Gesamtverband der Deutschen Versicherungswirtschaft e. V.

Compliance im Erst- und Rückversicherungsunternehmen

Ein Leitfaden für die Praxis

Stand: Oktober 2014

GDV
DIE DEUTSCHEN VERSICHERER

Compliance im Erst- und Rückversicherungsunternehmen

Ein Leitfaden für die Praxis

Stand: Oktober 2014

Impressum

Herausgeber:
Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GDV)
Wilhelmstraße 43 / 43 G, 10117 Berlin
www.gdv.de
Telefon (030) 2020-5415
Telefax (030) 2020-6415

Ansprechpartner:
Stefan Sawatzki, Recht
s.sawatzki@gdv.de

Oktober 2014

Inhaltsverzeichnis

A. Einführung

Unter Compliance wird gemeinhin die Einhaltung von Gesetzen einschließlich der Sicherstellung des gesetzmäßigen Verhaltens in einer Unternehmensorganisation verstanden. Dem Ursprung nach handelt es sich nicht um einen Begriff der Gesetzgebung, sondern um eine aus dem angelsächsischen Rechtskreis stammende allgemeine Anforderung und Umschreibung für gesetzmäßiges Verhalten im Unternehmen. Daher gibt es keine klare und allgemeingültige Definition von Compliance, was das Verständnis auch bezüglich der Reichweite und des organisatorischen Handlungsbedarfs im Unternehmen erschwert. Heute besteht aber Einigkeit, dass es jedenfalls nicht ausreicht, nur rechtskonformes Verhalten im Unternehmen sicherzustellen. Die Beachtung ethisch-moralischer Grundsätze hat in den letzten Jahren signifikant an Bedeutung gewonnen. Dies kann als Compliance-Aufgabe ausgestaltet werden.

Bei aus den Unternehmen heraus begangenen Rechtsverstößen drohen diesen erhebliche wirtschaftliche und finanzielle Nachteile sowie – zum Teil noch schwerwiegender – Schäden der Reputation. Speziell in der Versicherungsbranche haben die Aufsichtsbehörden zudem die Möglichkeit, einschneidende aufsichtsrechtliche Sanktionen zu verhängen. Bei wesentlichen Rechtsverstößen reichen diese bis hin zur Abberufung von Vorstands- oder Aufsichtsratsmitgliedern oder dem Entzug der Geschäftserlaubnis. Eine effektive Compliance kann ganz maßgeblich dazu beitragen, diese Risiken zu verringern.

Als wesentlicher Teil der Finanzwirtschaft tragen Versicherungsunternehmen mit ihrer Vertrauenskultur eine besondere Verantwortung für die Einhaltung von ethischen Grundsätzen und Werten. Die Wahrnehmung dieser Verantwortung im Rahmen eines Compliance-Management-Systems (CMS) fördert die unternehmerische Professionalität und unterstützt die Mitarbeiter, sich in einer zunehmend komplexer werdenden Prozess- und Regelungslandschaft zurechtzufinden. Zudem gibt die Compliance-Funktion den Mitarbeitern die notwendige Orientierung und steht ihnen beratend zur Seite. Neben der Überwachung von Regelkonformität erzeugt ein ganzheitlicher Compliance-Ansatz damit auch qualitativen geschäftlichen Mehrwert.

Die Solvency II-Richtlinie fordert von den Versicherungsunternehmen, dass diese eine Compliance-Funktion als Teil ihres Internen Kontrollsystems einrichten. Unter einer Funktion versteht die Richtlinie die administrative Kapazität innerhalb des Governance-Systems zur Übernahme praktischer Aufgaben.[1]

Die Ausführungen dieses Papiers sollen die Verantwortlichen dabei unterstützen, effektive Compliance-Strukturen in den Unternehmen einzurichten. Zu diesem Zweck werden zunächst in einem ersten Teil (B.) die Grundlagen eines jeden Compliance-Systems zusammengefasst. Unter C. werden sodann die gesellschafts- sowie die

1 Art. 13 Abs. 29 Solvency-II-Richtlinie.

versicherungsaufsichtsrechtlichen Vorgaben für die Compliance in einem Versicherungsunternehmen erläutert. Diese decken sich z. T. mit den unter B. beschriebenen praktischen Anforderungen, gehen aber z. T. auch über diese hinaus. Teil D. widmet sich der Aufgabe der Compliance-Funktion und zeigt die unternehmensindividuellen Spielräume bei der Aufgabenzuweisung auf. Da die praktische Umsetzung der aufsichtsrechtlichen Vorgaben in den Unternehmen erfahrungsgemäß viele Fragen aufwirft, werden abschließend spezifische Themenfelder der Compliance-Praxis aufgegriffen und Gestaltungshinweise gegeben (E.).

Die in dem Papier dargestellten Ergebnisse geben keinen Mindeststandard wieder. Sie sind als Hilfestellung für die Unternehmen gedacht, individuelle Lösungen zu entwickeln. Naturgemäß kann die Darstellung nicht abschließend sein, da der Gesetzgebungsprozess auf europäischer Ebene (Delegierte Rechtsakte, EIOPA-Leitlinien) sowie die nationale Umsetzung (BaFin-Verlautbarungen, VAG-Novelle) noch nicht beendet sind. Das vorliegende Papier bildet den Gesetzes- und Diskussionsstand im Oktober 2014 ab.

B. Grundelemente der Compliance-Arbeit

Für die Compliance-Arbeit im Versicherungsunternehmen lassen sich wesentliche Grundelemente identifizieren. Diese können als Richtschnur bei der Gestaltung eines effektiven CMS dienen. In jedem Fall erforderlich ist es jedoch, die Grundelemente entsprechend der unternehmensindividuellen Gegebenheiten zu konkretisieren bzw. anzupassen (z. B. in Abhängigkeit von der Größe und dem Risikoprofil des Unternehmens). Die einzelnen Aspekte finden sich so oder in ähnlicher Form auch in Prüfungsstandards, wie etwa dem IDW PS 980.

I. Compliance-Kultur

Grundlage eines jeden Compliance-Systems ist es, im Unternehmen eine wahrnehmbare Compliance-Kultur zu schaffen. Es kommt dabei ganz maßgeblich darauf an, dass das Topmanagement die Einhaltung der rechtlichen und moralischen Regeln vorlebt („tone at/from the top“). Ausgangspunkt und elementarer Bestandteil der Compliance-Kultur ist in der Regel ein Verhaltenskodex, sofern dieser auch einen echten Wertekanon enthält, er hinreichend bekannt gemacht und im Unternehmen auch praktiziert wird. Wichtig für die Compliance-Kultur sind für die Mitarbeiter sichtbare Bekenntnisse des Top-Managements zur Compliance. Diese sind dann glaubwürdig und erzeugen Wirkung, wenn gemäß diesen Bekenntnissen auch im Tagesgeschäft gehandelt wird. Eine im Unternehmen etablierte Compliance-Kultur wirkt sich positiv auf die Bereitschaft der Mitarbeiter aus, sich regelkonform zu verhalten.

Einen weiteren wichtigen Teil der Compliance-Kultur bildet die verlässliche und transparente Sanktionierung von Fehlverhalten. Im Unternehmen müssen Prozesse implementiert werden, die festlegen, wie mit (Rechts-)Verstößen von Mitarbeitern umgegangen werden soll. Dabei ist es nicht erforderlich, dass ein starrer Sanktionskatalog aufgestellt wird. Es ist vielmehr sogar empfehlenswert, den verantwortlichen Personen Spielraum für eine individuelle, am konkreten Sachverhalt orientierte und ausreichend dokumentierte Sanktionsentscheidung einzuräumen.

II. Compliance-Ziele

Der Vorstand legt die Compliance-Ziele fest. Diese werden auf Basis der allgemeinen Unternehmensziele entwickelt und anhand der Bedeutung für das Unternehmen gewichtet. Insbesondere muss bestimmt werden, welche Teilbereiche des Unternehmens für die Compliance-Vorgaben relevant sind. Die Compliance-Ziele sind zu berücksichtigen, wenn die Compliance-Risiken ermittelt werden (vgl. unter IV.).

Ein solches Compliance-Ziel kann beispielsweise der Schutz vor Reputationsschäden oder der Schutz vor Bußgeldern sein, um zum Gesamterfolg des Unternehmens beizutragen.

III. Dokumentation der Organisation der Compliance (Compliance-Leitlinie)

Die Einrichtung der Compliance-Funktion ist in einer Compliance-Leitlinie niederzulegen und zu dokumentieren. Diese sollte sowohl die Aufgabenfelder, Verantwortlichkeiten und Befugnisse als auch die Berichtspflichten der Compliance-Funktion klar definieren.[2] Ein solches Dokument dient der klaren Festlegung von Kompetenzen und beschreibt die konkrete Organisationsstruktur. Die Leitlinie muss durch den Vorstand beschlossen werden. Sie wird häufig als Compliance-Charta oder Compliance-Handbuch bezeichnet. Es ist denkbar, dass hier die Tätigkeiten der Compliance-Funktion wie die Erstellung von Richtlinien, Durchführung von Schulungen oder Überprüfungshandlungen näher beschrieben werden. Ein solches Werk sollte regelmäßig auf Aktualisierungsbedarf hin überprüft werden.

IV. Risikoanalyse

Die Compliance-Funktion ist für die Identifizierung und Beurteilung des mit der Nichteinhaltung der rechtlichen Vorgaben verbundenen Risikos (Compliance-Risiko) verantwortlich. Hierfür ist es erforderlich, sicherzustellen, dass diese Risiken sowie Veränderungen dieser Risiken frühzeitig erkannt und verfolgt werden, um die erforderlichen Maßnahmen zu treffen. Auf Basis der Risikoanalyse, die alle Geschäftsbereiche und Tätigkeitsfelder des Unternehmens erfasst, weist das Unternehmen der Compliance-Funktion die von ihr wahrzunehmenden Aufgaben zu. Die Bewertung strategischer Risiken ist dabei keine Aufgabe der Compliance-Funktion.

Es empfiehlt sich eine systematische Aufnahme und Analyse der bestehenden Compliance-Risiken, wobei dies beispielsweise durch Interviews und Workshops mit den Fachbereichen erfolgen kann. Zudem bietet es sich an, im Unternehmen verfügbare Informationen auszuwerten, z. B.:

- Revisions- oder Fachrevisionsberichte;
- Risikoberichte;
- Berichte des/der Geldwäsche- oder Datenschutzbeauftragten, soweit diese nicht in der Compliance-Organisation eingegliedert sind;
- Ergebnisse des Beschwerdemanagements;
- Ergebnisse eines Hinweisgebersystems.

Nach Bedarf können im Anschluss weitere vertiefte Berichte in den Fachbereichen abgerufen werden.

2 Vgl. Art. 270 Abs. 1 der Delegierten Rechtsakte (DDA) sowie die BaFin-Verlautbarung zu „Interne Kontrollen und interne Revision“, Rz.16.

Bewährte Praxis ist es, zunächst alle denkbaren Compliance-Risiken zu erfassen und dann zu priorisieren. Die festgestellten wesentlichen Risiken sollten im Hinblick auf Eintrittswahrscheinlichkeit und mögliche Folgen analysiert werden. Dabei können sich bereits bestehende Kontroll- und Risikominimierungsmaßnahmen der Compliance-Funktion, wie z. B. spezielle Compliance-Richtlinien und durchgeführte Schulungen, als risikominimierend auswirken. Die Geschäftsleitung ist über die identifizierten Compliance-Risiken zu unterrichten. Für die Bewertung sollten sowohl innere als auch äußere Faktoren berücksichtigt werden. Ein enger Austausch sowohl mit der Rechtsabteilung als auch mit der Risikomanagement-Funktion sowie mit der Internen Revision kann für eine solche Risikobewertung hilfreich sein.

V. Compliance-Plan

Die Aktivitäten der Compliance-Funktion erfolgen insbesondere auf Basis eines Compliance-Plans, in welchem diese ihre einzelnen Tätigkeiten und Überwachungsmaßnahmen dokumentiert.[3] Der Compliance-Plan beschreibt konkret die Tätigkeiten, die in den kommenden Geschäftsjahren vorgesehen sind.[4] Dabei sollten diese zumindest mit einer groben zeitlichen Einordnung versehen werden.

Der Compliance-Plan sollte auf den Ergebnissen der Risikoanalyse aufbauen und die hier identifizierten Risiken aufnehmen und versuchen, diese durch gezielte Gegenmaßnahmen zu minimieren. So könnten zum Beispiel die Erstellung von Compliance-Richtlinien zum Umgang mit Einladungen und Geschenken sowie gezielte Schulungen vorgesehen sein, um das Korruptionsrisiko zu minimieren.

Die Auswahl der Aktivitäten sollte risikoorientiert erfolgen.[5] Das Unternehmen kann individuell eine Schwelle für „unwesentliche“ Risiken festlegen. Diese sollte dann auch dokumentiert werden. Soweit sich in der Risikoanalyse ergibt, dass ein Risiko die festgelegte Schwelle nicht überschreitet, kann unter Risikogesichtspunkten die Überwachung in den verantwortlichen Fachbereichen genügen.

