Aufsichtsrats-Compliance

Die Herausforderung der umfassenden Pflichterfüllung

Dr. Michael Beyer, Geschäftsführender Gesellschafter, Feingeist GmbH, Beratungsgesellschaft für Aufsichtsräte

Ab wann ist man als Aufsichtsrat individuell oder kollektiv „compliant"? Was ist darunter genau zu verstehen und wie lassen sich im Sinne einer verantwortungsvollen Grenzziehung Themen und Aufgaben definieren, derer man sich anzunehmen hat und eben die Fragestellungen ableiten, von deren Würdigung bzw. Bearbeitung ruhigen Gewissens abgesehen werden kann? In dem Beitrag geht der Autor auf die neuen Anforderungen des DCGK ein und erläutert, warum die umfassende Pflichterfüllung im Zusammenhang mit Compliance Aufsichtsräte vor eine große und interdisziplinäre Herausforderung stellt.

I. Aktualität

Der Begriff „Compliance" ist inzwischen aus dem Tagesgeschäft von Aufsichtsräten kaum noch wegzudenken. Häufig ist jedoch seine Bedeutung nicht klar und so wird er oftmals mit „Haftungsvermeidung" oder „Regeleinhaltung" übersetzt. Insbesondere die Abgrenzung zu den ebenfalls relevanten und benachbarten Themen der Corporate Governance und des Internen Kontrollsystems verschwimmt in der Praxis sehr häufig.

Das Thema Compliance und daraus folgend Compliance Management ist derzeit sehr brisant, vor allem aufgrund vieler Fälle von Korruption und kartellrechtswidriger Absprachen in den letzten Jahren, zuweilen auch unter direkter Mitwirkung oder Duldung des Top-Managements. Nur folgerichtig ist daher, dass die Vorstandsentscheidungen im Hinblick auf ihre Rechtmäßigkeit vom Aufsichtsrat geprüft und beurteilt werden und sich der Aufsichtsrat somit aktiv mit Compliance und den (möglichen) Compliance-Risiken beschäftigt.[1]

II. Grundsätzliches

Der Aufsichtsrat hat im Rahmen seiner Überwachungspflicht gem. § 111 Abs. 1 AktG die Geschäftsführung mit Blick auf ihre Recht-, Ordnungs- und Zweckmäßigkeit zu kontrollieren. Diese Aufsichtspflicht wird durch die Regelungen des Deutschen Corporate Governance Kodex (DCGK) ergänzt und verfeinert. Exemplarisch heißt es in Tz. 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)."

Zu beachten ist in 2017 insbesondere die Ausweitung der Empfehlungen im Bereich Compliance. Bislang verpflichtete § 91 Abs. 2 AktG zur Einrichtung eines Überwachungssystems. Künftig muss bei einer positiven Entsprechenserklärung der Vorstand für angemessene, an der Risikolage des Unternehmens ausgerichtete Maßnahmen sorgen, also für ein geeignetes Compliance Management System. Ferner hat er dessen Grundzüge offenzulegen und dafür zu sorgen, dass Beschäftigte geschützte Hinweise auf Rechtsverstöße geben können. Die Einräumung dieser Möglichkeit gegenüber Dritten bleibt eine Anregung.

Hintergrund ist die Absicht der Regierungskommission noch mehr Transparenz zu schaffen. Die Offenlegung von Grundzügen des Systems und etwaigen Maßnahmen sollen Shareholdern sowie der interessierten Öffentlichkeit ermöglichen, sich ein klares Bild vom Unternehmen zu schaffen und Vertrauen in die Unternehmensführung zu gewinnen. Darüber hinaus wird durch Empfehlung ein geschütztes Hinweisgebersystem erwartet, Fehlverhalten durch geeignete Kommunikationswege frühzeitig aufzudecken. Durch transparentes Handeln sollen so nationale und internationale Compliance-Verstöße vorgebeugt werden.

