Gesamtverband der Deutschen Versicherungswirtschaft e. V.

Aktualisierter Leitfaden für die Praxis

Compliance in Versicherungsunternehmen

Stand: Januar 2021

GDV
DIE DEUTSCHEN VERSICHERER

Gesamtverband der Deutschen Versicherungswirtschaft e. V.

Aktualisierter Leitfaden für die Praxis

Compliance in Versicherungsunternehmen

Stand: Januar 2021

GDV
DIE DEUTSCHEN VERSICHERER

Impressum

Herausgeber
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

Karen Bartel
Leiterin Recht / Compliance / Verbraucherschutz
Tel. 030 / 20 20 – 52 60
E-Mail: k.bartel@gdv.de

Autor
Peter Glöckle
Recht / Compliance / Verbraucherschutz
Tel. 030 / 20 20 – 54 15
E-Mail: p.gloeckle@gdv.de

Publikationsassistenz
Kerstin Handrack
Tel. 030 / 20 20 – 51 72
E-Mail: k.handrack@gdv.de

Redaktionsschluss dieser Ausgabe
Februar 2021

Hinweis:
Sämtliche Personenbezeichnungen in diesem Leitfaden gelten gleichermaßen für männliche, weibliche und anderweitige Geschlechter.

Inhaltsverzeichnis

A. Einführung

Die erste Auflage dieses Leitfadens wurde zu einem Zeitpunkt erarbeitet, als die grundlegende Novellierung des Versicherungsaufsichtsrechts durch Solva II noch in der Entwicklung begriffen war. Mittlerweile ist die Umsetzung der Compliance-Vorgaben in den Versicherungsunternehmen[1] etablierte Praxis.

Aufgrund der Komplexität der Regulierung gibt es aber weiterhin Unsicherheiten bei der Auslegung und Anwendung der relevanten Vorschriften. Die Überarbeitung des Leitfadens soll dieser Tatsache Rechnung tragen. Sie aktualisiert insbesondere die rechtlichen Vorgaben und bindet zudem die „GDV-Hilfestellung zur Compliance-Organisation unter Solvency II“ ein. Dabei gelten die in der Erstauflage benannten Grundsätze fort. Die Aktualisierung veranlasst daher für sich keine Änderung der etablierten Compliance-Abläufe in den Versicherungsunternehmen.

Die in dem Papier dargestellten Ergebnisse geben keinen Mindeststandard in der Versicherungsbranche wieder. Sie sind als Hilfestellung für die Unternehmen gedacht, individuelle Lösungen zu entwickeln und sollen die Verantwortlichen dabei unterstützen, effektive Compliance-Strukturen in den Unternehmen vorzuhalten.[2]

1 Als Versicherungsunternehmen werden hier sowohl Erst- als auch Rückversicherungsunternehmen erfasst. Für Einrichtungen der betrieblichen Altersversorgung (EbAV) gelten eigenständige Anforderungen (z. B. derzeit keine verpflichtende Einrichtung einer Compliance-Funktion).

2 Sämtliche Personenbezeichnungen im Leitfaden gelten gleichermaßen für Personen jeden Geschlechts.

B. Grundlagen der Compliance in Versicherungsunternehmen

Grundlage der Tätigkeit in Versicherungsunternehmen ist ein Handeln im Einklang mit der unternehmenseigenen Compliance-Kultur. Compliance-Kultur bedeutet, die vom jeweiligen Unternehmen vorgegebenen Werte (beispielsweise Integrität, Transparenz und Ehrlichkeit) in die täglichen Abläufe und Geschäftsentscheidungen miteinzubinden und sicherzustellen, dass jedes einzelne Mitglied der Geschäftsleitung und des Aufsichtsrats, jede Führungskraft und jeder Mitarbeiter sich den Zielen von Compliance verpflichtet fühlt, indem er in Übereinstimmung mit den anwendbaren Gesetzen und Regelungen handelt, um das Unternehmen und dessen Ruf zu schützen.

Compliance-Kultur ist als die Übereinstimmung aller unternehmerischen Aktivitäten mit den Gesetzen, Anforderungen und Vorschriften, die für die Geschäftstätigkeit relevant sind und dem Schutz vor Compliance-Risiken dienen, zu verstehen.

Das Versicherungsaufsichtsrecht enthält besondere Anforderungen im Hinblick darauf, wie die spezifische Compliance-Funktion in einem Versicherungsunternehmen ausgestaltet und implementiert sein muss. Grundlegend sind zudem die Governance- und Compliance-Anforderungen des Gesellschaftsrechts. Diese sind im Aktiengesetz geregelt und finden auf Versicherungsvereine auf Gegenseitigkeit entsprechende Anwendung (vgl. §§ 188, 189 VAG).

I. Gesellschaftsrechtliche Compliance-Verantwortung der Geschäftsleitung

Dem **Vorstand** erwächst aus seinen aktienrechtlichen Pflichten eine Compliance-Verantwortung. Grundlage ist die aus §§ 76 Abs. 1, 93 Abs. 1 AktG abgeleitete[3] Legalitätspflicht des Vorstands.[4] 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 (Legalitätskontrollpflicht).