Der Compliance-Plan ist ein umfassendes Dokument und erstreckt sich auf die gesamten Aktivitäten der Compliance-Funktion. Danach müssen sich die festgelegten Maßnahmen nicht nur auf Maßnahmen der Prävention, Detektion und Reaktion beziehen. Regelmäßig werden im Compliance-Plan auch andere Maßnahmen adressiert, wie bspw. die Risikoanalyse oder organisatorische Themen, welche die Weiterentwicklung und Optimierung des Compliance-Systems sicherstellen.

3 Vgl. Art. 270 DDA.
4 BaFin-Verlautbarung zu „Interne Kontrollen und interne Revision“, Rz. 36.
5 BaFin-Verlautbarung zu „Interne Kontrollen und interne Revision“, Rz. 36.

Der Compliance-Plan beschreibt in der Regel das Maßnahmenbündel im Rahmen des Compliance-Managements eines Unternehmens bezogen auf einzelne (rechtliche) Themengebiete. Grundlage für den Compliance-Plan ist die Bewertung der Compliance-Risiken. Im Compliance-Plan werden daher Maßnahmen festgelegt, mit denen ein regelkonformes Verhalten erreicht werden soll. Damit zielt der Compliance-Plan darauf ab, Compliance-Verstöße zu begrenzen, zu vermeiden, aufzudecken oder abzuklären. Mögliche Beispiele hierfür sind die Einführung von Richtlinien und deren interne Kommunikation, klare Zuständigkeiten und Verantwortlichkeiten, Überprüfung von Geschäftspartnern oder die Einführung eines Hinweisgebersystems.

Der Compliance-Plan enthält also Maßnahmen, die auf die Verhinderung von Regelverstößen abzielen (Prävention); dies umfasst auch das rechtzeitige Erkennen von Risiken für Compliance-Verstöße und die Reaktionen auf die erkannten Risiken. Da „Überwachung" die zentrale Aufgabe der zweiten Verteidigungslinie[6] ist, empfiehlt es sich, alle Maßnahmen mit Überwachungscharakter im Compliance-Plan zu kennzeichnen.[7] Weiterhin gehören oftmals Maßnahmen hierher, die zur Aufdeckung von Verstößen führen, bspw. die Einrichtung von Möglichkeiten der anonymen Hinweiserstattung.

Ein derartiges Maßnahmen-Programm wird nur dann erfolgreich sein, wenn es nachhaltig im Unternehmen und insbesondere in die Prozessabläufe integriert ist; wie z. B. die Einhaltung des 4-Augenprinzips im Rahmen risikobehafteter Prozesse sowie klare Berechtigungskonzepte und Genehmigungsverfahren.

Die Dokumentation darüber, inwieweit der Compliance-Plan umgesetzt ist, kann als Bericht an die Geschäftsleitung genutzt werden. Außerdem dient eine solche Planung der Eigenkontrolle und schafft Dokumentationssicherheit. Die Aktualität des Compliance-Plans ist regelmäßig zu überprüfen.

VI. Compliance-Kommunikation

Eine gute Compliance-Kommunikation setzt voraus, dass die betroffenen Mitarbeiter über die wesentlichen Regelungen zur Compliance-Funktion sowie die festgelegten Rollen und Verantwortlichkeiten informiert werden. Nur wenn dies sorgfältig erfolgt, können sie ihre Aufgaben im CMS ausreichend verstehen und sachgerecht erfüllen.

6 Vgl. zum Begriff D.II.1.

7 Vgl. dazu die BaFin-Verlautbarung zu „Interne Kontrollen und interne Revision" (Rz. 19), in der „interne Kontrolltätigkeit" und „Überwachung" unterschieden wird sowie Rz. 36: „Die Aktivitäten der Compliance-Funktion erfolgen auf Basis eines Compliance-Planes. Im Compliance-Plan sind zumindest alle Tätigkeiten und Überwachungsmaßnahmen aufzuführen, die in den kommenden Geschäftsjahren vorzusehen sind." Überwachung meint die i. d. R. stichprobenartige Überprüfung, ob erforderliche Kontrollen (durch die 1. Verteidigungslinie) implementiert sind, regelmäßig durchgeführt und dokumentiert werden.

Der Inhaber der Compliance-Funktion muss den Vorstand regelmäßig über die Ergebnisse der Analyse der Compliance-Risiken, mitigierende Maßnahmen (Stand des Ausbaus des CMS) und wesentliche Verstöße informieren.

Im Unternehmen sollte zudem festgelegt werden, in welchen Fällen (z. B. bei schweren Verstößen in den wesentlichen Risikobereichen) ad hoc die Pflicht zur Meldung des Verstoßes an vorgesetzte Stellen oder die Compliance-Organisation besteht, auch sofern sich diese Meldepflicht ggfs. bereits aus arbeitsrechtlichen Nebenpflichten ergibt.[8]

In größeren Unternehmen muss auch die Kommunikation innerhalb der Compliance-Funktion bzw. zwischen den mit Aufgaben der Compliance-Funktion befassten Organisationseinheiten festgelegt werden.

VII. Kontinuierliche Verbesserung des CMS

Die Compliance-Struktur und -Organisation muss regelmäßig überprüft werden. Dazu muss das CMS hinreichend dokumentiert sein.

Schwachstellen in der Aufbau- und Ablauforganisation der Compliance-Funktion und des CMS können durch Prüfungen der Internen Revision oder externer Prüfer, eigene Analysen der Compliance-Organisation (sog. Self-Assessments) oder durch Regelverstöße festgestellt werden. Schwachstellen sind an das Management bzw. die hierfür bestimmte Stelle im Unternehmen zu berichten. Die gesetzlichen Vertreter müssen die Durchsetzung des CMS, die Beseitigung von Mängeln und die ständige Verbesserung des Systems sicherstellen. Die Compliance-Funktion selbst sollte hierzu Vorschläge unterbreiten.

Zur ständigen Verbesserung gehört auch die ständige zielgerichtete und systematische Fortbildung aller Personen, die für die Compliance-Funktion tätig sind.

8 Näher zu Berichtswegen unten E.VI.

C. Rechtsgrundlagen der Compliance in Versicherungsunternehmen

Die Solvency II-Rahmenrichtlinie enthält besondere Anforderungen im Hinblick darauf, wie die Compliance-Funktion in einem Versicherungsunternehmen ausgestaltet und implementiert sein muss. Dabei weisen die Vorgaben zum Teil Parallelen zu dem bestehenden Governance-Konzept der nationalen Regelungen im AktG oder VAG auf. Jedoch ergeben sich auch einige wesentliche Abweichungen, die es erforderlich machen, die bisherigen (Unternehmens-)Strukturen grundlegend zu überprüfen.

I. Compliance-Verantwortung der Geschäftsleitung

Das **Gesellschaftsrecht** erwähnt den Begriff Compliance bislang nicht ausdrücklich. In Rechtsprechung und Literatur ist aber anerkannt, dass dem **Vorstand** aus dessen aktienrechtlichen Pflichten eine Compliance-Verantwortung erwächst.

Grundlage der Compliance-Verantwortung ist die aus §§ 76, 93 Abs. 1 AktG abgeleitete Legalitätspflicht des Vorstands.[9] Jedes Vorstandsmitglied muss danach in seinem Verantwortungsbereich dafür sorgen, dass es sich selbst rechtstreu verhält. Zum anderen muss es sicherstellen, dass das Unternehmen so organisiert und beaufsichtigt wird, dass keine Gesetzesverstöße stattfinden.

Diese Überwachungspflicht des Vorstands wird durch die Organisationsvorgabe in § 91 Abs. 2 AktG konkretisiert. Danach muss der Vorstand ein Überwachungssystem einrichten, um bestandsgefährdende Entwicklungen für das Unternehmen frühzeitig zu erkennen. Der Vorstand genügt dieser Organisationspflicht bei entsprechender Gefährdungslage unter anderem dann, wenn er eine Compliance-Organisation einrichtet, die auf Schadenprävention und Risikokontrolle angelegt ist.

Die Compliance-Verantwortung ist als zentrale Leitungsaufgabe (§ 76 AktG) dem **Gesamtvorstand** zugewiesen. Dieser muss alle grundlegenden Entscheidungen über die Compliance-Organisation selbst treffen und sich regelmäßig bzw. anlassbezogen von deren Wirksamkeit überzeugen. Die Compliance-Verantwortung als solche kann daher nicht delegiert werden.[10]

Möglich ist es indes, konkrete Einzelpflichten im Wege der Arbeitsteilung entweder horizontal oder vertikal zu übertragen:

- Der Gesamtvorstand kann ein Einzelmitglied beauftragen, die im Gremium beschlossenen Entscheidungen umzusetzen und die Implementierungen des Com-

9 Das Landgericht München I hat hierzu in seinem Siemens/Neubürger-Urteil vom 10.12.2013 – 5HK O 1387/10 – wesentliche Aussagen getroffen. Das Urteil ist noch nicht rechtskräftig. Die Berufung ist anhängig beim OLG München.

10 So auch die BaFin-Verlautbarung zu „Interne Kontrollen und interne Revision“, Rz. 11.

pliance-Systems zu überwachen. Der Gesamtvorstand muss aber weiterhin sicherstellen, dass das ressortzuständige Vorstandsmitglied diese Aufgabe ordnungsgemäß wahrnimmt. Dazu gehört, dass Informationen zu bekannt gewordenen Vorfällen eingeholt werden. Sind Fehlentwicklungen der eingerichteten Compliance-Organisation erkennbar, trifft auch das nicht ressortzuständige Vorstandsmitglied die Pflicht, Maßnahmen zur Abhilfe anzustoßen und, sofern es überstimmt wird, ggf. den Aufsichtsrat einzuschalten.

- Zulässig ist auch die Übertragung vom Ressortvorstand auf nachgelagerte Unternehmensebenen (z. B. Compliance-Beauftragte). Auch hier gilt, dass die Letztverantwortung beim Gesamtvorstand verbleibt. Dieser muss die ordnungsgemäße Aufgabenerfüllung der nachgelagerten Ebenen überwachen.

Der **Aufsichtsrat** muss überwachen, dass der Vorstand seine Compliance-Aufgabe ordnungsgemäß wahrnimmt. Er kann die Compliance-Organisation gegenüber dem Vorstand beanstanden. Der Aufsichtsrat kann keine direkten Anweisungen an den Vorstand oder den Compliance-Officer geben, jedoch bei Pflichtverstößen von seiner Personalkompetenz Gebrauch machen und ggf. Schadensersatzansprüche der Gesellschaft gegenüber einem Vorstand geltend machen.

II. Branchenspezifische Regeln für Versicherungsunternehmen

Die allgemeinen gesellschaftsrechtlichen Anforderungen werden durch die besonderen Organisationspflichten des Versicherungsaufsichtsrechts überlagert. Die Versicherungsunternehmen werden bereits seit 2008 durch § 64a VAG verpflichtet, eine ordnungsgemäße Geschäftsorganisation vorzuhalten, welche die Einhaltung der zu beachtenden Gesetze, Verordnungen und aufsichtsrechtlichen Anforderungen gewährleistet. Umstritten war bislang, ob aus dieser Vorgabe die Verpflichtung abgeleitet werden kann, eine Compliance-Funktion einzurichten.

1. Solvency II-Rahmenrichtlinie und nationale Umsetzung

Die **Rahmenrichtlinie Solvency II** sieht nunmehr vor, dass die Versicherungsunternehmen über ein wirksames Governance-System verfügen müssen, um ein solides und vorsichtiges Management des Geschäfts zu gewährleisten.[11] Zentraler Bestandteil des Governance-Systems ist ein wirksames Internes Kontrollsystem, welches gem. Art. 46 Abs. 1 der Richtlinie obligatorisch „eine Funktion der Überwachung der Einhaltung der Anforderungen („Compliance-Funktion“)“ umfassen muss. Die Letztverantwortung dafür, dass die „gemäß dieser Richtlinie erlassenen Rechts- und Verwaltungsvorschriften durch das Unternehmen“ beachtet werden, trägt der Vorstand.[12]

11 Art. 41 Abs. 1 Solvency II-Richtlinie.
12 Art. 40 Solvency II -Richtlinie.

Nach der sog. „Quick fix 2"-Richtlinie müssen die Vorgaben der Richtlinie bis zum 1. Januar 2016 in nationales Recht umgesetzt werden. Der deutsche Gesetzgeber hat hierzu einen Entwurf für eine **Novelle des Versicherungsaufsichtsgesetzes (VAG-E)** vorgelegt. Die Vorgaben für die Compliance-Funktion sind in § 29 VAG-E verankert. Die nationale Umsetzung geht dabei zum Teil über die Vorgaben in Art. 46 der Richtlinie hinaus.