Der Überwachungspflicht des Aufsichtsrats unterliegt, ob und in welcher Weise der Vorstand dieser Pflicht nachkommt. Zu erwähnen ist jedoch, dass weder das Gesetz noch der DCGK näher definieren, was eine gute Compliance ist und wie diese um-

INHALT

Keywords
Compliance; Compliance Management System; DCGK

1 In Anlehnung an Beyer M./Heyd R./George N. (2017): Aufsichtsrat kompakt, S. 174 ff.

zusetzen ist. Notwendig, aber auch ausreichend ist es, wenn die Unternehmensleitung Strukturen schafft, damit das Unternehmen „compliant" ist. Auch muss sichergestellt sein, dass das von der Unternehmensleitung implementierte Vorgehen funktioniert und zu den Risiken und der Komplexität angemessen ist. Je nach Größe und Komplexität muss und soll es daher nicht zwingend zu einer unangebrachten Aufblähung der Organisation oder nicht pragmatischen Kontrollauswüchsen kommen.

III. Compliance Management System

Die Implementierung eines funktionierenden Compliance Management Systems (CMS) ist eindeutig eine originäre Aufgabe des Vorstands bzw. der Geschäftsführung. Der Aufsichtsrat muss daran anknüpfend überwachen, ob dieses System ordnungsgemäß erfolgt ist und dabei insbesondere auf Konzeption, Angemessenheit und Wirksamkeit achten. Er hat umgehend Maßnahmen zu ergreifen, falls Schwächen festgestellt werden.

Fraglich ist jedoch, wie die Überwachung für Aufsichtsräte konkret aussieht bzw. wie dieses umzusetzen ist?

Zunächst sollte sich der Aufsichtsrat mit den Kriterien für ein ordnungsgemäßes bzw. angemessenes CMS beschäftigen. Die Schwierigkeit dabei ist jedoch, dass er sich nicht an allgemeingültigen, in allen Unternehmen praktisch und pragmatisch umsetzbaren Mindeststandards ausrichten kann. Als hilfreiche Anregungen können jedoch beispielsweise der IDW-Prüfungsstandard 980 „Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen" oder der ISO Standard 19600 für Compliance Management Systeme dienen.

Empfehlenswert ist durchweg ein geschärfter Blick dafür, dass die Maßnahmen in einem angemessenen Verhältnis zur Größe des Unternehmens, zur Komplexität des Geschäfts und zu den Erkenntnissen der jedem CMS zugrunde liegenden Risikoanalyse stehen. Sollte der Aufsichtsrat Zweifel an der Existenz, Angemessenheit oder Wirksamkeit des CMS hegen und lassen sich diese auch nach Gesprächen mit der Unternehmensführung nicht ausräumen, ist die Veranlassung einer externen Prüfung des CMS im Hinblick auf die Gewährleistung der sorgfältigen Ausübung der eigenen Überwachungsfunktion ratsam.

Um die Eignung des Compliance Management Systems (CMS) zu beurteilen, wird der Aufsichtsrat regelmäßig den Compliance Officer oder Verantwortlichen befragen und im Zweifelsfall auch externen Sachverstand hinzuziehen. Üblich ist es auch, dass er diese spezifische Überwachungsaufgabe auch an den Prüfungsausschuss überträgt, der sich nach Tz. 5.3.2 DCGK ohnehin mit Fragen der Compliance befassen soll.

Zusammenfassend kann festgehalten werden: Verpasst der Vorstand die Einrichtung oder aber die Aufrechterhaltung eines funktionierenden und angemessenen Compliance Management Systems, so handelt es sich dabei um eine Pflichtverletzung, die der Aufsichtsrat nicht übersehen darf. Der DCGK sieht z.B. in Tz. 3.4 für den Vorstand vor, den Aufsichtsrat regelmäßig über alle für das Unternehmen relevanten Fragen der Compliance zu informieren. Übersehen werden sollte jedoch aufgrund der Formulierung nicht, dass es zugleich eine Holschuld des Aufsichtsrats ist, die notwendigen Informationen anzufordern.