Gem. § 91 Abs. 2 AktG muss der Vorstand ein Überwachungssystem einrichten, um bestandsgefährdende Entwicklungen für das Unternehmen frühzeitig zu erkennen. Der Vorstand genügt dieser Organisationspflicht bei entsprechender Gefährdungslage u. a. dann, wenn er eine Compliance-Organisation einrichtet, die auf Schadenprävention und Risikokontrolle angelegt ist. Darüber hinaus hat der Vorstand ein weites Ermessen, wie er der Compliance-Verantwortung im Übrigen gerecht wird.

Die Compliance-Verantwortung ist als Leitungsaufgabe (§ 76 Abs. 1 AktG) dem **Gesamtvorstand** zugewiesen. Dieser muss alle grundlegenden Entscheidungen über die

---

3 Darüber hinaus lässt sich die Pflicht, Compliance-Maßnahmen zu ergreifen, gesellschaftsunabhängig auf § 130 OWiG stützen. Während die Compliance-Verantwortung des Vorstands als solche anerkannt ist, ist die konkrete Herleitung in der Literatur umstritten und wird teils auch auf eine Gesamtanalogie einzelner Compliance-Vorgaben gestützt.

4 Das Landgericht München I hat hierzu in seinem Siemens/Neubürger-Urteil vom 10.12.2013 – 5HK O 1387/10, NZG 2014, 345 – wesentliche Aussagen getroffen.

Compliance-Organisation selbst treffen und sich regelmäßig bzw. anlassbezogen von deren Wirksamkeit überzeugen. Die Compliance-Verantwortung als solche kann daher nicht delegiert werden.[5]

Möglich ist es indes, konkrete Einzelpflichten im Wege der Arbeitsteilung entweder horizontal auf einzelne Vorstandsmitglieder oder vertikal auf nachgeordnete Ebenen zu übertragen. Die Letztverantwortlichkeit des (Gesamt-)Vorstands bleibt hiervon unberührt.

Der **Aufsichtsrat** muss überwachen, ob der Vorstand seine Compliance-Aufgabe ordnungsgemäß wahrnimmt (§ 111 Abs. 1 AktG). Er kann die Compliance-Organisation gegenüber dem Vorstand beanstanden. Der Aufsichtsrat kann keine direkten Anweisungen an den Vorstand oder den Inhaber der Compliance-Funktion geben, jedoch bei Pflichtverstößen von seiner Personalkompetenz Gebrauch machen und ggf. Schadenersatzansprüche der Gesellschaft gegenüber einem Vorstandsmitglied geltend machen.

II. Aufsichtsrechtliche Anforderungen der Compliance-Funktion

1. Die Compliance-Funktion im Governance-System von Solva II

Aufsichtsrechtlich wird durch die Solva II-RL für Versicherungsunternehmen eine spezifische Governance-Organisation vorgegeben, die eine wirksame Compliance-Funktion voraussetzt. Die allgemeinen gesellschaftsrechtlichen Anforderungen werden durch diese besonderen Organisationspflichten des Versicherungsaufsichtsrechts überlagert.

Die **Solva II-RL** sieht vor, dass die Versicherungsunternehmen über ein **wirksames Governance-System** verfügen müssen, um ein solides und vorsichtiges Management des Geschäfts zu gewährleisten.[6] § 23 Abs. 1 Satz 2 VAG setzt diese Voraussetzung einer ordnungsgemäßen Geschäftsorganisation national um. Die Geschäftsorganisation muss danach die Einhaltung der relevanten Vorgaben, also die Compliance gewährleisten. Vorgaben speziell für die Compliance-Funktion enthält Art. 274 Solva II-VO[7] lediglich zur Compliance-Leitlinie und zum Compliance-Plan.[8] Daneben enthält Art. 268 Solva II-VO Vorgaben für alle Governance-Funktionen, die somit auch für die Compliance-Funktion gelten. Dies umfasst:

- Integration der Funktion und der entsprechenden Berichtslinien in die Organisationsstrutkur,
- objektive, faire und unabhängige Aufgabenwahrnehmung,
- Letztverantwortlichkeit des Vorstands (VMA),

---

5 Die Letztverantwortlichkeit des „Verwaltungs-, Management- oder Aufsichtsorgans" (VMA) wird zudem durch Art. 40 der Solva II-RL vorgegeben.
6 Art. 41 Abs. 1 Solva II-RL.
7 Die Vorgaben der Solva II-RL zum Governance-System werden durch delegierte Rechtsakte, namentlich der Solva II-VO, näher bestimmt (Art. 50 Abs. 1), die gegenüber den Versicherungsunternehmen und den Aufsichtsbehörden unmittelbare Geltung entfalten (Art. 288 UAbs. 2 AEUV). Die Solva II-VO ist neben den nationalen Umsetzungsrechtsakten zu beachten und geht dieser vor.
8 Siehe dazu unter C. III. und C. IV.

- Berichtspflichten,
- Zusammenarbeit mit anderen Funktionen,
- Informationszugang.