2. Delegierte Rechtsakte

Die Vorgaben der Solvency II-Richtlinie zum Governance-System werden durch Durchführungsregelungen näher bestimmt (Art. 50 Abs. 1). Die EU-Kommission hat einen Entwurf für entsprechende **delegierte Rechtsakte (Draft Delegated Acts – DDA)** vorgelegt. Diese entfalten, nachdem sie verabschiedet sind, gegenüber den Versicherungsunternehmen und den Aufsichtsbehörden unmittelbare Geltung (Art. 288 UAbs. 2 AEUV). In der Praxis sind die Anforderungen der delegierten Rechtsakte daher neben den nationalen Umsetzungsrechtsakten zu beachten und gehen diesen vor.

Der Entwurf der delegierten Rechtsakte enthält im Hinblick auf die Compliance-Funktion nur wenige konkretisierende Vorgaben. In Art. 270 DDA ist in Ergänzung zu Art. 46 Abs. 2 der Richtlinie festgelegt, dass die Versicherungsunternehmen eine Compliance-Leitlinie und einen Compliance-Plan erstellen müssen, ohne jedoch nähere Angaben zu machen, was dies genau bedeutet.[13] Es wird lediglich darauf verwiesen, dass in der Compliance-Leitlinie Verantwortlichkeiten, Kompetenzen und Berichtspflichten festzulegen sind. Der Compliance-Plan soll nach den DDA die geplanten Aktivitäten der Compliance-Funktion unter Berücksichtigung aller relevanten Unternehmensbereiche und des bestehenden Compliance-Risikos umfassen.

Zudem wird der Compliance-Funktion die Aufgabe zugewiesen, zu bewerten, ob die präventiven Maßnahmen, die zur Vermeidung von Rechtsverstößen ergriffen worden, angemessen sind. Weitere konkrete Aussagen zur Compliance-Funktion finden sich in den Entwürfen der Delegierten Rechtsakte nicht.

3. EIOPA-Leitlinien

Wegen der Verzögerung des Anwendungsbeginns von Solvency II hat EIOPA[14] Leitlinien erlassen, die der Vorbereitung auf die neuen Regelungen dienen sollen. Die EIOPA-Leitlinien zum Governance-System dienen derzeit der Vorbereitung auf die künftige Geltung von Solvency II. EIOPA wird die Leitlinien überarbeiten und in endgültige Leitlinien überführen, die nach dem 1. Januar 2016 gelten sollen. Die Leitlinien richten sich an die nationalen Aufsichtsbehörden der Mitgliedstaaten und sind

13 Vgl. hierzu oben B.III und B.V.
14 = European Insurance and Occupational Pensions Authority (Europäische Versicherungsaufsichtsbehörde).

für die Unternehmen unverbindlich. Die nationalen Aufsichtsbehörden können entscheiden, ob sie die Leitlinien umsetzen. Sie müssen berichten, ob sie umgesetzt haben. In jedem Fall ist eine nationale Umsetzung, ist eine Erklärung gegenüber EIOPA notwendig („comply-or-explain").

Die **Leitlinien zum Governance-System** enthalten zur Compliance-Funktion lediglich allgemeine Aussagen. Sie setzen sie als Schlüsselfunktion voraus, geben aber nicht vor, wie diese ausgestaltet werden soll.[15] In dem Abschlussbericht zur Konsultation der Leitlinien zum Governance-System betont EIOPA, dass es der Gestaltungsfreiheit der Unternehmen obliege zu entscheiden, wie die Compliance-Funktion am besten organisiert werden kann.[16]

4. Verlautbarungen der BaFin

Die BaFin hat als Adressat der „Vorbereitungsleitlinien" vollständig „comply" erklärt. Sie will diese bis zum vorgesehenen Anwendungsbeginn von Solvency II Anfang 2016 im Rahmen eines „strukturierten Dialogs" mit den Unternehmen sukzessive implementieren.

Zur Compliance-Funktion hat sich die BaFin in der am 9. Juli 2014 veröffentlichten konsultierten Fassung der Verlautbarung zu Themenblock 6 „Interne Kontrollen und interne Revision" geäußert: Sie erwartet im Grundsatz, dass die Compliance-Funktion auf Solo- und auf Gruppenebene implementiert und organisatorisch eingebunden wird. Bei der Ausgestaltung sollen die Unternehmen grundsätzlich frei sein, solange die Anforderungen der Solvency II-Rahmenrichtlinie an Schlüsselfunktionen eingehalten werden. Es ist zu erwarten, dass die BaFin ihre Aufsichtspraxis entsprechend den Äußerungen der Verlautbarung ausrichtet. Es ist daher wichtig, die inhaltlichen Grundzüge zu kennen. In der Folge wird an geeigneter Stelle auf entsprechende Aussagen hingewiesen.

15 EIOPA-Leitlinien zum Governance-System (Vorbereitungsphase), Leitlinien 5 und 9.
16 Abschlussbericht zur Konsultation der Leitlinien zum Governance-System (EIOPA/13/413), Ziff. 3.79 und 3.80.

D. Die Aufgabe der Compliance-Funktion

I. Begriff der Compliance-Funktion

Art. 13 Nr. 29 der Solvency II-Richtlinie definiert den Begriff der Funktion als „interne Kapazität innerhalb des Governance-Systems zur Übernahme praktischer Aufgaben". Für die Praxis ist von großer Bedeutung, die Compliance-Funktion klar von der Compliance-Organisation zu unterscheiden. Mit dem Begriff der Compliance-Funktion wird nicht vorgegeben, von wem und in welcher organisatorischen Form diese Funktion ausgeübt wird. Insbesondere ist die Compliance-Funktion grundsätzlich nicht mit einer eigenständigen Compliance-Abteilung gleichzusetzen. Dennoch ist es den Unternehmen möglich, ihr Governance-System so auszugestalten, dass Compliance-Funktion und Compliance-Abteilung identisch sind.

II. Aufgabe der Compliance-Funktion

Im Hinblick auf die Aufgabe der Compliance-Funktion sind drei Stufen zu unterscheiden:

- Die Solvency II-Rahmenrichtlinie stellt **Mindestanforderungen** an die Aufgabe der Compliance-Funktion. Sie formuliert damit ein aufsichtsrechtliches Pflichtprogramm für deren Tätigkeit.
- Jenseits der speziellen aufsichtsrechtlichen Compliance-Funktion unterliegen Versicherungsunternehmen – wie jedes andere Unternehmen – der **allgemeinen Legalitätspflicht**, stets alle für ihren Geschäftsbetrieb geltenden Vorschriften einzuhalten. Sie müssen daher alle Strukturen und Prozesse im Unternehmen so ausrichten, dass die Einhaltung sämtlicher externer und interner Vorschriften gewährleistet ist (siehe 2.).
- Es obliegt der **unternehmensorganisatorischen Entscheidung** einer im Unternehmen vorhandenen Compliance-Organisation, darüber hinausgehend Aufgaben zuzuweisen. Diese Entscheidung orientiert sich unter anderem **am spezifischen Risikoprofil** des Unternehmens (siehe 3.).

Die genaue **Unterscheidung** der Aufgaben nach ihrer Herleitung **hat nicht nur akademischen Charakter**, sondern praktische Konsequenzen: Die BaFin versteht ihr Aufsichtsmandat gemessen an der Solvency II-Richtlinie bislang sehr weit und behält sich vor, die Aufgabenerfüllung der Compliance-Funktion in den Versicherungsunternehmen umfassend zu überwachen. Eine Rechtsgrundlage für eine aufsichtsbehördliche Kontrolle ergibt sich jedoch nur im Hinblick auf die Aufgabe als spezielle aufsichtsrechtliche Compliance-Funktion, also soweit es um die Einhaltung der im Zusammenhang mit der Solvency II-Richtlinie erlassenen Vorschriften geht. Aufsichtsrechtliche Eingriffsbefugnisse wie z. B. Fragerechte oder die Abberufung

von Geschäftsleitern kann die BaFin daher nur im Hinblick auf dieses aufsichtsrechtliche Pflichtprogramm durchsetzen.

1. Aufsichtsrechtliches Pflichtprogramm nach Solvency II

a. Aufgaben gem. Art. 46 Solvency II-Rahmenrichtlinie

Die Aufgaben der Compliance-Funktion unter Solvency II ergeben sich aus Art. 46 Solvency II-Richtlinie. Sie können wie folgt zusammengefasst werden:

- **Überwachungsaufgabe:** Die Compliance-Funktion hat die Einhaltung der rechtlichen Anforderungen an das Versicherungsunternehmen zu überwachen.

  Die Solvency II-Richtlinie folgt in ihrem Governance-Konzept dem „Modell der drei Verteidigungslinien“: In der „1. Verteidigungslinie“ sind die Mitarbeiter/Führungskräfte dafür verantwortlich, Risiken im Tagesgeschäft zu identifizieren, zu analysieren und zu bewerten. Auf dieser Basis müssen erforderliche Kontrollen eingerichtet und durchgeführt werden. Die Compliance-Funktion agiert in der „2. Verteidigungslinie“. Sie überwacht, dass prozessintegrierte, compliance-relevante Kontrollen im operativen Bereich ordnungsgemäß durchgeführt werden. Zudem überwacht sie, dass die anderen Governance-Funktionen (Risikomanagement, Interne Revision, Versicherungsmathematische Funktion) ordnungsgemäß eingerichtet und wirksam sind. Nicht zwingend erforderlich ist es, dass die Compliance-Funktion selbst angemessene Kontrollen implementiert.[17] Auf der „3. Verteidigungslinie“ prüft schließlich die Revision das Governance-System prozessunabhängig und nachgelagert.
- **Beratungsaufgabe:** Zu den Aufgaben der Compliance-Funktion zählt ferner die Beratung des Vorstandes in Bezug auf die Einhaltung der in Übereinstimmung mit der Solvency II-Rahmenrichtlinie erlassenen Rechts- und Verwaltungsvorschriften und der auf dieser Basis ergangenen unternehmensinternen Leitlinien.
- **Risikokontrollaufgabe:** Die Compliance-Funktion soll das mit der Nicht-Einhaltung der rechtlichen Vorgaben verbundene Risiko („Compliance-Risiko“) identifizieren und beurteilen. Compliance-Risiken, die aus Sicht der BaFin durch die Compliance-Funktion identifiziert und bewertet werden sollen, sind das Risiko rechtlicher oder aufsichtsbehördlicher Sanktionen, das Risiko wesentlicher finanzieller Verluste und das Risiko von Reputationsverlusten, soweit diese Risiken aus der Nichteinhaltung externer Anforderungen oder interner Vorgaben resultieren.[18] Ein enger Austausch sowohl mit der Rechtsabteilung als auch mit der Risikomanagement-Funktion kann für eine solche Risikobewertung hilfreich sein.
- **Frühwarnaufgabe:** Zu den Aufgaben der Compliance-Funktion gehört auch die Beurteilung der möglichen Auswirkung von sich abzeichnenden Änderungen des

17 BaFin-Verlautbarung zu „Interne Kontrollen und interne Revision“, Rz. 31.
18 BaFin-Verlautbarung zu „Interne Kontrollen und interne Revision“, Rz. 34.

Rechtsumfeldes auf die Tätigkeit des betreffenden Unternehmens (Rechtsumfeldrisiken).[19] Davon umfasst sind alle Rechtsänderungs- und Rechtssprechungsrisiken, soweit diese den Versicherungsbetrieb betreffen. Unabhängig von der Frage, wie weit der aufsichtsrechtlich regulierte Teil der Frühwarnaufgabe reicht, hat sich jedes Unternehmen so zu organisieren, dass der Vorstand seiner Legalitätspflicht entsprechen kann. Dazu müssen die für das Versicherungsunternehmen relevanten Rechtsgebiete identifiziert werden sowie die in diesen Rechtsgebieten vorhandenen Rechtsänderungs- und Rechtsprechungsrisiken erkannt und bewertet werden. Die Compliance-Funktion muss dazu unter anderem die relevanten politischen Entwicklungen auf nationaler und internationaler Ebene sowie die einschlägige Rechtsprechung laufend verfolgen und systematisch analysieren. Dies muss auch unter Solvency II nicht vollumfänglich durch eine zentrale Compliance-Abteilung selbst geschehen. Vielmehr bieten sich sachgerechte Schnittstellen zu anderen Bereichen an, in denen Rechtsbeobachtung bereits geleistet wird.

b. Rechtlicher Tätigkeitsumfang der Compliance-Funktion

Die Compliance-Funktion soll nach § 29 Abs. 1 VAG-E die Einhaltung der (d. h. aller) Anforderungen an das Unternehmen überwachen. Für die Beratung des Vorstands beschränkt § 29 Abs. 2 VAG-E den Umfang auf die „Einhaltung der Gesetze und Verwaltungsvorschriften, die für den Betrieb des Versicherungsgeschäftes gelten". Die BaFin führt in der konsultierten Fassung der Verlautbarung zu Themenkomplex 6 „Interne Kontrollen und interne Revision" aus, dass die Compliance-Funktion bei ihrer Überwachungsaufgabe „die Einhaltung aller zu beachtenden Gesetze und Verordnungen [und] aller regulatorischen Anforderungen" zu überwachen hat (Rz. 31). Die Beratungsaufgabe der Compliance-Funktion sei auf die „Einhaltung der für den Betrieb des Versicherungsgeschäftes geltenden Gesetze, Verordnungen und regulatorischen Anforderungen" bezogen (Rz. 32).