IV. Umsetzung

Die Erfassung, das Monitoring und Reporting der Compliance Risiken läuft idealerweise in einem strukturierten Prozess ab, der vom Vorstand verantwortet wird und mittels dem er die Kommunikation zum Aufsichtrat sicherstellt. Zentrale Aspekte wie die Risikoidentifikation, Präventivmaßnahmen oder Steuerung der Risiken dürfen keinesfalls fehlen. Der nachfolgend in der Abbildung 1 skizzierte Prozess stellt eine Möglichkeit dar, den Umgang mit Compliance-Risiken zu gestalten.

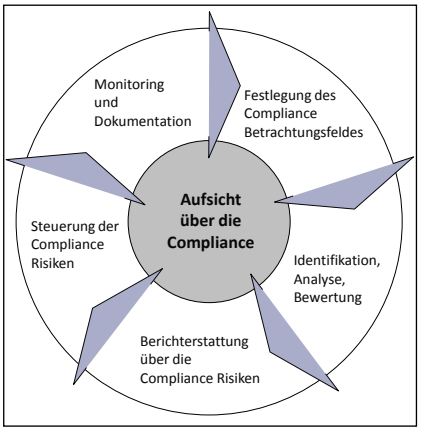

Abb. 1: Möglicher Prozess zur Aufsicht der Compliance Risiken

Im ersten Schritt geht es dabei um die Festlegung des Risikobetrachtungsfeldes. Hierbei soll der Vorstand Schwerpunkte für Auseinandersetzung mit Compliance Risiken festlegen und auch aufzeigen, dass die notwendigen Ressourcen finanzieller, technischer oder personeller Art zur Verfügung stehen und somit die Rahmenbedingungen stimmig sind. Der Aufsichtsrat hat diese Einschätzung des Vorstands zu überprüfen und, falls notwendig, zu korrigieren. Insbesondere die Antizipation neuer Risiken stellt hierbei eine Herausforderung dar.

Der zweite Schritt besteht aus der Identifikation, Analyse und Bewertung der Compliance Risiken. Die Schwierigkeiten bestehen zumeist in der Beschaffung der notwendigen Informationen und in der Messbarkeit der Risiken. Ein weiterer wichtiger Umstand ist, dass Interdependenzen zwischen den Risiken erkannt werden sollten, um frühzeitig Abhängigkeiten, Kettenreaktionen und Klumpenrisiken erkennen und begegnen zu können. Bei knappen Ressourcen kann der Aufsichtsrat eine wertvolle Hilfe im Rahmen der Priorisierung der Compliance Risiken sein; ebenso bei der Auswahl der Kriterien dafür.

Der nächste, also dritte Schritt beinhaltet die Berichterstattung der Compliance-Risiken an den Aufsichtsrat. Hierfür hat der Aufsichtsrat sicher-

zustellen, dass er alle aus seiner Sicht notwendigen Informationen auch erhält bzw. diese ggf. bei Fehlen nachfordert. Auch sollte er prüfen, ob alle wesentlichen Unternehmensbereiche mit dem notwendigen Berichtsmaterial versorgt werden. Neben den Turnusberichten vom Vorstand ist zu definieren, wie mit Sachverhalten umzugehen ist, die ad hoc berichtspflichtig sind. Berichte von Prüfern, Revisoren und ggf. Beratern sind ebenfalls regelmäßig auszuwerten.

Im vorletzten, dem vierten, Schritt geht es um die Steuerung der Compliance-Risiken. Dafür ist es vor allem notwendig, sich mit den Maßnahmen und deren Plausibilität zu befassen. Die Berichtsschwelle bzw. Wesentlichkeitsgrenze für die Risiken hängt von der Unternehmensgröße und der wirtschaftlichen Lage ab. Wobei hier zwischen den Risiken auch variiert werden kann, wenn beispielsweise reputationsschädigende Vorfälle deutlich enger überwacht werden sollen als andere Themen.

Der letzte Schritt ist gekennzeichnet durch das Compliance-Risikomonitoring und die dazugehörige Dokumentation. Ein wesentlicher Aspekt des Monitorings ist die Weiterentwicklung der implementierten Compliance-Prozesse und die regelmäßige Überprüfung der Maßnahmen auf ihre Wirksamkeit. Mit der Dokumentation weist der Aufsichtsrat nach, dass er seiner Sorgfaltspflicht entsprochen hat.