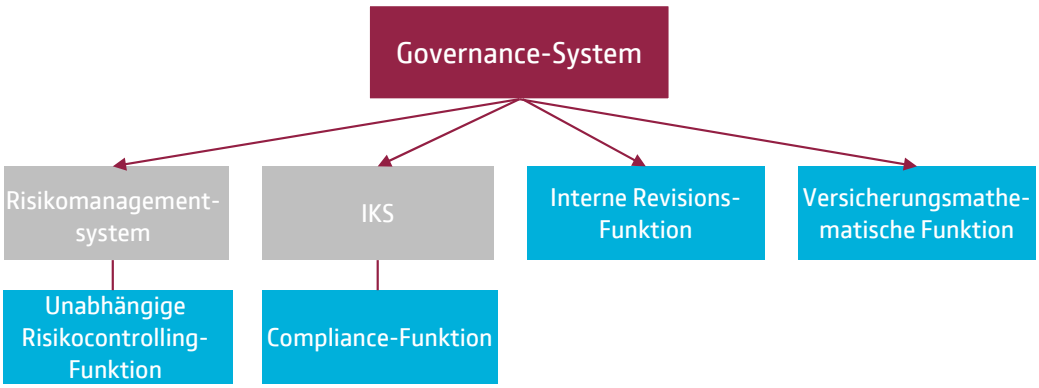
Übergreifende Vorgaben für die Qualifikation enthält Art. 273 Solva II-VO[9] und für die Vergütung Art. 275 Solva II-VO mit detaillierten Grundsätzen für die Vergütungspolitik und -praxis.

Zentrale Bestandteile des Governance-Systems sind ein **wirksames internes Kontrollsystem (IKS)**, ein Risikomanagementsystem mit einer unabhängigen Risikocontrollingfunktion (§ 26 Abs. 1 und 8 VAG),[10] eine Interne Revisions-Funktion (§ 30 VAG) und eine versicherungsmathematische Funktion (§ 31 VAG).

Das IKS muss gem. Art. 46 Abs. 1 Solva II-RL bzw. § 29 Abs. 1 Satz 2 VAG obligatorisch „eine Funktion zur Überwachung der Einhaltung der Anforderungen („**Compliance-Funktion**“) umfassen.“[11] Das IKS soll „die Einhaltung der geltenden Rechts- und Verwaltungsvorschriften“ gewährleisten (Art. 266 Solva II-VO) und verfolgt daher ebenfalls die Compliance als wesentliches Ziel.

Die Einführung und Ausgestaltung des Governance-Systems und des internen Kontrollsystems und damit der Compliance-Funktion ist als Teil der Geschäftsorganisation Aufgabe der Geschäftsleitung, die auch die Letztverantwortung trägt.[12]

Schaubild Governance-System[13]



Demnach sind als Schlüsselfunktionen zwingend (nur) die unabhängige Risikocontrolling-Funktion, Compliance-Funktion, interne Revisionsfunktion und versicherungsmathematische Funktion mit jeweils näher bestimmten organisatorischen Anforderungen und inhaltlichen Aufgaben vorausgesetzt.

---

9 Siehe dazu auch unter D. V.
10 So das VAG; dagegen Solva II-RL „Risikomanagementfunktion“.
11 Gem. § 29 Abs. 1 VAG umfasst das IKS zudem mindestens: ein Verwaltungs- und Rechnungslegungsverfahren, einen internen Kontrollrahmen, eine angemessene unternehmensinterne Berichterstattung.
12 Vgl. Art. 40 Solva II-RL: Die Letztverantwortung dafür, dass die „gemäß dieser Richtlinie erlassenen Rechts- und Verwaltungsvorschriften durch das Unternehmen“ beachtet werden, trägt der Vorstand.
13 Angelehnt an Prölss/Dreher/*Dreher*, VAG, 13. Aufl. 2018, § 23 Rn. 19.

Als bildhafte Veranschaulichung kann vor diesem Hintergrund das „Modell der drei Verteidigungslinien" verstanden werden. Danach sind auf der „1. Verteidigungslinie" die Mitarbeiter/Führungskräfte verantwortlich, Risiken im Tagesgeschäft zu identifizieren, zu analysieren und zu bewerten. Auf dieser Basis müssen angemessene und wirksame Verfahren zur Einhaltung der rechtlichen Vorgaben eingerichtet und durchgeführt werden. Die Compliance-Funktion überwacht auf der „2. Verteidigungslinie", dass prozessintegrierte Kontrollen im operativen Bereich ordnungsgemäß durchgeführt werden.[14, 15] Auf der „3. Verteidigungslinie" prüft die Revision das Governance-System prozessunabhängig und nachgelagert. Organisatorische Anforderungen sowie Gegenstand und Reichweite der Aufgaben lassen sich für die Schlüsselfunktionen aus dem Modell nicht unmittelbar ableiten, da die rechtlichen Vorgaben für Versicherungsunternehmen konkretere und teils abweichende Vorgaben machen. Insbesondere weist die Solva II-RL den Funktionen bestimmte Aufgaben zu, stellt aber keine „Hierarchie" zwischen den Schlüsselfunktionen auf.[16] Gleichzeitig ist für das Zusammenwirken der Schlüsselfunktionen der für die Risikocontrolling-Funktion und die interne Revisionsfunktion gesetzlich explizit hervorgehobene Grundsatz der Funktionsunabhängigkeit zu beachten.[17]