Sowohl das Verständnis des Gesetzgebers als auch das der BaFin ist aus Sicht des Verbandes, gemessen an der Richtlinie, zu weitgehend. Die Diskussion hierüber ist allerdings noch im Fluss. Der **Tätigkeitsumfang** der Compliance-Funktion umfasst nach Solvency II nur die Einhaltung **aller** Rechts- und Verwaltungsvorschriften, die **zur Umsetzung der Solvency II-Rahmenrichtlinie** erlassen wurden. Für die Beratungsaufgabe ergibt sich dies bereits nach dem eindeutigen Wortlaut der Richtlinie. Für die weiteren Aufgaben lässt sich diese Beschränkung systematisch mit Blick auf Art. 40 der Richtlinie begründen: Danach tragen die Geschäftsleiter die „letztendliche Verantwortung für die Einhaltung der gem. [der Solvency II-] Richtlinie erlassenen Rechts- und Verwaltungsvorschriften". Da die Compliance-Funktion eine delegierte Vorstandspflicht ist, kann ihr Verantwortungsumfang nicht über den der Geschäftsleitung hinausgehen.

19 BaFin-Verlautbarung zu „Interne Kontrollen und interne Revision", Rz. 33.

c. Sachliche Reichweite

Der Pflichtenkreis der Compliance-Funktion unter Solvency II umfasst zunächst die aufsichtsrechtlichen Vorgaben, die das VAG für den Betrieb des Versicherungsgeschäfts vorsieht. Dazu gehören die Anforderungen im Hinblick auf die Organisation und die zulässigen Aktivitäten der Versicherungsunternehmen. Weitere inhaltliche Vorgaben in Bezug auf die Rechtmäßigkeit der Produkte enthält das Versicherungsvertragsrecht (VVG). Schließlich muss die Compliance-Funktion unter Solvency II sicherstellen, dass das Vermittlerrecht bei dem Vertrieb der verschiedenen Versicherungsprodukte beachtet wird.

Nur soweit es sich um die Einhaltung dieser spezifischen, im Zusammenhang mit der Solvency II-Richtlinie erlassenen Vorschriften handelt, unterliegt die Aufgabe als spezielle aufsichtsrechtliche Compliance-Funktion der aufsichtsbehördlichen Kontrolle. Nach der BaFin-Verlautbarung zu Themenkomplex 6 ist aber davon auszugehen, dass die BaFin ihr Aufsichtsmandat ungeachtet der fehlenden rechtlichen Grundlage weiter versteht und auch auf die sonstigen Aufgaben der Compliance-Funktion (siehe unter 2.) erstrecken will.

2. Sonstige Aufgaben der Compliance-Funktion

Jenseits der speziellen aufsichtsrechtlichen Compliance-Funktion unterliegen Versicherungsunternehmen – wie jedes andere Unternehmen – der allgemeinen Legalitätspflicht. Daraus resultiert die Pflicht alle Strukturen und Prozesse im Unternehmen so auszurichten, dass die Einhaltung sämtlicher externer und interner Vorschriften gewährleistet ist. Aufgabe dieser Compliance-Funktion ist es, eine unternehmensindividuelle Analyse der Risiken durchzuführen, die aus der Nichteinhaltung dieser rechtlichen Anforderungen resultieren können. Auf dieser Basis muss unternehmensindividuell beurteilt werden, ob und wenn ja welche Vorkehrungen erforderlich sind, um die festgestellten Risiken auszuschließen bzw. zu reduzieren.

Diese Risikoanalyse und die Festlegung des „Ob“ und des „Wie“ von Vorkehrungen sind im weiteren Verlauf regelmäßig zu überprüfen: Einerseits ist also zu definieren, hinsichtlich welcher rechtlichen Anforderungen Ressourcen des Unternehmens im Sinne von eigenständigen Compliance-Aktivitäten als „2. Verteidigungslinie“ eingesetzt und vorgehalten werden sollen. Andererseits ist festzulegen, welche Maßnahmen dazu mit welchen Mitarbeiterkapazitäten oder sonstigen Ressourcen jeweils vorzunehmen sind.

Der sachliche Anwendungsbereich dieser Compliance-Funktionen umfasst zunächst alle auf den Geschäftsbetrieb des jeweiligen Unternehmens anwendbaren **externen Vorschriften**.

a. Aufsichtsnahe Rechtsgebiete

Besondere Bedeutung kommt in diesem Zusammenhang für Versicherungsunternehmen der Einhaltung der aufsichtsnahen Rechtsgebiete zu. Wenngleich diese Vorschriften nicht im Zusammenhang mit der Solvency II-Richtlinie erlassen wurden und daher nicht der speziellen aufsichtsrechtlichen Compliance-Funktion unterliegen, sollten wegen der im Versicherungsgeschäft regelmäßig im Hinblick auf entsprechende Normverstöße bestehenden hohen Risiken Vorkehrungen zu ihrer Einhaltung getroffen werden. Zu nennen sind hier zunächst **Datenschutzrecht, Geldwäschegesetz** und verwandte Rechtsgebiete wie **Sanktionsrecht** und **Terrorismusfinanzierung**. Zur Sicherstellung der Normenkonformität werden den Normadressaten dieser Vorschriften vielfach bereits vom Gesetz spezielle aufbau- und ablaufbezogene Vorkehrungen wie Kundenidentifizierungs- und Meldepflichten als Bestandteil ihrer Compliance-Funktion vorgeschrieben.[20] Darüber hinaus verpflichten Datenschutzrecht und Geldwäschegesetz die betroffenen Unternehmen zur Bestellung besonderer Beauftragter mit speziellen Aufgaben zur Sicherstellung der Normbefolgung.

Weitere aufsichtsnahe Rechtsgebiete mit besonderer Relevanz für den Versicherungsbetrieb stellen die allgemeinen **Bilanzregeln**[21] sowie die für Vermögens-/Kapitalanlagen und Finanzierungsgeschäfte geltenden Regeln wie bspw. **WpHG** sowie die sonstigen speziellen finanzwirtschaftlichen Regeln (**KAGB**) dar. Als Aufgabe der Compliance-Funktion hat das Unternehmen in diesem Bereich insbesondere die Erfassung von Insiderinformationen, das Führen von Insiderverzeichnissen, die Meldung von Directors‘ Dealings sowie die Anzeige des Über-/Unterschreitens der relevanten Schwellenwerte (insbesondere §§ 21 ff. WpHG) sicherzustellen.

Schließlich steht im Bereich der aufsichtsnahen Regeln das Thema „**Compliance im Vertrieb**“: Neben der Einhaltung der anlassbezogenen Beratungs- und Informationspflichten der Vermittler, der Anforderungen an die mit dem Vertrieb von Versicherungen befassten Personen sowie der Pflichten zur Offenlegung der Vertriebs- und Verwaltungskosten, die der speziellen aufsichtsrechtlichen Compliance zuzuordnen sind, liegt hier eine Schwerpunktaufgabe der Compliance-Funktion. Dazu gehören beispielsweise ein Verhaltenskodex für die Vermittler sowie Schulungs- und Überwachungsmaßnahmen, die die Einhaltung auch der über regulatorische Anforderungen hinausgehenden Regeln sicherstellen sollen.

b. Kartellrecht

Im Lichte der hohen Bußgelder und enormen Schadenersatzrisiken wird ein Versicherungsunternehmen häufig im Zuge der Risikoanalyse erwägen, im Rahmen der Compliance-Funktion auch zur Einhaltung der kartellrechtlichen Vorschriften besondere

20 Davon zu unterscheiden ist die Frage, inwieweit diese spezialgesetzlichen Aufgaben der Compliance-Funktion auch der Compliance-Organisation des Unternehmens zugewiesen werden. Siehe dazu unter E.

21 Dagegen unterliegen die besonderen solvabilitätsbezogenen Regelungsvorschriften sowie die aufsichtsrechtlichen Kapitalanlagevorschriften bereits der speziellen aufsichtsrechtlichen Compliance-Funktion. Siehe dazu unter II.

Vorkehrungen zu treffen. Im Vordergrund stehen dabei die Verbote aller wettbewerbsbeschränkenden Vereinbarungen und abgestimmter Verhaltensweisen sowie ggf. der Marktmissbrauchsregeln, deren Befolgung durch hinreichende Information der Mitarbeiter (beispielsweise durch Merkblätter, Schulungen etc.) und regelmäßige Kontrollmaßnahmen (beispielsweise Compliance-Audits) erreicht werden sollen.

c. Korruptionsbekämpfung

Weiterer Kernbereich der Compliance-Funktion ist typischerweise die Korruptionsprävention. Ziel der Compliance-Funktion in diesem Rahmen ist, durch Präventions- und Überwachungsmaßnahmen jeglicher Form von Korruption, namentlich der Vorteilsgewährung/-annahme im Sinne der §§ 299 StGB sowie der besonderen Straftatbestände für Amtsträger vorzubeugen.

In bestimmten Fällen haben auch ausländische Rechtsordnungen Einfluss auf dieses Thema. So können insbesondere Gesellschaften mit Geschäftstätigkeit im Ausland z. B. unter den UK Bribery Act 2010 oder den U.S. Foreign Corrupt Practices Act („FCPA“) fallen. Der UK Bribery Act 2010 stellt im Rahmen des Unternehmensstrafrechts die aktive und passive Bestechung, die Bestechung ausländischer Amtsträger und das Versäumnis, Bestechung zu vermeiden, unter Strafe. Er gilt nicht nur für britische Unternehmen, sondern für alle, die in irgendeiner Form in Großbritannien Geschäfte machen oder andere Bezugspunkte zu Großbritannien haben. Nur wer im Ernstfall vor Gericht Existenz und grundsätzliche Wirksamkeit von Kontrollen im eigenen Unternehmen nachweisen kann, hat eine Chance, nach dem UK Bribery Act straffrei zu bleiben. Für Unternehmen mit Geschäftstätigkeit und/oder Börsenzulassung in den USA ist der FCPA von erheblichem Interesse. Dieser regelt die Ahndung der Korruption ausländischer Amtsträger und eine entsprechende korrekte, transparente Buchführung. Dem Anwendungsbereich des FCPA unterfällt ein Unternehmen bereits bei geringfügigen Berührungspunkten mit den USA (z. B. Arbeit über einen amerikanischen Server, E-Mail an amerikanischen Empfänger).

Wegen der Schwierigkeit, die sehr generalklauselartig gefassten strafrechtlichen Tatbestandsmerkmale auf möglicherweise kritische Situationen des beruflichen Alltags (z. B. Einladungen, Geschenke von Geschäftspartnern) richtig einschätzen zu können, gehört es zur „best practice“, den Mitarbeitern/ggf. Vermittlern durch unternehmensindividuelle Richtlinien (Verhaltenskodices) konkrete Verhaltensmaximen in Bezug auf Erhalt und Vergabe von Zuwendungen geben. Der GDV hat dazu die „Unverbindliche Orientierungshilfe zu Einladungen und Geschenken gegenüber Geschäftspartnern und Amtsträgern“ herausgegeben, die § 299 StGB und die §§ 331 ff. StGB als rechtlichen Maßstab wählt.[22]

22 GDV-Orientierungshilfe für Einladungen und Geschenke an Geschäftspartner und Amtsträger, abrufbar im VIS.

3. Aufgaben der Compliance-Funktion nach unternehmensinternen Anforderungen in Abhängigkeit vom Risikoprofil

Der Compliance-Funktion können nach unternehmensspezifischen Anforderungen und abhängig vom Risikoprofil des Unternehmens weitere Aufgaben übertragen werden. Ausgangspunkt ist auch hier die unternehmensindividuelle Risikoentscheidung: Danach können entweder für allgemeine Prozessabläufe oder für bereichsspezifische Themen unternehmensinterne Anforderungen aufgestellt und die Vorsorge zu deren Einhaltung und ggf. die Kontrolle der Compliance-Funktion zugewiesen werden. Für die Praxis besonders relevant sind regelmäßig zusätzliche Regelungen zu Interessenkonflikten.[23] Diese zielen darauf ab, Konflikte zwischen den persönlichen Interessen der für sie tätigen Personen und den unternehmerischen Interessen zu vermeiden. Es soll zudem sichergestellt werden, dass mit entstandenen Interessenkonflikten mit der gebotenen Sorgfalt umgegangen wird. Weitere Beispiele für besondere unternehmensinterne Anforderungen sind: Regelungen zu Nebentätigkeiten, Einkaufsrichtlinien, Anwenderhandbücher zur IT-Sicherheit oder Regelungen zur Fortbildung von Mitarbeitern im Vertrieb/Vermittlern.

