



## L03 – Compliance-Leitfaden für den Aufsichtsrat

Autoren: Arbeitskreis Aufsichtsrat und Compliance

**DICO**

Deutsches Institut für Compliance



Stand: März 2015

**Disclaimer**

DICO Leitlinien richten sich an Compliance-Praktiker. Sie sollen einen Einstieg in das Thema erleichtern und einen Überblick verschaffen. Es wird daher bewusst darauf verzichtet, juristische Sonderfälle und Ausnahmeregelungen aufzuzeigen.

DICO Leitlinien bieten dem geeigneten Leser praxistaugliche und umsetzbare Empfehlungen für ausgewählte Compliance-Themen. Mit Veröffentlichung einer Leitlinie soll zugleich eine Diskussion zum jeweiligen Themenkreis angestoßen werden mit dem Ziel, darauf aufbauend einen Standard zu entwickeln, der von Compliance-Praktikern anerkannt wird.

Senden Sie Ihre Anregungen und Beiträge an [Leitlinien@dico-ev.de](mailto:Leitlinien@dico-ev.de). Wir freuen uns auf eine lebhaftige Diskussion und bedanken uns für Ihre konstruktive Unterstützung!



VORWORT	5
EINLEITUNG	6
1. PFLICHT ZU COMPLIANCE UND AUSGESTALTUNG EINES COMPLIANCE SYSTEMS	7
1.1 „Ob“	
1.2 „Wie“: Ausgestaltung eines Compliance Systems	
1.2.1 Vorgaben gemäß MaComp-Rundschreiben 4/2010	
1.2.2 Ausgestaltungsüberlegungen im Allgemeinen	
1.2.2.1 Keine „One-size-fits-all“-Lösung	
1.2.2.2 Allgemeiner Mindeststandard	
2. FRAGENKATALOGE	13
3. COMPLIANCEVERANTWORTUNG IM UNTERNEHMEN	17
3.1 Geschäftsleitung	
3.1.1 Allgemeines	
3.1.2 Business Judgement Rule und Vorgehensweise	
3.1.3 Gesamtverantwortung und Delegation	
3.2 Der Aufsichtsrat und seine grundsätzliche Verantwortung für Compliance	
3.2.1 Kontrollpflichten hinsichtlich Compliance	
3.2.2 Überwachungspflicht	
3.2.3 Beratungsfunktion	
3.2.4 Personalkompetenz	
3.2.5 Informationsgrundlage: Informationsrechte und Prüfungspflichten	
3.2.6 Reaktionsmöglichkeiten	
3.2.7 Haftung von Aufsichtsratsmitgliedern	
3.2.8 Interne Aufsichtsrat-Compliance	
4. GRUNDSÄTZLICHE COMPLIANCE-MASSNAHMEN	29
4.1 Compliance Management-System (CMS)	
4.2 Der Compliance Officer/Compliance-Beauftragte (CCO)	
4.3 Compliance-Richtlinie; Information; Hilfestellungen	
4.4 Kommunikation und Schulungen	
4.5 Hinweisgebersysteme (Whistleblower)	
5. WICHTIGE BEGRIFFE IM ZUSAMMENHANG MIT COMPLIANCE	34
LITERATURAUSWAHL	37

## Vorwort

Compliance, die organisatorische Einhaltung von selbst und fremdgesetzten Regeln, wird mittlerweile zutreffend als zwingender Bestandteil guter Unternehmensführung angesehen, dessen Miss- oder Nichtbeachtung auch zur persönlichen Haftung der verantwortlichen Personen führen kann. Entsprechend viel Aufmerksamkeit hat dieses Thema in der jüngeren Vergangenheit erfahren.

Als Bestandteil der Legalitätspflicht, d.h. der Pflicht dafür zu sorgen, dass das Unternehmen und seine Angestellten Recht und Gesetz einhalten, wird Compliance häufig nur als Verantwortung der Geschäftsleitung wahrgenommen. Compliance und Compliance-Verantwortlichkeit richtet sich aber nicht nur an die Geschäftsleitung, sondern ist auch integraler Bestandteil der Arbeit im Aufsichtsrat, der sämtliche Bestandteile der Geschäftsführung – und damit auch der Compliance – zu überwachen hat.

Der vorliegende Leitfaden soll eine erste Orientierung bieten, wie sich dem Thema Compliance aus Sicht des Aufsichtsrats genähert werden kann und praktische Hilfestellung bei der Einarbeitung in das Thema Compliance aus der Aufsichtsratsperspektive bieten.