Vor diesem Hintergrund überwacht die Compliance-Funktion auch, ob die anderen Governance-Funktionen ordnungsgemäß eingerichtet und wirksam sind. Die Überwachung des für alle Schlüsselfunktionen geltenden Kriteriums der Wirksamkeit ist angesichts der Gleichrangigkeit und Unabhängigkeit im Verhältnis der Schlüsselfunktionen zueinander eng auszulegen. So überwacht die Compliance-Funktion beispielsweise die Wirksamkeit der internen Revisionsfunktion nur dahingehend, ob sie objektiv ihrer gesetzlichen Prüfungsaufgabe nachkommt. Die Compliance-Funktion hat dagegen kein Mandat, auch die inhaltliche Eignung und Effektivität der Prozesse und Verfahren der internen Revisionsfunktion auf den Prüfstand zu stellen.

Zur Abgrenzung der Schlüsselfunktionen und ihrer jeweiligen Aufgaben siehe näher das GDV-Diskussionspapier „Governance-Funktionen unter Solvency II: Kernaufgaben und Schnittstellenfragen".

---

14 Nicht zwingend erforderlich ist es, dass die Compliance-Funktion selbst angemessene Verfahren implementiert, vgl. BaFin-MaGo (Vollnachweis s. Fn. 20), Rn. 87.

15 Zur 2. Verteidigungslinie gehören in diesem Modell auch die unabhängige Risikocontrolling-Funktion und die versicherungsmathematische Funktion; vgl. GDV-Diskussionspapier „Governance-Funktionen unter Solvency II: Kernaufgaben und Schnittstellenfragen" S. 10.

16 Prölss/Dreher/*Dreher,* VAG, 13. Aufl. 2018, § 29 Rn. 10; s. auch BaFin-MaGo Rn. 76.

17 §§ 26 Abs. 8, 30 Abs. 2 VAG, Art. 271 Abs. 2 Solva II-VO.

2. EIOPA-Leitlinien und BaFin-Verlautbarungen

Die **EIOPA-Leitlinien**[18] **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.[19]

Zur Compliance-Funktion hat sich die BaFin dennoch insbesondere in den **Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo)** in Kapitel 9.2 geäußert.[20] Mit der MaGo sollen die Vorschriften über die Geschäftsorganisation im VAG und in der Solva II-VO aus Sicht der BaFin für die Behördenpraxis verbindlich ausgelegt werden.[21] Für die Versicherungsunternehmen sind die MaGo rechtlich unverbindlich. Aufsichtsbehördlich ist zudem die BaFin-Verlautbarung zur Qualifikation[22] und die BaFin-Auslegungsentscheidung „Aspekte der Vergütung (Art. 275 DVO (EU) 2015/35)“ vom 20.12.2016 relevant.

III. Praxisstandards

Die Compliance-Organisation wird darüber hinaus in Leitlinien und Standards verschiedener Institutionen angesprochen. Hinweise sind etwa in der ISO-Leitlinie ISO 19600, im IDW PS 980, dem DICO-Standard „Compliance-Management-System“[23] oder auch im Deutschen Corporate Governance Kodex[24] sowie in einem Leitfaden des US-Department of Justice[25] enthalten.

Solche Standards sind für sich genommen rechtlich unverbindlich. Ihre Befolgung führt nicht per se zu einer hinreichenden Compliance-Organisation und kann eine Pflichtverletzung nicht ausschließen. Ratsam erscheint es, ohne eine Befolgungspflicht zugrunde zu legen, solche Standards in die Ausgestaltung der Compliance-Organisation einzubeziehen und ihre Inhalte ggf. entsprechend des unternehmensindividuellen Risikoprofils anzupassen. Maßgeblich bleiben jedoch allein die verbindlichen und für Versicherungsunternehmen konkreteren rechtlichen Vorgaben.

---

18 Die EIOPA-Leitlinien richten sich an die nationalen Aufsichtsbehörden der Mitgliedstaaten und sind für die Unternehmen rechtlich unverbindlich. Die nationalen Aufsichtsbehörden können entscheiden, ob sie die Leitlinien umsetzen. Sie müssen berichten, ob sie umgesetzt haben. In jedem Fall ist eine Erklärung gegenüber EIOPA notwendig („comply-or-explain“). Die BaFin hat als Adressat der EIOPA-Leitlinien insoweit vollständig „comply“ erklärt.

19 EIOPA-Leitlinien zum Governance-System, Ziffer 1.4 und 1.34. Als Begründung für diese Zurückhaltung teilt die EIOPA mit: „Article 46 of the Solvency II Directive and Article 270 of the Commission Delegated Regulation 2015/35 describe the tasks of the compliance function. EIOPA does not consider it necessary to explain further what the compliance function should do at this point in time.“, EIOPA-BoS-14/25328, Januar 2015, Ziffer 2.15.