23 Das Thema Interessenskonflikte steht derzeit sowohl europäisch als auch national im Fokus der Aufsicht.

E. Ausgestaltung der Compliance-Funktion in der Unternehmens-Organisation

Die unter C. skizzierten (aufsichts-)rechtlichen Vorgaben haben erhebliche Auswirkungen darauf, wie die Compliance-Funktion in den Versicherungsunternehmen ausgestaltet werden muss. Nachfolgend sollen praktische Hinweise für die Umsetzung gegeben werden. Zu berücksichtigen ist, dass die Diskussion zu vielen Problemen derzeit noch im Fluss ist. Auch die BaFin und EIOPA haben sich noch nicht zu allen Themen abschließend geäußert. Soweit bereits Aussagen der Aufsicht vorliegen, wird auf diese hingewiesen.

I. Allgemeine Prinzipien

- **Gestaltungsfreiheit im Rahmen der allgemeinen Organisationspflicht**

  Die Organisationsform bzw. die konkreten Prozessabläufe der Compliance-Funktion sind nicht detailliert vorgegeben. Die Solvency II-Richtlinie verfolgt den Ansatz einer prinzipienbasierten Regulierung. Es obliegt deshalb der Entscheidung der Unternehmen, wie diese die in der Richtlinie vorgegebenen Ziele erreichen. Aus der prinzipienbasierten Regulierung folgt für die Unternehmen im Rahmen der nationalen Umsetzung und der delegierten Rechtsakte eine weitgehende Freiheit im Hinblick auf die Ausgestaltung ihrer Corporate Governance.[24]

- **Proportionalitätsgrundsatz**

  Bei der Aufgabenwahrnehmung durch die Compliance-Funktion ist der **aufsichtsrechtliche Proportionalitätsgrundsatz** (Art. 41 Abs. 2 Solvency II-Richtlinie) zu beachten. Danach hängen die Anforderungen an die organisatorischen Maßnahmen zur Erfüllung der Compliance-Funktion wesentlich von der Größe sowie von Art und Umfang der Geschäftstätigkeit und des damit verbundenen Risikos ab. Wichtig ist, dass sich der Proportionalitätsgrundsatz nicht auf das „Ob“ der Aufgabenwahrnehmung durch die Compliance-Funktion, sondern immer nur auf deren Reichweite und Tiefe („Wie“) auswirkt.[25] Neben der Größe des Unternehmens haben etwa die Art, Umfang und regionale Ausdehnung des betriebenen Versicherungsgeschäfts, die Vertriebsformen einschließlich etwaiger Vertriebskooperationen sowie eine Börsennotierung wesentlichen Einfluss auf die Compliance-Themen und deren Komplexitätsgrad. Art und Umfang der organisatorischen Maßnahmen müssen hierzu in einem angemessenen Verhältnis stehen. Das Argument fehlender interner Kapazitäten wird von der Aufsicht hingegen nicht akzeptiert.

24 BaFin-Verlautbarung zu „Interne Kontrollen und interne Revision“, Rz. 29; Abschlussbericht zur Konsultation der Leitlinien zum Governance-System (EIOPA/13/413).

25 BaFin-Verlautbarung zu „Interne Kontrollen und interne Revision“, Rz. 5.

- **Ausreichende Befugnisse und Unabhängigkeit**

  Bei der Organisation der Compliance-Funktion sind die **zur Aufgabenerfüllung notwendigen Befugnisse und die gebotene Unabhängigkeit** sicherzustellen.[26] Nach Ansicht der BaFin ist die Compliance-Funktion so einzurichten, dass sie jederzeit frei von Einflüssen ist, die eine objektive, faire und unabhängige Aufgabenerfüllung beeinträchtigen können.[27]

  Zu den notwendigen Kompetenzen gehört insbesondere der Zugang zu Informationen und Mitarbeitern. Ferner muss der Compliance-Funktion das Recht auf Durchführung von Prüfungen und Untersuchungen möglicher Compliance-Verstöße eingeräumt sein; in ernsten Fällen auch unter Hinzuziehung von internen oder externen Sachverständigen. Selbstverständlich ist schließlich die Möglichkeit freier Berichterstattung im Rahmen der dafür vorgesehenen Berichtslinien an die Geschäftsleitung bzw. das zuständige Aufsichtsgremium.

- **Gruppendimensionale Ausgestaltung**

  Bei der Ausgestaltung der Compliance-Funktion in Unternehmensgruppen sind die Anforderungen in Art. 246 Solvency II-Richtlinie sowie die nationale Umsetzung in § 275 Abs. 1 VAG-E zu berücksichtigen. Danach muss die Compliance-Funktion (wie auch die übrigen Schlüsselfunktionen) auf Gruppenebene eingerichtet und entsprechend gemeinsamer Mindeststandards gruppenweit gesteuert werden.

II. Zentrale oder dezentrale Organisation

1. Organisationsfreiheit

Es obliegt dem Unternehmen zu entscheiden, inwieweit es seine Compliance-Funktion zentralen oder dezentralen Einheiten überträgt. Selbst bei Einrichtung einer zentralen Compliance-Organisation können im Regelfall aber nicht alle Themen der Compliance-Funktion durch diese abgedeckt werden.

Unabhängig von der Frage einer eigenständigen Compliance-Abteilung ist die Benennung eines Verantwortlichen für die Compliance-Funktion (Schlüsselfunktionsinhaber) durch die Geschäftsleitung erforderlich und wird von der Aufsicht erwartet. Im Falle einer zentralen Compliance-Abteilung gibt es ohnehin einen Compliance-Officer. Bei einer dezentralen Organisation ist es beispielsweise möglich, dass der Leiter der Rechtsabteilung mit dieser Aufgabe betraut wird.

26 Vgl. hierzu Art. 268 DDA.
27 BaFin-Verlautbarung zu „Interne Kontrollen und interne Revision“, Rz. 29f.

2. Dezentrale Organisation mit Compliance-Beauftragten

Bei dieser Organisationsstruktur sind die mit einzelnen Compliance-Aufgaben und Verantwortlichkeiten beauftragten Mitarbeiter den verschiedenen Bereichen zugeordnet (Compliance-Beauftragte). Welche Stellen im Unternehmen die Compliance-Funktion wahrnehmen, ist in der Compliance-Leitlinie zu definieren. Hinzu kommen die Sonderfunktionen des Datenschutzbeauftragten und des Geldwäschebeauftragten. Jedoch muss auch bei diesem Ansatz ein zentral verantwortlicher Compliance-Officer benannt sein. Es ist daher empfehlenswert, dass dieser regelmäßig bzw. ad hoc über die Tätigkeit der Compliance-Beauftragten informiert wird.[28]

Darüber hinaus wird zu prüfen sein, inwieweit für einzelne Themenbereiche zudem Ausschüsse oder Arbeitskreise zu bilden sind, in denen diese Compliance-Beauftragten wesentliche Themen gemeinsam behandeln und entscheiden können. Die Mitglieder der Ausschüsse sind in dieser Struktur dem Compliance-Officer in der Regel nicht disziplinarisch unterstellt, sondern nehmen ihre Compliance-Aufgabe im Rahmen ihres jeweiligen Ressorts wahr und berichten dort anfallende Compliance-Themen auch an die jeweils zuständigen Vorstandsmitglieder. Eine zusätzliche Berichtslinie an den Compliance-Officer – insbesondere zu aktuellen Compliance-Fällen – ist jedoch empfehlenswert.

3. Zentrale Compliance-Abteilung

Bei einer zentralen Ausgestaltung wird eine eigenständige Abteilung unmittelbar unterhalb der Geschäftsleiterebene eingerichtet. Denkbar sind aber auch eine Compliance-Gruppe oder spezialisierte Mitarbeiter im Rechtsbereich, wenn deren Leiter zugleich die Funktion des Compliance-Officer wahrnimmt. Für eine spezielle Compliance-Abteilung können je nach Größenordnung und Komplexitätsgrad des Geschäftsbetriebs Kapazitätsgründe, Effizienzgewinne im Bereich der Schnittstellen und der Koordination sowie bessere Voraussetzungen für die Fokussierung und den Aufbau spezieller Expertise sprechen. Bisweilen spielt auch die Betonung des Compliance-Gedankens im Innen- und im Außenverhältnis eine gewisse Rolle.

Aktuell finden sich in den Konzernorganisationen ebenso eine Mischform mit einer eigenständigen Compliance-Abteilung in der Muttergesellschaft und einer dezentralen Struktur auf der Tochterebene. Hierbei ist jedoch sicherzustellen, dass auch hier die Rolle und Verantwortlichkeit der Compliance-Funktion auf Ebene der Tochtergesellschaft ausreichend definiert und festgelegt ist und dass ein Berichtswesen sowohl an die Geschäftsleitung auf Ebene der Tochtergesellschaft eingerichtet ist als auch eine ergänzende Berichtlinie an die zentrale Organisationseinheit auf Ebene der Muttergesellschaft.

28 Vgl. zu den Berichtswegen unten E.V.

III. Organisatorisches Verhältnis zu anderen Schlüsselfunktionen und Unternehmensbereichen

Für eine effektive Aufgabenerfüllung der Compliance-Funktion bietet es sich an, eng mit den anderen Schlüsselfunktionen sowie weiteren Unternehmenseinheiten zusammenzuarbeiten. Hierbei ist es besonders wichtig, dass zwischen den organisatorischen Einheiten ein wirksamer Informationsaustausch erfolgt. Zu den Möglichkeiten einer effektiven Kooperation und den Anforderungen an die entsprechenden Schnittstellen hat der GDV ein Diskussionspapier mit detaillierten Hinweisen veröffentlicht.[29]

Eine häufig aufgeworfene Frage ist, ob und in welcher Form eine organisatorische Kombination der Schlüsselfunktionen möglich ist. Dabei sind auch weitere Unternehmenseinheiten (wie die Rechtsabteilung) oder auch die schon nach gesetzlichen Anforderungen bestellten Geldwäsche- und Datenschutzbeauftragten zu berücksichtigen.

Im Grundsatz gilt, dass die Versicherer in der organisatorischen Ausgestaltung der Schlüsselfunktionen frei sind. Nach den europäischen Vorgaben soll es in kleinen und weniger komplexen Unternehmen möglich sein, mehr als eine Funktion auf eine Person oder Organisationseinheit zu vereine.[30] Eine organisatorische Kombination von Funktionen muss aber auch in mittleren und größeren Unternehmen möglich sein, soweit dies dem Risikoprofil entspricht. Dabei ist sicherzustellen, dass jede Schlüsselfunktion frei von Einflüssen bleibt, die gefährden, dass sie ihren Pflichten objektiv, fair und unabhängig nachkommen kann.[31] Dies bedingt nicht zwingend eine Trennung von Schlüsselfunktionen, vielmehr kann dies bei der organisatorischen Ausgestaltung auch durch flankierende Maßnahmen (die sich unternehmensindividuell wieder am Risikoprofil und Proportionalitätsgrundsatz zu orientieren haben) ausgestaltet werden. Hingegen ist gemäß Ziff. 131 der BaFin-Verlautbarung zu den „Allgemeinen Governance-Anforderungen“ eine Zuweisung der Verantwortung für eine Schlüsselfunktion an mehrere Personen aus Sicht der Aufsicht generell unzulässig.

Hinsichtlich solcher flankierender Maßnahmen gilt, dass diese unternehmensindividuell, risikoorientiert und unter Berücksichtigung des Proportionalitätsgrundsatzes auszugestalten sind. Denkbar sind klar definierte Berichtslinien der Schlüsselfunktionen zum Vorstand, klar definierte Zuständigkeiten und Abgrenzung der Schlüsselfunktionen, klar definierte Aufgaben- und Stellenbeschreibungen, eine Absicherung, dass sich Interessenkonflikte nicht ergeben durch ein transparentes 4-Augen-Prinzip, Verlagerung von Aufgaben bei Interessenkonflikten auf einen Stellvertreter.

29 GDV-Diskussionspapier „Governance-Funktionen unter Solvency II: Kernaufgaben und Schnittstellen“.
30 Erwägungsgrund 32 der Solvency II-Richtlinie.
31 Art. 268 Abs. 1 DDA.

Sämtliche Schnittstellen der Compliance-Organisation und -Funktion sollten in unternehmensinternen Leitlinien und im CMS beschrieben sein.

In Bezug auf **das organisatorische Verhältnis** der Compliance-Funktion **zu** der **Internen Revision**, der **Versicherungsmathematischen Funktion** sowie der **Risikomanagement-Funktion** wird auf das GDV-Diskussionspapier „Governance-Funktionen unter Solvency II: „Kernaufgaben und Schnittstellen“ verwiesen.

