DICO Leitlinie

L03 – Compliance-Leitfaden für den Aufsichtsrat

Autoren: Arbeitskreis Aufsichtsrat und Compliance

DICO
Deutsches Institut für Compliance

AdAR
Arbeitskreis deutscher Aufsichtsrat e.V.

Stand: April 2020

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 geneigten 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. Wir freuen uns auf eine lebhafte Diskussion und bedanken uns für Ihre konstruktive Unterstützung!

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 beziehungsweise, soweit vorhanden, des Compliance Officers oder Compliance-Beauftragten wahrgenommen. Compliance und Compliance-Verantwortlichkeit richten sich aber nicht nur an die Geschäftsleitung, sondern sind auch integraler Bestandteil der Arbeit im Aufsichtsrat, der sämtliche Bestandteile der Geschäftsführung – und damit auch die Vorgehensweise der Geschäftsführung im Einklang mit Recht und Gesetz – zu überwachen hat. Andernfalls droht dem Aufsichtsrat im schlimmsten Fall eine eigene Haftung aufgrund eines Organisations- und Überwachungsverschuldens.

Der vorliegende Leitfaden soll eine erste Orientierung bieten, wie der Aufsichtsrat seiner Kontrollfunktion in Zusammenhang mit Compliance-rechtlichen Vorgaben gerecht werden kann, und praktische Hilfestellung bei der Einarbeitung in das Thema Compliance aus der Aufsichtsratsperspektive bieten. In Fortschreibung des DICO Leitfadens aus dem Jahr 2015 sollen aktuelle Impulse und Entwicklungen im Kontext der Compliance-Arbeit des Aufsichtsrats aufgegriffen werden. So wurde das Compliance-rechtliche Pflichtenprogramm für Aufsichtsräte in jüngster Vergangenheit durch verschiedene Urteile, aber auch durch Anpassung der rechtlichen Rahmenbedingungen modifiziert. Anpassungsbedarf folgt daneben aus der zunehmenden Digitalisierung in fast allen Unternehmensbereichen. Hieraus können sich Potentiale und Anreize zum Aufsetzen und Optimieren eines Compliance-Management-Systems ergeben, welche vom Aufsichtsrat eingeschätzt und gegebenenfalls in Zusammenarbeit mit dem Vorstand umgesetzt werden müssen. Gleichzeitig steigen aber auch die Risiken. Gesteigerte Risiken ergeben sich etwa im Bereich der Cyberkriminalität sowie infolge des verstärkten investigativen Journalismus und des wachsenden Knowhows und der Eingriffsmöglichkeiten bei den Staatsanwaltschaften.

Der Leitfaden richtet sich insbesondere an Aufsichtsratsmitglieder, die weder besondere Vorkenntnisse im Bereich Compliance besitzen noch über eine herausgehobene Verantwortung im Compliance-Management-System verfügen, wie etwa die Mitglieder eines Prüfungsausschusses. Er konzentriert sich vielmehr auf solche Fragen, die sich jedes Aufsichtsratsmitglied zum Thema Compliance und seiner damit in Zusammenhang stehenden Kontrollfunktion 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 erläutert und ein thematischer Überblick gegeben (1.). Anschließend zeigen zwei Fragenkataloge beispielhaft die Inhalte auf, mit denen sich der Aufsichtsrat zu Fragen der unternehmensspezifischen Compliance auseinandersetzen sollte (2.). In einem dritten Teil werden die Inhalte und Compliance-rechtlichen Anforderungen an ein Unternehmen und deren systematische Umsetzung vertiefend erläutert (3.). Unter Ziffer 4 werden sodann die in der Praxis weitverbreiteten Bestandteile eines Compliance-Management-Systems aufgezeigt. Den Abschluss bilden ein Glossar (5.) sowie weiterführende Literaturhinweise.

Der Leitfaden berücksichtigt immer wieder den im September 2019 bekannt gewordenen Entwurf eines Gesetzes zur Bekämpfung von Unternehmenskriminalität (Verbandssanktionengesetz) und zeigt auf, welche Auswirkungen auf die Praxis eine Umsetzung des Entwurfes in geltendes Recht hätte. Es ist jedoch davon auszugehen, dass es im Zuge der Umsetzung des Verbandssanktionengesetzes noch zu Änderungen an diesem kommt, so dass sämtliche Ausführungen hierzu nur eine Tendenz zeigen bzw. eine Momentaufnahme sein können. »

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 (insb. Korruption), Kartellrecht und (Arbeitnehmer-) Datenschutz rücken stärker in das öffentliche Bewusstsein.[1] Die sich hieraus unter anderem ergebende Zunahme von Haftungsrisiken, (indirekten) Schadenersatzforderungen und Imageschäden führt dazu, dass es für das Unternehmen und dessen Management an Bedeutung gewinnt, sich im Einklang mit gesetzlichen Vorschriften zu verhalten. Unter dem Begriff der „Compliance" hat sich dieses Themenfeld in der jüngeren Vergangenheit in der deutschen Rechtssprache etabliert.

Gemäß dem Deutschen Corporate Governance Kodex (DCGK) hat der Vorstand für die Einhaltung der gesetzlichen Bestimmungen und der internen Richtlinien zu sorgen und wirkt auf deren Beachtung im Unternehmen hin (Compliance).[2] Die hinter Compliance stehende Absicht, Regelverstöße zu vermeiden und ein unternehmenseigenes Wertesystem zu etablieren, ist damit ein notwendiger Bestandteil „guter Corporate Governance". »

1 Man denke nur an die Korruptions-, Datenschutz- oder Finanzskandale der jüngsten Zeit bei Firmen wie der Deutschen Bank, Bilfinger, VW oder Steinhoff.

2 Grundsatz 5 DCGK, der Ziffer 4.1.3. S. 1, DCGK leicht modifiziert.

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

www.dico-ev.de