20 BaFin, Rundschreiben 2/2017 (VA) v. 25.01.2017, geändert am 02.03.2018. Eine Überarbeitung der MaGo ist angekündigt.

21 So Kapitel 1 des Rundschreibens.

22 Siehe näher unten D. V.

23 Der DICO e. V. entwickelt derzeit (Stand November 2020) einen solchen Standard zu Compliance-Management-Systemen mit einem branchenübergreifenden Ansatz.

24 Die Erklärungspflicht zum Deutschen Corporate Governance Codex gilt gem. § 161 AktG für börsennotierte Gesellschaften. Der Kodex kann aber auch ggf. darüber hinaus für Versicherungsunternehmen hilfreiche Hinweise liefern.

25 U.S. Department of Justice, Evaluation of Corporate Compliance Programs (Updated June 2020), abrufbar unter *https://www.justice.gov/criminal-fraud/page/file/937501/download* (zuletzt abgerufen: Februar 2021).

C. Operative Anforderungen der Compliance-Funktion

I. Begriff der Compliance-Funktion

Die Compliance-Funktion ist ein mit adäquaten Personal- und Sachmitteln ausgestatteter Aufgabenbereich (vgl. Art. 13 Nr. 29 der Solva II-RL) zur Übernahme der durch die Richtlinie zugewiesenen Compliance-Aufgaben.

II. Aufgabe der Compliance-Funktion

1. Aufsichtsrechtliches Pflichtprogramm nach Solva II

a. Aufgaben gem. Art. 46 Solva II-RL bzw. § 29 VAG

Die Aufgaben der Compliance-Funktion unter Solva II ergeben sich aus Art. 46 Solva II-RL bzw. § 29 Abs. 1 und 2 VAG sowie aus Art. 270 Solva II-VO. Sie können wie folgt zusammengefasst werden:

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

Hilfestellung:

- **Überwachung** ist die Beurteilung des Aufbaus und der kontinuierlichen operativen Funktionsfähigkeit der Kontrollen zur Mitigierung von Compliance-Risiken. Die Überwachung sollte periodisch wiederkehrend und/oder durch einen Einzelfall getrieben erfolgen. Die Schnittstelle zwischen den Aufgaben der Überwachung und Risikokontrolle sind fließend, da im Zuge der Analyse von Compliance-Risiken, Maßnahmen zu deren Mitigation definiert und deren Umsetzung überwacht wird. **Kontrollen** sind interne Maßnahmen, die dazu dienen, Compliance-Risiken zu steuern und die Wahrscheinlichkeit zu erhöhen, dass bestehende Vorgaben eingehalten und gesetzte Ziele erreicht werden.
- Typische Kontrollen sind das Mehr-Augen-Prinzip, Funktionstrennung, aber auch IT-basierte Überprüfungen. Kontrollen können auf Verhinderung und/oder Aufdeckung von Fehlern und Verstößen gerichtet sein.

Objekte der Überwachung:

- Beurteilung, ob die internen Vorgaben die Einhaltung der externen Anforderungen sicherstellen, d. h. ob bspw. eine Richtlinie ausreichend ist, um einen Verstoß gegen eine externe Anforderung zu verhindern oder aufzudecken („Test of Design").
- Beurteilung, ob interne Vorgaben effektiv in den operativen Bereichen umgesetzt sind („operative Funktionsfähigkeit").
- Festlegung des Umfangs und die Auswahl der zu prüfenden Kontrollen und Gesellschaften erfolgen risikobasiert oder einzelfallgetrieben.

Die Überwachungsaufgabe der Compliance-Funktion bezieht sich auch auf die externen Anforderungen an eine ordnungsgemäße Geschäftsorganisation. Diese ist vom gesetzlichen Prüfungsmandat der internen Revisionsfunktion bezüglich der

Angemessenheit und Wirksamkeit der gesamten Geschäftsorganisation und insbesondere des internen Kontrollsystems sachgerecht abzugrenzen.[26]

Zudem wird der Compliance-Funktion gem. Art. 270 Abs. 2 Solva II-VO die Aufgabe zugewiesen, zu bewerten, ob die präventiven Maßnahmen, die zur Vermeidung von Rechtsverstößen ergriffen wurden, **angemessen** sind.

- **Beratungsaufgabe:** Ferner zählt zu den Aufgaben der Compliance-Funktion auch die Beratung des Vorstandes in Bezug auf die Einhaltung der in Übereinstimmung mit der Solva II-RL erlassenen Rechts- und Verwaltungsvorschriften[27] und der auf dieser Basis erforderlichen unternehmensinternen Leitlinien. Weitergehend bezieht § 29 Abs. 2 Satz 1 VAG die Beratungsaufgabe auf Rechtsvorschriften, „die für den Betrieb des Versicherungsgeschäfts gelten".[28]

  Über den Vorstand können Unternehmen auch die Mitarbeiter des Unternehmens als Adressaten der Beratung einbeziehen, was die anderen Schlüsselfunktionen einschließt.[29]

- **Risikokontrollaufgabe:** Die Compliance-Funktion hat das mit der Nicht-Einhaltung der rechtlichen Vorgaben verbundene Risiko („Compliance-Risiko") zu identifizieren und beurteilen, § 29 Abs. 2 Satz 2 VAG.