- **Verhältnis der Compliance-Funktion zur Rechtsabteilung**

  Die Überschneidung der Aufgaben der Compliance-Organisation mit der Rechtsabteilung ist naturgemäß hoch, da es im Kern um die Sicherstellung rechtmäßigen Verhaltens geht. Bei einzelnen Aufgaben der Compliance-Funktion ist die Affinität zum materiellen Recht besonders hoch, etwa im aufsichtsrechtlichen Bereich, bei der kartellrechtlichen Compliance oder der Beratung zur Entwicklung von Gesetzgebung und Rechtsprechung. Im Vergleich zur klassischen Aufgabenstellung einer Rechtsabteilung gibt es jedoch Unterschiede. Hervorzuheben ist die systematisch präventive und überwachende Funktion von Compliance. Dies bedingt eine entsprechende Ausrichtung und eine engere operative Einbindung der mit Compliance-Aufgaben betrauten Mitarbeiter. Die Rechtsabteilung ist keine der zwingend durch Solvency II vorgesehenen Schlüsselfunktionen, kann aber unternehmensindividuell als „andere Schlüsselaufgabe“ definiert werden.

  Sofern es eine eigenständige Compliance-Abteilung gibt, werden dort Compliance-Aufgaben gebündelt. Auch in diesem Fall empfiehlt es sich, rechtsspezifische Aufgaben, die unter die Compliance-Funktion fallen, von der Rechtsabteilung wahrnehmen zu lassen, sofern in der Compliance-Abteilung das notwendige rechtliche Know-how nicht selbst vorgehalten wird. Werden hiernach Compliance-Aufgaben der Rechtsabteilung zugewiesen, muss jedoch darauf geachtet werden, dass die notwendige Unabhängigkeit gewahrt ist (vgl. hierzu unter E.I.). Ferner muss die Verantwortung für die Erfüllung dieser Aufgaben eindeutig geklärt sein. Sofern der Inhaber der Compliance-Funktion nicht der Rechtsabteilung angehört, hat er sich im Hinblick auf seine Verantwortung für die Schlüsselfunktion Compliance von der ordnungsgemäßen Wahrnehmung zu vergewissern.

  Die BaFin hat gelegentlich Skepsis hinsichtlich einer Kopplung gezeigt, da sie Interessenskonflikte befürchtet. Nach Ansicht des Verbandes kann jedoch jedes Unternehmen grundsätzlich frei entscheiden, ob es die beiden Bereiche organisatorisch zusammenfassen oder trennen bzw. einzelne Compliance-Aufgaben der Rechtsabteilung zuweisen möchte. Interessenskonflikte können allerdings auftreten, wenn die Rechtsabteilung operative Tätigkeiten ausübt, z. B. eigenständig Risikopositionen verwaltet. In diesem Fall muss durch flankierende organisatorische Maßnahmen die gebotene Unabhängigkeit, z. B. durch die Einrichtung klar getrennter Berichtswege, gewährleistet sein.

- **Koppelung der Compliance-Funktion mit dem Geldwäschebeauftragten**

  Der Geldwäschebeauftragte ist ein durch das Geldwäschegesetz (GwG) vorgeschriebener Betriebsbeauftragter. Seine gesetzlich zugewiesenen Befugnisse sollen dem Allgemeinwohlinteresse dienen. Sofern im Unternehmen ein Compliance-Beauftragter vorhanden ist, nimmt dieser dem Vorstand obliegende Pflichten im Wege der Delegation wahr. Beide Positionen sind gleichermaßen, wenn auch konzeptionell unterschiedlich, dem Vorstand gegenüber berichtspflichtig (vgl. § 9 Abs. 2 Nr. 1 GwG).

  Die originäre Aufgabe des Geldwäschebeauftragten, die Einhaltung der GwG-Vorschriften sicherzustellen, ist grundsätzlich mit der Stellung als Compliance-Beauftragter vereinbar und Teil der Compliance-Funktion. Auch hier ist aber sicherzustellen, dass es nicht zu Interessenkonflikten kommt. Diese könnten sich beispielhaft ergeben, wenn die Geldwäscheorganisation vom Compliance-Beauftragten geprüft wird. Auch sind die vorstehend beispielhaft genannten organisatorischen Maßnahmen zur Absicherung der jeweiligen Aufgaben möglich.

- **Koppelung der Compliance-Funktion mit dem Datenschutzbeauftragten**

  Höher sind die Hürden bezüglich der Koppelung mit dem Datenschutzbeauftragten. Dem Datenschutzbeauftragten ist für den Bereich der Verarbeitung personenbezogener Daten eine umfassende Überwachungstätigkeit zugewiesen. Der Datenschutzbeauftragte soll seine Aufgabe nach § 4f Abs. 3 S. 2 BDSG aber unabhängig und vor allem weisungsfrei wahrnehmen können. Diese Tätigkeitsbeschreibung kann mit der Stellung des Compliance-Beauftragten im Unternehmen kollidieren. Denn dieser nimmt delegierte Leitungsaufgaben wahr und unterliegt daher verschärften Berichts- und Rechenschaftspflichten gegenüber der Leitungsebene.

  Nimmt der Compliance-Beauftragte z. B. selbst Ermittlungen vor, kann es zu einem Interessenkonflikt bei der datenschutzrechtlichen Bewertung der eigenen Compliance-Prozesse kommen. Die Compliance-Funktion erhebt i. d. R. selbst Daten, wertet sie aus und speichert, was ebenfalls eine Kollision der Interessen bedeuten kann.

  Vereint man beide Funktionen in ein und derselben Person, muss daher sichergestellt sein, dass Interessenskonflikte vermieden werden und die Weisungsgebundenheit nicht die Unabhängigkeit des anderen Bereiches beeinträchtigt. In Betracht kommt, klar getrennte Berichtswege einzurichten.

- **Organisatorisches Verhältnis der Compliance-Funktion zu anderen Unternehmensbereichen**

  Nach den vorangehend dargestellten Grundsätzen ist eine organisatorische Kombination der Compliance-Funktion auch mit anderen als den genannten Schlüsselfunktionen/Unternehmensbereichen denkbar. Rechtlich ist dies nicht ausgeschlossen, solange die jeweilige Aufgabenerfüllung hierdurch nicht beeinträchtigt wird.

IV. Outsourcing der Compliance-Funktion

1. Rechtliche Vorgaben

Ein Outsourcing liegt vor, wenn die Compliance-Funktion durch einen externen Dienstleister übernommen wird.[32] Dabei kann es sich auch um ein Unternehmen der gleichen Gruppe handeln (dazu unter 4.).

Nach **Art. 38 und Art. 49** der Solvency II-Richtlinie gelten bestimmte aufsichtsrechtliche Anforderungen, wenn es sich um die Ausgliederung von „Funktionen oder Versicherungs- oder Rückversicherungstätigkeiten" handelt. Art. 49 Abs. 2 und 3 Solvency II-Richtlinie sehen im Fall der Ausgliederung von kritischen und wichtigen Funktionen oder Versicherungstätigkeiten darüber hinausgehend besondere Organisations- und Anzeigepflichten vor. Wichtig ist, dass gem. Art. 49 Abs. 1 Solvency II-Richtlinie die ausgliedernden Versicherungsunternehmen voll für die Einhaltung der aufsichtsrechtlichen Vorgaben bei dem Dienstleister verantwortlich bleiben.

Die Vorgaben der Richtlinie werden durch die delegierten Rechtsakte auf Level 2 konkretisiert. Auch diese unterscheiden wie die Richtlinie zwischen **kritischen oder wichtigen operativen Funktionen oder Tätigkeiten** einerseits und sonstigen Tätigkeiten anderseits. Nur die Ausgliederung kritischer oder wichtiger Funktionen oder Tätigkeiten wird nach **Art. 274 DDA** strengeren Anforderungen unterworfen: Dies betrifft insbesondere die Auswahl des Dienstleisters sowie die Gestaltung der vertraglichen Beziehungen. Für den Inhalt des Ausgliederungsvertrags selbst macht Art. 274 Abs. 4 DDA konkrete Vorgaben. Nach Art. 41 Abs. 3 Solvency II-Richtlinie sowie Art. 274 Abs. 1 DDA haben die Unternehmen zudem **schriftliche Leitlinien zum Outsourcing** zu erstellen und mindestens jährlich zu überprüfen. Erforderlich ist zudem, dass der Dienstleister über angemessene finanzielle Ressourcen und Notfallpläne verfügt (Art. 274 Abs. 5 lit. c) DDA). Vorgaben für unkritische oder weniger wichtige Tätigkeiten werden hier nicht gemacht. Gleichwohl muss auch dieses Outsourcing sinnvoll in Unternehmensprozesse eingegliedert sein.

Im Zuge der VAG-Novelle 2014 wird der deutsche Gesetzgeber diese europäischen Vorgaben in nationales Recht überführen. In dem aktuellen Referentenentwurf des neuen VAG enthält § 32 VAG-E entsprechende Vorschriften.

2. Aufsichtsbehördliche Konkretisierung

Die BaFin hat angekündigt, Anfang 2015 im Rahmen der Vorbereitungshase eine Verlautbarung zum Thema Outsourcing zu veröffentlichen, in der weitere Konkretisierungen vorgenommen werden sollen. Bereits zum jetzigen Zeitpunkt hat die BaFin einige Aspekte der Ausgliederung behandelt. In der Verlautbarung zu den Fit & Proper-Anforderungen vom 30. April 2014 schreibt die BaFin in Rz. 33 vor, dass Versi-

32 Zur Definition der Solvency II-Richtlinie vgl. Art. 13 Nr. 28.

cherungsunternehmen beim Outsourcing von Schlüsselfunktionen einen Ausgliederungsbeauftragten zu benennen haben, der die operative Verantwortung für eine ordnungsgemäße Leistungserbringung durch den Dienstleister trägt.

EIOPA hat die aufsichtsrechtlichen Anforderungen an das Outsourcing in ihren **Leitlinien zum Governance-System** näher erläutert. Auch hier sind besondere Anforderungen für **kritische oder wichtige operative Funktionen oder Tätigkeiten** vorgesehen. Bei der Ausgliederung der Compliance-Funktion sollen die schriftlichen Leitlinien der Versicherungsunternehmen folgende Punkte beinhalten:

- **Zur internen Organisation:**
  - Erläuterung, warum Outsourcing ggf. sinnvoll;
  - Kriterien für die Einstufung einer Funktion/Tätigkeit als kritisch oder wichtig;[33]
  - Auslagerung von Schlüsselfunktionen – Fit & Proper-Anforderungen des Verantwortlichen im Unternehmen und der Mitarbeiter beim Dienstleister;[34]
  - Regelungen zum Managen und Überwachen des Outsourcings;[35]
  - Wahrung der Steuer- und Kontrollmöglichkeiten der Geschäftsleitung.[36]
- **Zur externen Organisation:**
  - Unternehmensinterner Prozess zur Auswahl der Dienstleister („due diligence process“);
  - Vertragsinhalte mit dem Dienstleister;[37]
  - Notfallpläne und Ausstiegsstrategien für ausgelagerte kritische oder wichtige Funktionen oder Tätigkeiten,[38] insbesondere ist hierbei zu berücksichtigen, wie die Funktion ggf. auf einen anderen Dienstleister übertragen oder ins eigene Unternehmen zurückgeholt werden kann;[39]
  - Beschreibung der Bedingungen für ein Sub-Outsourcing, u. a. Genehmigungspflicht des Unternehmens bei Sub-Outsourcing von wichtigen/kritischen Funktionen;[40]
  - ggf. Besonderheiten von Outsourcing ins EU-Ausland bzw. gruppeninternes Outsourcing.

33 EIOPA-Leitlinien zum Governance-System (Vorbereitungsphase), Leitlinie 47.
34 EIOPA-Leitlinien zum Governance-System (Vorbereitungsphase), Leitlinie 14; gilt wohl auch für die Auslagerung anderer kritischer/wichtiger Funktionen, vgl. Art. 274 Abs. 5 c) DDA.
35 Wie und wie oft: Ziff. 1.187, 1.189 Erläuterungen der EIOPA-Leitlinien zum Governance-System (Vorbereitungsphase).
36 Ziff. 1.188 f. der Erläuterungen der EIOPA-Leitlinien zum Governance-System (Vorbereitungsphase).
37 EIOPA-Leitlinien zum Governance-System (Vorbereitungsphase), Leitlinie 47.
38 Ziff. 1.186 der Erläuterungen der EIOPA-Leitlinien zum Governance-System (Vorbereitungsphase).
39 Ziff. 1.186 der Erläuterungen der EIOPA-Leitlinien zum Governance-System (Vorbereitungsphase).
40 Ziff. 1.184 der Erläuterungen der EIOPA-Leitlinien zum Governance-System (Vorbereitungsphase).