V. Verantwortung

Bei der Erörterung der Verantwortung soll eingangs kurz auf die Situation in der GmbH eingegangen werden, da bisher lediglich Ableitungen aus dem Aktiengesetz vorgenommen wurden. An der grundsätzlichen Übertragbarkeit der Aussagen zur Compliance Pflicht auf eine GmbH ist nicht zu zweifeln, im Gegenteil: Dort fehlt zwar eine § 91 Abs. 2 AktG entsprechende, ausdrückliche gesetzliche Pflicht zur Einrichtung eines Überwachungssystems. Bei der Einführung

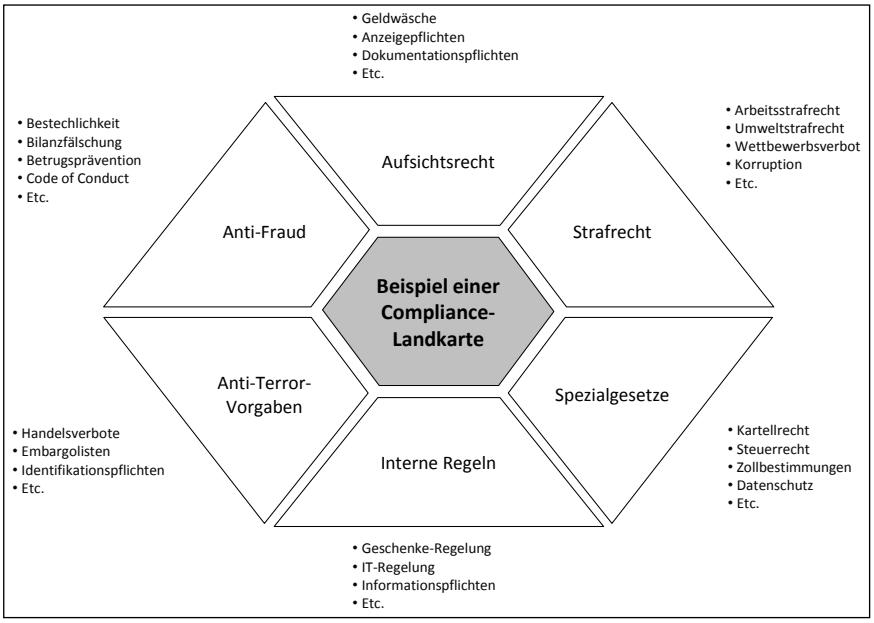

Abb. 2: Beispiel einer Compliance-Landkarte

der aktienrechtlichen Norm (durch das KonTraG) ging der Gesetzgeber jedoch davon aus, dass für die GmbH im Grundsatz nichts anderes gilt und die Neuregelung insoweit Ausstrahlungswirkung habe.[2] Dies ist für die GmbH auch anerkannt. Da die Überwachungspflichten des Aufsichtsrats in der Regel übertragen werden können, folgt daraus, dass auch ein Aufsichtsrat einer GmbH im Rahmen seiner Überwachung Sorge zu trage hat, dass die Gesellschaft „compliant" ist.

Viele Gremien tragen der Bedeutung Rechnung und etablieren inzwischen Compliance-Ausschüsse oder Compliance-Beauftragte. Erschwerend ist jedoch, dass die Anforderungen nicht eindeutig benannt sind, zumal der Gesetzgeber bereits dem Vorstand nur sehr vage Orientierungshilfen für die Ausgestaltung entsprechender Strukturen an die Hand gibt. Es stellen sich z.B. folgende grundlegende Fragen:[3]

- Wie umfassend muss über Compliance- Anstrengungen berichtet werden?
- Muss der Aufsichtsrat dabei die Implementierung bestimmter, grundlegender Einzelmaßnahmen prüfen?
- Muss beispielsweise sichergestellt sein, dass fortlaufend die Erkenntnisse der aktuellen Rechtsprechung ausgewertet und in die Struktur überführt werden?
- Gibt es zum Beispiel „Mittelstandsbesonderheiten"?