  Gegenständlich sind hiervon alle Rechtsbereiche erfasst.[30] Die Identifizierung und Beurteilung des Compliance-Risikos setzt eine unternehmensindividuelle Risikoanalyse durch die Compliance-Funktion voraus. Darauf aufbauend sind entsprechende risikomitigierende Compliance-Aktivitäten abzuleiten und im Compliance-Plan zu erfassen.

- **Frühwarnaufgabe:** Zu den Aufgaben der Compliance-Funktion gehört auch die Beurteilung der möglichen Auswirkung von sich abzeichnenden Änderungen des Rechtsumfeldes auf die Tätigkeit des betreffenden Unternehmens (Rechtsumfeldrisiken).[31] 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 Legalitätskontrollpflicht entsprechen kann. Dazu müssen die für das Versicherungsunternehmen relevanten Rechtsgebiete identifiziert sowie die in diesen Rechtsgebieten vorhandenen Rechtsänderungs- und Rechtsprechungsrisiken erkannt und bewertet werden. Die Compliance-Funktion muss dazu u. a. die relevanten politischen Entwicklungen auf nationaler und internationaler Ebene sowie die einschlägige Rechtsprechung laufend verfolgen und systematisch analysieren. Dies muss auch unter Solva II nicht vollumfänglich durch eine zentrale Complian-

26 § 30 Abs. 1 VAG.
27 So Art. 46 Abs. 2 Satz 1 Solva II-RL.
28 Die engere Formulierung des Art. 46 Abs. 2 Satz 1 Solva II-RL ist insoweit nicht abschließend („zählt auch").
29 *Bürkle*, Compliance in Versicherungsunternehmen, 3. Aufl. 2020, § 2 Rn. 150; weitergehend Prölss/Dreher/*Dreher*, VAG, 13. Aufl. 2018, § 29 Rn. 127 („hat daher eine Beratungsaufgabe").
30 *Bürkle*, Compliance in Versicherungsunternehmen, 3. Aufl. 2020, § 2 Rn. 158.
31 § 29 Abs. 2 Satz 2 VAG; s. dazu auch BaFin-MaGo, Rn. 91.

ce-Abteilung selbst geschehen. Vielmehr bieten sich sachgerechte Schnittstellen zu anderen Bereichen an, in denen Rechtsbeobachtung bereits geleistet wird.

Die konkrete Aufgabenerfüllung der Compliance-Funktion ist unternehmensindividuell am Grundsatz der Risikoorientierung[32] und Proportionalität (Verhältnismäßigkeit) bzw. Wesentlichkeit[33] auszurichten. Dies ermöglicht eine zum jeweiligen Unternehmen passende Priorisierung und Ausgestaltung der Tätigkeiten.

b. Tätigkeitsumfang der Compliance-Funktion

Gem. Art. 46 Abs. 1 Solva II-RL bzw. § 29 Abs. 1 VAG **überwacht** die Compliance-Funktion die Einhaltung der Anforderungen (an das Unternehmen). Nach wie vor wird der rechtlich zwingende Tätigkeitsumfang der Compliance-Funktion unterschiedlich beurteilt.

Verbreitet werden die Aufgaben der Compliance-Funktion über die versicherungsorganisatorischen Vorgaben der Solva II-RL hinaus auf versicherungsspezifische Vorgaben oder auf sämtliche für das Unternehmen geltenden rechtlichen Vorgaben bezogen.[34] Die BaFin führt dahingehend in den MaGo aus, dass die Compliance-Funktion „die Einhaltung der zu beachtenden Gesetze und Verordnungen, aufsichtsbehördlichen Anforderungen sowie sonstigen externen Vorgaben und Standards" überwacht.[35]

Allerdings spricht die Solva II-RL für eine einschränkende Auslegung.[36] Der **Tätigkeitsumfang** der Compliance-Funktion umfasst nach Solva II nur die Einhaltung **aller Rechts- und Verwaltungsvorschriften**, die **zur Umsetzung der Solva II-RL** erlassen wurden. Diese Beschränkung lässt sich systematisch mit Blick auf Art. 40 der Richtlinie begründen: Danach tragen die Geschäftsleiter die „letztendliche Verantwortung für die Einhaltung der gem. dieser [Solva II-]Richtlinie erlassenen Rechts- und Verwaltungsvorschriften". Da die Compliance-Funktion eine delegierte Vorstandspflicht ist, kann ihr Verantwortungsumfang nicht über den der Geschäftsleitung hinausgehen. Für die **Beratungsaufgabe** ergibt sich die Beschränkung des Tätigkeitsumfangs bereits nach dem eindeutigen Wortlaut von Art. 46 Abs. 2 der Richtlinie, der den Umfang auf die „Einhaltung der in Übereinstimmung mit dieser Richtlinie erlassenen Rechts- und Verwaltungsvorschriften" beschränkt; umgesetzt in § 29 Abs. 2 VAG: **„Einhaltung der Gesetze und Verwaltungsvorschriften, die für den Betrieb des Versicherungsgeschäftes gelten"**.[37]