3. Ausgliederung der Compliance-Funktion

Wird ein Dienstleister mit der Erfüllung von Compliance-Aufgaben betraut, stellt dies eine aufsichtsrelevante Ausgliederung dar. Denn die Compliance-Funktion ist als Schlüsselfunktion eine „kritische oder wichtige Funktion" im Sinne der Richtlinie. Folglich sind bei dem Outsourcing von Compliance-Aufgaben die erhöhten Anforderungen der Solvency II-Gesetzgebung nach Art. 274 DDA zu erfüllen, welche sich auch in § 32 Abs. 3 VAG-E finden. Bereits im Rahmen der schriftlichen Leitlinien zum Outsourcing ist daher auszuführen, welche unternehmensinternen Kontrollprozesse vorgesehen sind, um die ordnungsgemäße Leistungserbringung durch den Dienstleister sicherzustellen. Dies betrifft sowohl die Auswahl des Dienstleisters und dessen laufende Überwachung wie auch die Gestaltung der vertraglichen Grundlagen.[41] So ist auch sicherzustellen, dass das Risikomanagement und das interne Kontrollsystem des Dienstleisters in der Lage sind, eine ordnungsgemäße Leistungserbringung zu gewährleisten.[42] Weiter muss eine angemessene Einbindung in das eigene Risikomanagementsystem und das interne Kontrollsystem im Unternehmen erfolgen.

Die große Bandbreite an Themen und Rechtsgebieten, welche für die Compliance-Funktion relevant sind, führt dazu, dass im Fall einer Ausgliederung insbesondere die Anforderungen an die fachliche Eignung der Personen bei dem Dienstleister sowie der überwachenden Person im VU im Mittelpunkt stehen. Hierbei muss gewährleistet sein, dass die verantwortliche Person bei dem Dienstleister in gleicher Weise geeignet und qualifiziert ist wie eine Person, welche die Schlüsselfunktion bei dem Versicherungsunternehmen innehaben würde.

4. Gruppeninternes Outsourcing

Die Governance-Anforderungen und damit auch die Outsourcing-Regelungen gelten gemäß Art. 246 Abs. 1 Solvency II-Richtlinie grundsätzlich auch auf Gruppenebene.[43]

Das Unternehmen muss im Falle eines gruppeninternen Outsourcings von kritischen oder wichtigen Funktionen bzw. Tätigkeiten den Umfang berücksichtigen, in dem das Unternehmen den Dienstleister kontrolliert oder in der Lage ist, sein Handeln zu beeinflussen.[44] Bei der Auslagerung auf ein gruppenangehöriges Unternehmen sind gem. Art. 274 Abs. 2 DDA grundsätzlich dieselben Anforderungen zu erfüllen wie bei dem Outsourcing auf einen externen Dienstleister. Dies betont auch die BaFin in Rz. 35 der Verlautbarung zur Qualifikation vom 30. April 2014. Nach den EIOPA-Leitlinien zum Governance-System soll das zuständige Unternehmen – sofern Schlüsselfunktionen innerhalb der Gruppe ausgelagert werden – dokumentieren, wel-

41 Vgl. hierzu zusammenfassend: Ziff. 1.188 der Erläuterungen der EIOPA-Leitlinien zum Governance-System (Vorbereitungsphase)
42 Art. 274 Abs. 5 DDA.
43 Vgl. Zum Gruppenbegriff Art. 212 Abs. 1 lit c) Solvency II-Richtlinie sowie zum Begriff der Beteiligung Art. 13 Nr. 20 Solvency II-Richtlinie.
44 Art. 274 Abs. 2 DDA.

che Funktionen welche juristische Person betreffen und dafür Sorge tragen, dass die Durchführung der Aufgaben der Schlüsselfunktionen auf der Ebene des Unternehmens nicht durch derartige Outsourcing-Vereinbarungen beeinträchtigt wird.[45] Danach müssen die Zuständigkeiten/Verantwortlichkeiten innerhalb des VU klar geregelt werden.

5. Anzeigepflichten gegenüber der BaFin

Art. 49 Abs. 3 Solvency II-Richtlinie sieht vor, dass die Unternehmen der BaFin das Outsourcing kritischer oder wichtiger Funktionen oder Tätigkeiten anzeigen. Danach haben die Unternehmen die Aufsicht über das Outsourcing und wesentliche Änderungen zu informieren. Auch sieht Leitlinie 14 der EIOPA-Leitlinien zum Governance-System vor, dass eine Person in dem Versicherungsunternehmen benannt werden muss, welche die Gesamtverantwortung für die ausgegliederte Schlüsselfunktion trägt. Die BaFin leitet daraus in Rz. 33 der Verlautbarung zur Qualifikation ab, dass die ausgliedernden Versicherungsunternehmen einen Ausgliederungsbeauftragten zu benennen und auch gegenüber der BaFin anzuzeigen haben.

V. Fit & Proper-Anforderungen an die Compliance-Funktion

Zu den Anforderungen an die fachliche Qualifikation und die persönliche Zuverlässigkeit unter Solvency II hat der Verband ein umfangreiches Diskussionspapier veröffentlicht.[46] Im Folgenden sind die für die Compliance-Funktion wesentlichen Aspekte zusammengefasst.

1. Betroffener Personenkreis

Das nationale Aufsichtsrecht verlangt bislang in § 7a VAG nur von den Mitgliedern des Vorstandes sowie des Aufsichtsrates, dass diese ihre fachliche Qualifikation und ihre persönliche Zuverlässigkeit nachweisen. Art. 42 der Solvency II-Richtlinie erweitert zukünftig den betroffenen Personenkreis: Erfasst sind nunmehr „alle Personen, die das Unternehmen tatsächlich leiten oder andere Schlüsselaufgaben innehaben“. Eine entsprechende Regelung ist auf nationaler Ebene in § 24 VAG-E vorgesehen.

Die Compliance-Funktion ist als Schlüsselaufgabe nach Solvency II von den Qualifikations- und Zuverlässigkeitsanforderungen erfasst. EIOPA[47] und die BaFin[48] interpretieren Art. 42 Solvency II aber sehr weitgehend und wollen die enthaltenen Anforderungen auf alle Personen erstrecken, die für die Compliance-Funktion fachlich

45 EIOPA-Leitlinien zum Governance-System (Vorbereitungsphase), Leitlinie 46 Ziff. 1.85.
46 GDV-Diskussionspapier: „Fachliche Qualifikation und persönliche Zuverlässigkeit unter Solvency II“.
47 Abschlussbericht zur Konsultation der Leitlinien zum Governance-System (EIOPA/13/413), Rz. 3.54.
48 BaFin-Verlautbarung zur Qualifikation, Rz. 1 und Rz. 10.

tätig sind. Betroffen wären danach alle Mitarbeiter, die den Inhaber der Schlüsselfunktion fachlich unterstützen.

Nach Ansicht des Verbandes lässt sich diese Auffassung nicht mit den Vorgaben der Richtlinie vereinbaren.[49] Nur für den Leiter bzw. Inhaber der Schlüsselfunktion ist eine Beurteilung anhand der besonderen Kriterien des Art. 42 Solvency II-Richtlinie gefordert. Erfasst sein dürften darüber hinaus auch Stellvertreter, sofern diese vom Unternehmen dauerhaft benannt und mit entsprechenden Rechten und Pflichten ausgestattet sind.[50] Im Übrigen gelten (nur) die allgemeinen Anforderungen im Sinne von Erwägungsgrund 34.

2. Qualifikationsanforderungen gem. Art. 42 Solvency II-Richtlinie („Fit“)

Die erforderlichen Qualifikationen für Personen, die Schlüsselfunktionen innehaben, sind hinsichtlich der drei Kriterien Berufsqualifikation, Kenntnisse und Erfahrungen bisher nur schwach konturiert. Der Entwurf der Delegierten Rechtsakte bestimmt insoweit, dass die Pflichten der jeweiligen Person zu berücksichtigen sind, wenn die Qualifikationsanforderungen festgelegt werden.[51] Die BaFin scheint diese Frage gleich zu beurteilen.[52] Zu den konkreten Anforderungen an den Inhaber der Compliance-Funktion wird auf das Diskussionspapier des GDV verwiesen.[53]

3. Zuverlässigkeitsanforderungen gem. Art. 42 Solvency II-Richtlinie („Proper“)

Nach Art. 273 DDA und den EIOPA-Leitlinien zum Governance-System[54] soll die persönliche Zuverlässigkeit eines Mitarbeiters anhand seiner persönlichen Redlichkeit und finanziellen Zuverlässigkeit bewertet werden. Dabei sind strafrechtliche, finanzielle und aufsichtsrechtliche Aspekte zu berücksichtigen.

Die Beurteilung der persönlichen Zuverlässigkeit ist in der Praxis problematisch. EIOPA und die BaFin haben darauf hingewiesen, dass der Proportionalitätsgrundsatz hier keine Anwendung findet.[55] Immerhin hat die BaFin zu erkennen gegeben, dass sie es für angemessen hält, wenn ein behördlicher Nachweis (z. B. Führungszeugnis) eingeholt wird.

Näheres hierzu findet sich im GDV-Diskussionspapier: „Fachliche Qualifikation und persönliche Zuverlässigkeit unter Solvency II“.

---

49 Detailliert hierzu: GDV-Diskussionspapier: „Fachliche Qualifikation und persönliche Zuverlässigkeit unter Solvency II“, Ziff. 3.
50 Vgl. auch BaFin-Verlautbarung zur Qualifikation, Rz. 11.
51 Art. 273 Abs. 2 DDA.
52 BaFin-Verlautbarung zur Qualifikation, Rz. 23.
53 GDV-Diskussionspapier: „Fachliche Qualifikation und persönliche Zuverlässigkeit unter Solvency II“.
54 EIOPA-Leitlinien zum Governance-System (Vorbereitungsphase), Leitlinie 12 Rz. 1.33.
55 EIOPA-Leitlinien zum Governance-System (Vorbereitungsphase), Leitlinie 12 Rz. 1.39; BaFin-Verlautbarung zur Qualifikation, Rz. 26.

4. Anzeigepflicht

Die Solvency II-Richtlinie sieht vor, dass die Versicherungsunternehmen der Aufsichtsbehörde melden, wenn es relevante Änderungen bei von den Qualifikations- und Zuverlässigkeitsvorgaben betroffenen Mitarbeitern gibt (Art. 42 Abs. 2 und Abs. 3).

Die BaFin geht zwar davon aus, dass alle in Schlüsselfunktionen tätigen Mitarbeiter vom Anwendungsbereich des Art. 42 Solvency II-Richtlinie umfasst sind (s. o). Entsprechende Anzeigepflichten leitet sie aber nur für die „verantwortlichen Inhaber" ab.[56] Die konkrete Aufsichtspraxis im Hinblick auf Umfang und Zeitpunkt der Anzeige bleibt abzuwarten.

Aus Verbandssicht ist darauf hinzuweisen, dass die Anzeigepflichten nicht Bestandteil der Vorbereitungsphase sind. Diese gelten daher erst ab Inkrafttreten von Solvency II am 1. Januar 2016.[57]

5. Fit & Proper-Anforderungen beim Outsourcing der Compliance-Funktion

Die Versicherungsunternehmen bleiben unter dem Regime von Solvency II auch bei ausgegliederten Funktionen voll für die Erfüllung der Verpflichtungen aus der Richtlinie verantwortlich. Dies stellt nunmehr auch § 32 Abs. 1 VAG-E ausdrücklich klar. Nach Art. 49 Solvency II und Art. 274 Abs. 5 lit. c) DDA muss das auslagernde Unternehmen insbesondere gewährleisten, dass alle Beschäftigten des Dienstleisters, die an der Durchführung der ausgelagerten Tätigkeit beteiligt sein werden, ausreichend qualifiziert und zuverlässig sind.

Nach Ansicht von EIOPA und BaFin sollen die Kriterien gem. Art. 42 Solvency II umfassend für alle mit der Durchführung der ausgelagerten Schlüsselfunktion Beschäftigten gelten.[58] Das auslagernde Unternehmen muss insoweit die Einhaltung der Fit & Proper-Anforderungen beim Dienstleister sicherstellen. Eine rein vertragliche Verpflichtung des Dienstleisters soll dabei nicht ausreichen. Die BaFin fordert, dass der Dienstleister dem Versicherungsunternehmen seinen Prüfprozess darlegt und eine schriftliche Bestätigung mit dem Ergebnis der Prozessprüfung aushändigt.[59]

Wie bei der unternehmensinternen Wahrnehmung der Schlüsselfunktionen interpretieren die Aufsichtsbehörden den Anwendungsbereich zu weitgehend: Auch bei der Auslagerung muss nur der Inhaber der Schlüsselfunktion beim Dienstleister qualifi-

56 BaFin-Verlautbarung zur Qualifikation, Rz. 1 und Rz. 10.
57 Siehe im Detail hierzu: GDV-Diskussionspapier: „Fachliche Qualifikation und persönliche Zuverlässigkeit unter Solvency II", S. 24.
58 Abschlussbericht zur Konsultation der Leitlinien zum Governance-System (EIOPA/13/413), Rz. 3.53; BaFin-Verlautbarung zur Qualifikation, Rz. 32.
59 BaFin-Verlautbarung zur Qualifikation, Rz. 32.

ziert und zuverlässig im Sinne des Art. 42 Solvency II sein. Im Übrigen gelten die allgemeinen Anforderungen im Sinne von Erwägungsgrund 34 der Richtlinie (s. o.).