VI. Herausforderung vielfältiger Compliance-Gebiete

Eigentlich ist mit der umfassenden Definition bezüglich der Einhaltung externer Vorschriften (Gesetze, Auflagen etc.) und interner Vorgaben (Anweisungen, betriebsinterne Regeln etc.) alles Notwendige beschrieben. Bei näherer Betrachtung wird jedoch offenkundig, wie herausfordernd diese Aufgabe ist.

Die Abbildung 2[4] zeigt die diversen Themengebiete exemplarisch auf.

Zusätzlich haben sich eigene „Disziplinen" gebildet, wie die IT-Compliance, Corporate Compliance, Strategie-Compliance etc., zu deren Überwa-

2 Siehe BT-Drucks. 13/9712, S. 15.

3 Schemmel, A./Minkoff, A. (2013): Aufsichtsrat und Compliance, in: Der Aufsichtsrat 2013, Heft 06/2013, S. 95 und Remberg, M. (2015): Compliance im Mittelstand: Die Rolle des Aufsichtsrats, in: Der Aufsichtsrat 2015, Heft 03/2015, S. 40–41.

4 Beyer M./Heyd R./George N. (2017): Aufsichtsrat kompakt, S. 185.

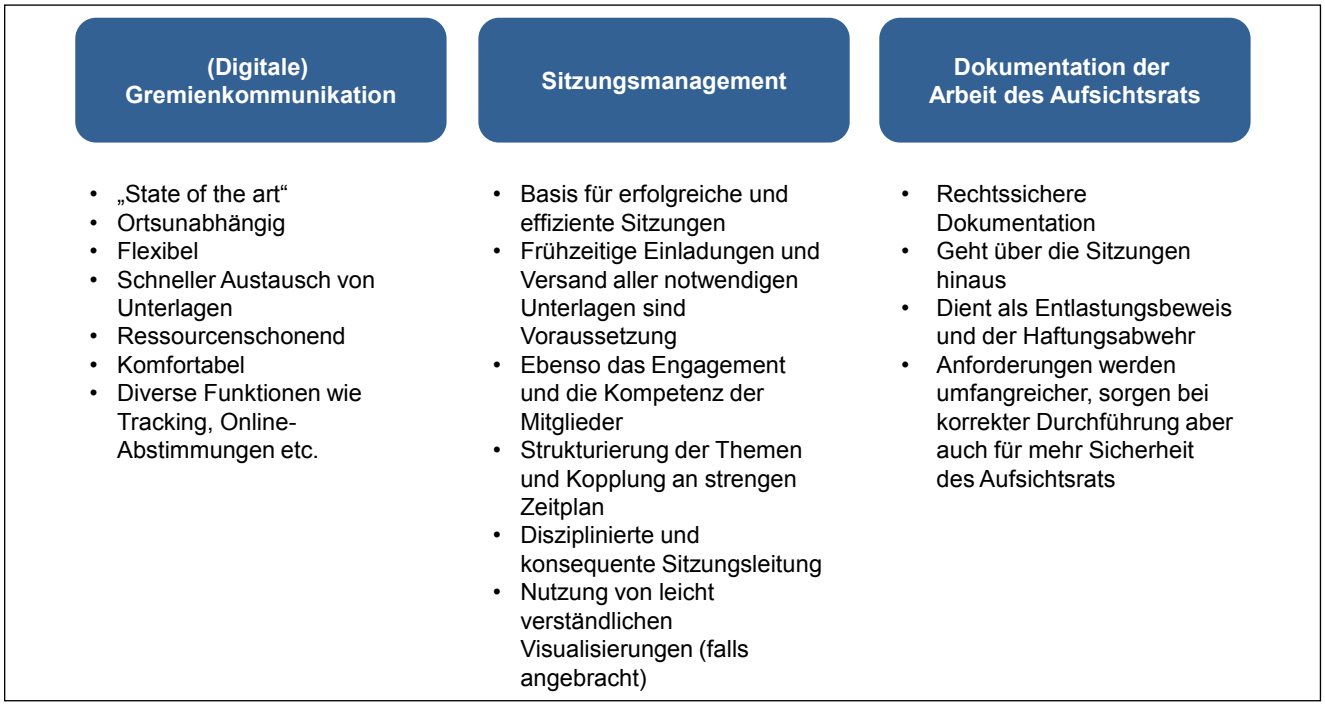

Abb. 3: Aktuelle Entwicklungen im Rahmen des Sitzungsmanagements

chung wiederum spezielle Kompetenzen erforderlich und im Gremium vorzuhalten sind. Die bloße Prüfung der Regeleinhaltung ist sicher nicht zielführend, sondern eine inhaltliche Durchdringung sollte die Basis für die Beurteilung sein.

Für weitere Komplexität sorgt die Tatsache, dass die Grenzen zwischen den Compliance-nahen Themen wie z.B. die Corporate Governance oder dem Internen Kontrollsystem fließend sind.

VII. Herausforderung Rollenverständnis

Die Entwicklung des Aufsichtsrats von der reinen Kontroll- bzw. Überwachungsinstanz hin zum Berater und Sparringspartner für den Vorstand erfordert nun weit mehr, als die vergangenheitsorientierte „Brille“. Es benötigt vielmehr die Fähigkeit Entwicklungen vorherzusehen und somit auch existenzielle Trends bezüglich des Geschäftsmodells oder sogar drohende Einschränkungen, Verbote etc. als strategischer Partner des Vorstands zu antizipieren und das Wissen darum einfließen zu lassen.