---

32 Prölss/Dreher/*Dreher*, VAG, 13. Aufl. 2018, § 29 Rn. 102 ff.

33 Zur Proportionalität vgl. Prölss/Dreher/*Dreher*, VAG, 13. Aufl. 2018, § 29 Rn. 108 f. und MüKo VVG/*Nowak-Over*, 2. Aufl., Band 3, 2. Teil., 2. Kapitel., 170., Rn. 106.

34 Prölss/Dreher/*Dreher*, VAG, 13. Aufl. 2018, § 29 Rn. 112 ff., nach dem der Aufgabenbereich allerdings anhand der Risikoorientierung sachgerecht zu bestimmen ist. Ebenfalls weit Kaulbach/Bähr/Pohlmann/*Pohlmann*, VAG, 6. Aufl., § 29 Rn. 26, 29, wonach „alle verbindliche Regelungen, deren Nichteinhaltung den Schutz der Belange der Versicherten und die Gewährleistung der Erfüllbarkeit der Verpflichtungen gefährden kann", einzubeziehen sind, was jedenfalls versicherungsaufsichtsrechtliche und versicherungsspezifische Regelungen erfasse. Darüber hinaus müsse das Unternehmen prüfen, welche Rechtsbereiche in die Überwachung einzubeziehen seien.

35 BaFin-MaGo Rn. 86.

36 *Bürkle* in Bürkle, Compliance in Versicherungsunternehmen, 3. Aufl. 2020, § 2 Rn. 129 ff.

37 Vgl. dazu auch BaFin-MaGo Rn. 90.

Bedeutung hat der Streit im Hinblick auf die Reichweite der Kompetenzen der Aufsichtsbehörden und für deren Eingriffsbefugnisse gegenüber dem Unternehmen, den Unternehmensorganen und den Inhabern der Compliance-Funktion. In der Praxis dürfte der Streit dadurch entschärft werden, dass die BaFin für die Überwachung auf die Rechtsbereiche abstellt, die mit **wesentlichen Risiken** verbunden sind und hierfür die für den Betrieb des Versicherungsgeschäftes geltenden Gesetze, Verordnungen und aufsichtsbehördlichen Anforderungen nennt.[38] Gleichwohl fasst die BaFin dies als Mindestaufgabe auf, sodass davon auszugehen ist, dass sie ihr Aufsichtsmandat ungeachtet der fehlenden rechtlichen Grundlage weiter versteht und auch auf Compliance-Tätigkeiten außerhalb des durch Solva II vorgegebenen Rahmens erstreckt.

Weitergehend führt die BaFin in den MaGo aus, dass die Compliance-Funktion auch **sonstige „externe Vorgaben und Standards"** überwacht.[39] Dies ist kritisch, soweit sie sich auf Standards und Vorgaben von „national oder international anerkannten Akteuren" mit hoher Fachkompetenz bezieht.[40] Versicherungsunternehmen sollten demnach anhand ihrer Geschäftstätigkeit und ihres Risikos individuell beurteilen, welche Vorgaben und Standards für sie „von großer Bedeutung sind oder mit wesentlichen Risiken einhergehen."[41] Hier geht die Aufsicht über die Grenze der gesetzlichen Überwachungspflicht hinaus, da Standards nicht mit verbindlichen rechtlichen Vorgaben gleichgesetzt werden können. Damit ist es keine Aufgabe der Compliance-Funktion. Solche Standards und Anforderungen können allerdings – auch soweit sie keine (formale) Rechtsqualität haben – im Einzelfall beachtliche Hinweise enthalten und als Rechtserkenntnisquelle zu berücksichtigen sein.[42] Zu berücksichtigen ist auch, dass unternehmerische Entscheidungen auf informierter Grundlage zum Wohle der Gesellschaft getroffen werden müssen (§ 93 Abs. 1 Satz 2 AktG).

Entsprechend der dargestellten unterschiedlichen Auffassungen ist die **sachliche Reichweite der Compliance-Funktion** umstritten. Im Sinne der aufgezeigten engeren richtlinienkonformen Auslegung umfasst der Pflichtenkreis der Compliance-Funktion jedenfalls die aufsichtsrechtlichen Vorgaben, die das VAG in Umsetzung der Solva II-RL für den Betrieb des Versicherungsgeschäfts vorsieht, und die unmittelbar geltenden Vorgaben der Solva II-VO. Dazu gehören die Anforderungen im Hinblick auf die Organisation und die zulässigen Aktivitäten der Versicherungsunternehmen.