VI. Berichtswege

Zu unterscheiden ist hier, an wen die Compliance-Organisation berichtet und welche Stellen im Unternehmen an die Compliance-Organisation berichten sollten.

1. Berichterstattung durch die Compliance-Funktion an Vorstand und Aufsichtsrat

- **Vorstand**[60]

  Die Compliance-Funktion muss regelmäßig und – wenn ein Anlass gegeben ist – auch ad hoc an den Vorstand berichten.[61] Den Vorstand trifft seinerseits die Pflicht, sich über die Arbeit und die Entwicklung der Compliance-Funktion zu informieren. Diese ergibt sich aus seiner gesellschafts- und aufsichtsrechtlichen Compliance-Verantwortung.[62] Die Anforderungen werden in den Verlautbarungen der Aufsichtsbehörden konkretisiert.[63]

  Es ist in jedem Fall sicherzustellen, dass der Vorstand die notwendigen Mindestinformationen hat, um seine Pflichten wahrzunehmen.[64] In welcher Periodik die Berichterstattung erfolgt und in welcher Form (schriftliche Berichte oder persönlicher Vortrag des Inhabers der Schlüsselfunktion) obliegt grundsätzlich der Entscheidung des VU. Erforderlich ist, dass die Berichterstattung in angemessenen Zeitabständen – zumindest einmal jährlich – stattfindet und dokumentiert wird.[65]

  Inhalte dieser regelmäßigen Compliance-Berichterstattung können beispielsweise sein:

  - Beschreibung der Compliance-Organisation bzw. deren essenziellen (Weiter-)Entwicklungen sowie Angaben zur Angemessenheit der Personal- und Sachausstattung;
  - Zusammenfassung der identifizierten Compliance-Risiken und der durchgeführten bzw. durchzuführenden Maßnahmen zur Risikoreduzierung;[66]
  - Festgestellte Compliance-Verstöße (hierzu empfiehlt sich die Definition von Kriterien, welche Verstöße an die Geschäftsleitung berichtet werden, z. B. Schadenssummen über einem gewissen Schwellenwert oder wesentliche strafrechtliche Verstöße) und die ergriffenen Gegenmaßnahmen.[67]

60 Vorstand steht hier stellvertretend für die Geschäftsleitung.
61 BaFin-Verlautbarung zu „Interne Kontrollen und interne Revision“, Rz. 37.
62 Vgl. hierzu oben B.
63 Vgl. die BaFin-Verlautbarung zu „Allgemeine Governance-Anforderungen“, insb. Rz. 41, 80 und 135.
64 Vgl. oben B.I.2.
65 So auch BaFin-Verlautbarung zu „Interne Kontrollen und interne Revision“, Rz. 37.
66 So auch BaFin-Verlautbarung zu „Interne Kontrollen und interne Revision“, Rz. 38.
67 Vgl. dazu BaFin-Verlautbarung zu „Interne Kontrollen und interne Revision“, Rz. 38.

Der Vorstand sollte zudem über Entwicklungen und allgemeine Trends des Rechtsumfeldes informiert werden,[68] damit dieser entsprechende Vorkehrungen und Maßnahmen einleiten kann.[69]

Darüber hinaus hat der Compliance-Verantwortliche dem Vorstand erhebliche Feststellungen unverzüglich mittels eines anlassbezogenen **Ad-hoc-Berichts** mitzuteilen. Anders als bei der regelmäßigen Berichterstattung muss dabei nicht umfassend über alle Feststellungen berichtet werden. Vielmehr empfiehlt es sich, unternehmensindividuell eine Schwelle für erhebliche Feststellungen, z. B. schwerwiegende Verstöße, festzulegen. Der Bericht hat – soweit bereits möglich – einen Vorschlag hinsichtlich zu ergreifender Abhilfemaßnahmen zu enthalten.

In Konzernstrukturen prüft die Compliance-Organisation anlässlich jeder Berichterstattung, ob eine Berichterstattung auch an die übergeordnete Compliance-Organisation innerhalb des Unternehmensverbunds erforderlich ist.

- **Aufsichtsrat**

  Es ist festzulegen, in welchen zeitlichen Abständen und mit welchem Inhalt die regelmäßige Berichterstattung der Compliance-Funktion an den Aufsichtsrat erfolgt. Die Übermittlung des Berichts an den Aufsichtsrat erfolgt grundsätzlich über den Vorstand.

  Sofern der Aufsichtsrat einen Prüfungsausschuss eingerichtet hat,[70] wird in dessen Sitzungen regelmäßig auch über Compliance-relevante Sachverhalte berichtet.

2. Berichtswege an die Compliance-Funktion

Die effektive Aufgabenerfüllung durch die Compliance-Funktion setzt voraus, dass diese aus dem Unternehmen heraus angemessen informiert wird. In Betracht kommen eine regelmäßige sowie eine anlassbezogene Berichterstattung.

- **Compliance-Beauftragte und besondere Beauftragte**

  Sind Compliance-Beauftragte in einzelnen Unternehmensteilen installiert, sollten diese auf regelmäßiger Basis über ihre Aktivitäten und Feststellungen an den Schlüsselfunktionsinhaber berichten. Der Turnus ist unternehmensindividuell festzulegen. Darüber hinaus sollte auch eine anlassbezogene Berichterstattung erfolgen. Zweckmäßig ist es, Kriterien festzulegen, die eine Berichtspflicht auslösen. So kann ein Kriterienkatalog (bei Verstößen bspw. Höhe finanzieller Schaden, Strafzahlungen, Strafmaß; Anzahl durchgeführter Überwachungsmaßnahmen oder Compliance-Schulungen, etc.) mit definierten Auslösern sowie ein vorgegebenes Format die systematische Steuerung und Bearbeitung der Berichte unter-

68 Vgl. oben C. II. 1. a.
69 Vgl. dazu BaFin-Verlautbarung „Interne Kontrollen und interne Revision“, Rz. 33.
70 Vgl. hierzu die Vorgaben in Ziffer 5.3.2 des Deutschen Corporate Governance Kodex.

stützen. Auch bei besonderen Beauftragten, wie etwa dem Geldwäsche- oder dem Datenschutzbeauftragten, bietet es sich an, entsprechend vorzugehen.

Folgende Sachverhalte sollten von der Berichterstattung der Compliance-Beauftragten an den Schlüsselfunktionsinhaber umfasst sein:

- Einschätzung der Wirksamkeit implementierter Präventionsmaßnahmen;
- behördliche Verfahren (zu Compliance-relevanten Themen, insbesondere Anfragen, Prüfungen und Untersuchungen von Aufsichts- und Strafverfolgungsbehörden);
- schwerwiegende Verstößen gegen Gesetze und andere Rechtsvorschriften sowie gegen interne Vorschriften (wie z. B. Verhaltenskodizes, Compliance-Richtlinien) einschließlich Verdachtsfälle sowie
- sonstige wesentlichen Ereignisse oder Vorfälle, die die Reputation des Unternehmens oder der berichtenden Einheit negativ beeinträchtigen können.
- Die Unternehmen können individuell weitere Themen für die Berichterstattung vorsehen.

- **Führungskräfte**

  Führungskräfte relevanter Zentral- und Geschäftsbereiche sollten über bekanntgewordene Verstöße ad hoc an eine definierte Stelle der Compliance-Funktion berichten. Auch hier können Kriterien/Schwellen festgelegt werden.

- **Andere Schlüsselfunktionen**

  Weiterhin sollte zwischen den verschiedenen Schlüsselfunktionen ein Prozess festgelegt werden, der einen angemessenen Informationsaustausch sicherstellt. Bspw. sollte die Compliance-Funktion alle Berichte der Internen Revision erhalten, die für ihre Aufgabenerfüllung notwendig sind, die Risikokontrollfunktion sollte alle Informationen an die Compliance-Funktion weiterleiten, die Compliance-Risiken betreffen.

- **Meldung von Compliance-Verstößen durch Mitarbeiter**

  Zusätzlich sollten den Mitarbeitern Möglichkeiten eingeräumt werden, Verstöße freiwillig und ggfs. anonym zu melden. Es muss sichergestellt sein, dass derartige Meldungen auch die vorgesehene Stelle in der Compliance-Funktion erreichen.

  Unternehmensindividuell muss entschieden werden, ob in diesem Zusammenhang auch allen Mitarbeitern die Pflicht zur Meldung bestimmter, schwerer Verstöße auferlegt wird.[71]

71 Hierbei sind Regeln des Arbeitnehmerdatenschutzes zu beachten. In der Regel ist der Betriebsrat zu beteiligen.

- **Rechtsumfeldrisiken**

  Um relevante Änderungen und Entwicklungen regulatorischer Anforderungen sowie die zur Sicherstellung ihrer Einhaltung ergriffenen bzw. zu ergreifenden Maßnahmen im Berichtszeitraum überwachen und an die Organe berichten zu können, ist ein internes Meldesystem in relevanten Geschäfts- und Zentralbereichen empfehlenswert. Dies erfolgt durch Beteiligung des Compliance-Verantwortlichen an dem Prozess, der zur Früherkennung rechtlicher Risiken im Unternehmen eingerichtet ist.

F. Anhang

Rechtsquellen

Abschlussbericht zur Konsultation der Leitlinien zum Governance-System (EIOPA/13/413)	EIOPA Final Report on Public Consultation No. 13/008 on the Proposal for Guidelines on the System of Governance, EIOPA/13/413, vom 27. September 2013
BaFin-Verlautbarung zu „Allgemeinen Governance-Anforderungen“	BaFin-Verlautbarung zu Themenkomplex 1 „Allgemeine Governance-Anforderungen“ vom 30. Mai 2014
BaFin-Verlautbarung zur Qualifikation	Verlautbarung der BaFin zu Themenkomplex 2 „Prüfung der fachlichen Eignung und Zuverlässigkeit“, vom 30. April 2014
BaFin-Verlautbarung zu „Interne Kontrollen und interne Revision“	Konsultierte Fassung der BaFin-Verlautbarung zu Themenblock 6 „Interne Kontrollen und interne Revision“ vom 9. Juli 2014
Consultation Paper on the Proposal for Guidelines on the System of Governance	Consultation Paper on the Proposal for Guidelines on the System of Governance, EIOPA-CP-13/08, vom 27. März 2013
Delegierte Rechtsakte (DDA)	Draft Delegated Acts der Europäischen Kommission, Stand: Oktober 2014
EIOPA-Leitlinien zum Governance-System (Vorbereitungsphase)	Leitlinien zum Governance-System, EIOPA-CP- 13/08 DE, EIOPA 2013 http://www.bafin.de/SharedDocs/Downloads/DE/Leitfaden/VA/dl_lf_solvency_governance_deutsch_061113.pdf
Erläuterungen der EIOPA-Leitlinien zum Governance-System (Vorbereitungsphase)	Erläuterungen zu Leitlinien zum Governance-System http://www.bafin.de/SharedDocs/Downloads/DE/Leitfaden/VA/dl_lf_solvency_erlaeuterung_governance.pdf;
Novelle des Versicherungsaufsichtsgesetzes (VAG-E)	Regierungsentwurf eines Gesetzes zur Modernisierung der Finanzaufsicht über Versicherungen vom 3. September 2014
Omnibus II-Richtlinie	Richtlinie 2014/51/EU des Europäischen Parlaments und des Rates vom 16. April 2014 zur Änderung der Richtlinien 2003/71/EG und 2009/138/EG und der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 im Hinblick auf die Befugnisse der Europäischen Aufsichtsbehörde (Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung) und der Europäischen Aufsichtsbehörde (Europäische Wertpapier- und Marktaufsichtsbehörde)
Quick fix 2-Richtlinie	Richtlinie 2013/58/EU des Europäischen Parlaments und des Rates vom 11. Dezember 2013 zur Änderung der Richtlinie 2009/138/EG (Solvabilität II) hinsichtlich des Zeitpunkts ihrer Umsetzung und des Zeitpunktes ihrer Anwendung sowie des Zeitpunkts der Aufhebung bestimmter Richtlinien (Solvabilität I), veröffentlicht im Amtsblatt Nr. L 341/1 am 18. Dezember 2013
Solvency II-Richtlinie	Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates vom 25. November 2009 betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit (Solvabilität II), veröffentlicht im Amtsblatt Nr. L 335/1 am 17. Dezember 2009

Gesamtverband der Deutschen Versicherungswirtschaft e. V.

Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin

Tel. 030 / 20 20-50 00, Fax 030 / 20 20-60 00
www.gdv.de, berlin@gdv.de