Als das aktuelle Beispiel einer sich verändernden Arbeitswelt mit Rückkopplungen auf wohl fast alle Branchen ist die Digitalisierung zu nennen. Dabei sind zuweilen auch sehr wertvolle Rückschlüsse auf die Anpassungsfähigkeit des Aufsichtsrats möglich und letztlich auch im Hinblick auf seine Beratungsfunktion für die Weiterentwicklung des Unternehmens. Konkret geht es um die Organisation der Gremienarbeit und selbige an sich:

- Erhält jedes Aufsichtsratsmitglied noch regelmäßig ein postalisches Paket mit Unterlagen?
- Läuft die Gremienarbeit bereits „online“?
- Falls ja: Wie wird mit diesen IT-Risiken umgegangen? (Datensicherheit, Zugriffsrechte etc.)
- Falls ja, wie ist sichergestellt, dass z.B. der Vorstand oder Mitarbeiter des Unternehmens (auch aus der IT-Abteilung) keinen Zugriff auf streng vertrauliche Dokumente des Aufsichtsrats haben.

Die aktuellen Entwicklungen des Sitzungsmanagements sind in beiliegendem Schaubild zusammengefasst:[5]

5 Beyer M./Heyd R./George N. (2017): Aufsichtsrat kompakt, S. 51.

Neben der reinen Fragestellungen der Compliance wird an dem Beispiel deutlich, inwiefern die Arbeitsweise des Aufsichtsrats auch für Wandlungsfähigkeit, Adaptionsfähigkeit und Offenheit interpretiert und als Botschaft an das Management und die Belegschaft gesehen werden kann.

VIII. Fazit

Die Ausführungen zeigen auf, dass die trennscharfe Abgrenzung von Compliance-Themen und den übrigen Aufgaben unter Umständen schwerlich möglich ist. Die Überwachung der Einhaltung bestimmter Regelungen bedarf in der Regel gleichermaßen ein (grundlegendes) inhaltliches Verständnis sowie die Kompetenz, als Aufsichtsrat effektive und effiziente Kontrollen einzufordern, zu erkennen und zu nutzen. Die vermeintlich juristisch geprägte Interpretation der Aufgabe ist aus Sicht des Autors zu eng gefasst, da in der Regel ein profundes Verständnis für die zugrundeliegenden zu beurteilenden Sachverhalte, Kontrollen etc. notwendig ist.