-169-6	24,00
Heinz-Jürgen Klepzig, Johann Lachhammer, Ulrike Martina Dambmann Going-offshore – Standortverlagerung ins Ausland Handbuch	13275	978-3-86593-163-3	25,00

Ihre Bestellungen senden Sie bitte unter Angabe der Bestellnummern an den Setzkasten oder unter Angabe der ISBN an Ihre Buchhandlung. Ausführliche Informationen zu den einzelnen Bänden können Sie dem aktuellen Gesamtverzeichnis der Buchreihe **edition** entnehmen.

Setzkasten GmbH
Kreuzbergstraße 56
40489 Düsseldorf
Telefax 0211-408 00 90 40
E-Mail mail@setzkasten.de

Hans-Böckler-Stiftung

Die Hans-Böckler-Stiftung ist das Mitbestimmungs-, Forschungs- und Studienförderungswerk des Deutschen Gewerkschaftsbundes. Gegründet wurde sie 1977 aus der Stiftung Mitbestimmung und der Hans-Böckler-Gesellschaft. Die Stiftung wirbt für Mitbestimmung als Gestaltungsprinzip einer demokratischen Gesellschaft und setzt sich dafür ein, die Möglichkeiten der Mitbestimmung zu erweitern.

Mitbestimmungsförderung und -beratung

Die Stiftung informiert und berät Mitglieder von Betriebs- und Personalräten sowie Vertreterinnen und Vertreter von Beschäftigten in Aufsichtsräten. Diese können sich mit Fragen zu Wirtschaft und Recht, Personal- und Sozialwesen, zu Aus- und Weiterbildung an die Stiftung wenden.

Wirtschafts- und Sozialwissenschaftliches Institut (WSI)

Das Wirtschafts- und Sozialwissenschaftliche Institut (WSI) in der Hans-Böckler-Stiftung forscht zu Themen, die für Arbeitnehmerinnen und Arbeitnehmer von Bedeutung sind. Globalisierung, Beschäftigung und institutioneller Wandel, Arbeit, Verteilung und soziale Sicherung sowie Arbeitsbeziehungen und Tarifpolitik sind die Schwerpunkte. Das WSI-Tarifarchiv bietet umfangreiche Dokumentationen und fundierte Auswertungen zu allen Aspekten der Tarifpolitik.

Institut für Makroökonomie und Konjunkturforschung (IMK)

Das Ziel des Instituts für Makroökonomie und Konjunkturforschung (IMK) in der Hans-Böckler-Stiftung ist es, gesamtwirtschaftliche Zusammenhänge zu erforschen und für die wirtschaftspolitische Beratung einzusetzen. Daneben stellt das IMK auf der Basis seiner Forschungs- und Beratungsarbeiten regelmäßig Konjunkturprognosen vor.

Forschungsförderung

Die Forschungsförderung finanziert und koordiniert wissenschaftliche Vorhaben zu sechs Themenschwerpunkten: Erwerbsarbeit im Wandel, Strukturwandel – Innovationen und Beschäftigung, Mitbestimmung im Wandel, Zukunft des Sozialstaates/Sozialpolitik, Bildung für und in der Arbeitswelt sowie Geschichte der Gewerkschaften.

Studienförderung

Als zweitgrößtes Studienförderungswerk der Bundesrepublik trägt die Stiftung dazu bei, soziale Ungleichheit im Bildungswesen zu überwinden. Sie fördert gewerkschaftlich und gesellschaftspolitisch engagierte Studierende und Promovierende mit Stipendien, Bildungsangeboten und der Vermittlung von Praktika. Insbesondere unterstützt sie Absolventinnen und Absolventen des zweiten Bildungsweges.

Öffentlichkeitsarbeit

Mit dem 14tägig erscheinenden Infodienst „Böckler Impuls“ begleitet die Stiftung die aktuellen politischen Debatten in den Themenfeldern Arbeit, Wirtschaft und Soziales. Das Magazin „Mitbestimmung“ und die „WSI-Mitteilungen“ informieren monatlich über Themen aus Arbeitswelt und Wissenschaft.
Mit der Homepage **www.boeckler.de** bietet die Stiftung einen schnellen Zugang zu ihren Veranstaltungen, Publikationen, Beratungsangeboten und Forschungsergebnissen.

Hans-Böckler-Stiftung
Hans-Böckler-Straße 39 Telefon: 02 11/77 78-0
40476 Düsseldorf Telefax: 02 11/77 78-225

www.boeckler.de

Hans **Böckler Stiftung**

Fakten für eine faire Arbeitswelt.

www.boeckler.de

Compliance umfasst alle Maßnahmen, die dazu dienen, dass ein Unternehmen und seine Beschäftigten Recht, Gesetz und Richtlinien des Unternehmens einhalten. Im anschaulichen Überblick werden wesentliche Aspekte, die Betriebs- und Aufsichtsräte im Zusammenhang mit dem Thema Compliance kennen und beachten sollten, erläutert. Dazu gehören: Juristische Grundlagen, die für die Aufgabenwahrnehmung des Aufsichtsrates sowie des Betriebsrates von Bedeutung sind, Entwicklung von betrieblichen Vereinbarungen zur Umsetzung von Whistleblowing-Systemen, das Zusammenspiel von Compliance- und Risiko-Management-Systemen sowie Fragen zur externen Zertifizierung und Prüfung von Compliance-Systemen.

9 783865 931740

ISBN 978-3-86593-174-0
€ 22,00