Der Leitfaden richtet sich insbesondere an Aufsichtsratsmitglieder, die weder besondere Vorkenntnisse im Bereich Compliance besitzen, noch eine herausgehobene Stellung in Bezug zum Compliance-System innehaben, wie etwa die Mitglieder eines Prüfungsausschusses. Er konzentriert sich vielmehr auf solche Fragen, die sich jedes Aufsichtsratsmitglied zum Thema Compliance stellt oder stellen sollte.

Dementsprechend wurde auf die Darstellung rechtstheoretischer Begründungen und Meinungsstreitigkeiten soweit wie möglich verzichtet bzw. dort, wo eine Darstellung unerlässlich scheint, diese entsprechend vereinfacht. Der Leitfaden erhebt auch keinen Anspruch auf Vollständigkeit, sondern konzentriert sich auf solche Compliance-Vorgaben, wie sie für die meisten Unternehmen von praktischer Bedeutung sind. Zur Ergänzung und Vertiefung sei auf die Literaturliste im Anhang zu diesem Leitfaden verwiesen.

Im Folgenden wird nach einer kurzen Einführung zunächst die Bedeutung von Compliance als elementarer Bestandteil guter Corporate Governance kurz erläutert und ein kurzer thematischer Überblick gegeben. Anschließend zeigen zwei Fragenkataloge beispielhaft die Inhalte auf, mit denen sich der Aufsichtsrat zu Fragen der unternehmensspezifischen Compliance auseinandersetzen sollte, wobei diese zum einen allgemein und zum anderen auf die Inhalte der Aufsichtsratsarbeit zugeschnitten sind. In einem dritten Teil werden die Inhalte und Anforderungen an Compliance und deren systematische Umsetzung vertiefend erläutert. Den Abschluss bilden ein Glossar sowie weiterführende Literaturhinweise. »

# Einleitung

Unternehmen sind verpflichtet, Rechtsverstöße ihrer Mitarbeiter zu verhindern. Geschäftsführungsbefugte Gesellschafter, gesetzliche Vertreter und Organe eines Unternehmens müssen die erforderlichen und zumutbaren Aufsichtsmaßnahmen ergreifen, damit die geltenden Gesetze eingehalten werden.

Rechtsverstöße von Wirtschaftsunternehmen finden weltweit eine immer größere Aufmerksamkeit. Insbesondere die Themen Wirtschaftskriminalität, (Arbeitnehmer-) Datenschutz und Korruption rücken stärker in das öffentliche Bewusstsein.<sup>1</sup> Die sich hieraus unter anderem ergebende Zunahme von Haftungsrisiken, (indirekten) Schadenersatzforderungen und Imageschäden führen dazu, dass es für das Unternehmen und dessen Management an Bedeutung gewinnt, sich im Einklang mit gesetzlichen Vorschriften zu verhalten. Unter dem englischen Begriff „Compliance“ hat sich dieser Problembereich in der jüngeren Vergangenheit begrifflich in der deutschen Rechtssprache etabliert.

„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).“<sup>2</sup> Die hinter Compliance stehende Absicht, Regelverstöße zu vermeiden und ein unternehmenseigenes Wertesystem zu etablieren, ist damit ein notwendiger Bestandteil „guter Corporate Governance“. »

---

<sup>1</sup> Man denke nur an die Korruptions-, Datenschutz- oder Finanzskandale der jüngsten Zeit bei Firmen wie Siemens, Daimler, MAN, der Deutschen Bahn, der Deutschen Telekom, Bilfinger-Berger, Lidl oder VW.

<sup>2</sup> Ziffer 4.1.3 Deutscher Corporate Governance Kodex.

## Über DICO:

DICO – Deutsches Institut für Compliance e.V. wurde im November 2012 in Berlin auf Betreiben führender Compliance-Praktiker und -Experten gegründet und hat als gemeinnütziger Verein Mitglieder aus allen Branchen in Deutschland, darunter namhafte DAX-Unternehmen, Wirtschaftsprüfungs- und Beratungsgesellschaften sowie aus der Wissenschaft. DICO versteht sich als unabhängiges interdisziplinäres Netzwerk für den Austausch zwischen Wirtschaft, Wissenschaft, Politik und Verwaltung und sieht sich als zentrales Forum für die konsequente und praxisbezogene Förderung und Weiterentwicklung von Compliance in Deutschland.

DICO fördert Compliance in Deutschland, definiert in diesem Bereich Mindeststandards, begleitet Gesetzgebungsvorhaben und unterstützt zugleich die praktische Compliance-Arbeit in privaten und öffentlichen Unternehmen, fördert Aus- und Weiterbildung und entwickelt Qualitäts- sowie Verfahrensstandards.



DICO – Deutsches Institut für Compliance

Chausseestraße 13

D-10115 Berlin

[info@dico-ev.de](mailto:info@dico-ev.de)

[www.dico-ev.de](http://www.dico-ev.de)