2. Compliance im Rahmen der Legalitätskontrollpflicht

Jedenfalls im Rahmen der allgemeinen gesellschaftsrechtlichen Legalitätskontrollpflicht,[43] die über die aufsichtsrechtsrechtliche Pflicht hinausgeht, unterliegen Versicherungsunternehmen der Pflicht, alle Strukturen und Prozesse im Unternehmen so auszurichten, dass die Einhaltung sämtlicher wesentlicher externer und interner Vor-

38 BaFin-MaGo Rn. 88
39 BaFin-MaGo Rn. 86.
40 BaFin, FAQ zu MaGo, zu Rn. 86.
41 Näher BaFin, FAQ zu MaGo, zu Rn. 86.
42 *Bürkle* in Bürkle, Compliance in Versicherungsunternehmen, 3. Aufl. 2020, § 2 Rn. 24 f.
43 Siehe oben B. I.

schriften gewährleistet ist.[44] Im Rahmen dieser gesellschaftsrechtlichen Compliance-Pflicht ist es Aufgabe, 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 eingesetzt und vorgehalten werden sollen. Andererseits ist festzulegen, welche Maßnahmen dazu mit welchen Mitarbeiterkapazitäten oder sonstigen Ressourcen jeweils vorzunehmen sind.

Unternehmensindividuell kann festgelegt werden, diese Aufgabe im Rahmen der Compliance-Funktion wahrzunehmen.

Risikorelevante Rechtsgebiete

Besondere Bedeutung kommt für Versicherungsunternehmen der Einhaltung der Vorgaben für risikorelevante Rechtsgebiete zu, bei denen eine Non-Compliance zu hohen Geldbußen, hohen finanziellen Belastungen oder Reputationsverlusten führen kann. Hierzu gehören insbesondere folgende Bereiche:

- Kartellrecht,
- Korruptionsprävention (insbes. §§ 299 ff. StGB),[45]
- Datenschutzrecht,
- Wirtschaftssanktionen,
- Vorgaben zur Verhinderung von Geldwäsche und Terrorismusfinanzierung,
- Kapitalmarktrecht.

Ebenfalls steht im Bereich der risikorelevanten Regeln z. B.[46] das Thema „**Compliance im Vertrieb**": Neben der Einhaltung der anlassbezogenen Beratungs- und Informationspflichten der Versicherungsunternehmen und 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-Tätigkeit. Dazu gehören beispielsweise ein Verhaltenskodex[47] für die Vermittler sowie Schulungs- und Überwachungsmaßnahmen, die die Einhaltung auch der über regula-

---

44 Eine Differenzierung zwischen gesellschaftsrechtlicher und aufsichtsrechtlicher Compliance dagegen ablehnend etwa Kaulbach/Bähr/*Pohlmann*, VAG, 6. Aufl. 2019, § 29 Rn. 26.

45 Siehe hierzu auch die GDV-Orientierungshilfe zur strafrechtlichen Beurteilung von Einladungen und Geschenken, abrufbar im GDVportal.

46 Die in diesem Abschnitt illustrierten Regelungsbereiche erheben mit Blick auf ihre Risikorelevanz keinen Anspruch auf Vollständigkeit. Compliance-Risiken können auch durch regulatorische Vorgaben in anderen Geschäftsbereichen, wie z. B. Kapitalanlage oder Einkauf entstehen.

47 Siehe auch den GDV-Verhaltenskodex für den Vertrieb, der die Möglichkeit einer freiwilligen Selbstverpflichtung bietet; hier abrufbar: *https://www.gdv.de/de/themen/news/verhaltenskodex-fuer-den-vertrieb-11518*.

torische Anforderungen hinausgehenden Regeln sicherstellen sollen. Relevant sind die Vorgaben zu **Product Oversight and Governance (POG)**, die auf der IDD-Richtlinie[48] beruhend in § 23 Abs. 1a-1d VAG sowie konkreter und vorrangig in der POG-VO geregelt sind. Weder die IDD noch die nationale Umsetzung sehen explizit eine Rolle der Compliance-Funktion vor. Über die Art und Weise der Einbindung der Compliance-Funktion ist daher im Einzelfall und abhängig von der konkreten Rolle der Compliance-Funktion im Unternehmen zu entscheiden.

Weitere inhaltliche Vorgaben in Bezug auf die Rechtmäßigkeit der Produkte enthält das **Versicherungsvertragsrecht (VVG)**.

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

Der Compliance-Funktion können schließlich 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. 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.

4. Aufgaben im Krisenfall

Besondere Bedeutung kann der Compliance-Funktion bzw. -Organisation im Fall einer Krise zukommen. Infolge äußerer Einflüsse kann es zu unvorhersehbaren und plötzlichen Änderungen des Rechtsumfeldes und tatsächlicher Umstände kommen, die sich auf die Geschäftstätigkeit der Versicherungsunternehmen auswirken können.[49] Dies kann Compliance-Risiken entstehen lassen, die von der Compliance-Organisation[50] zu berücksichtigen sind. Insbesondere wird es einer Intensivierung der Überwachungstätigkeit und der Beratung des Vorstands bedürfen. Die Rolle der Compliance-Funktion ändert sich damit nicht, führt aber ggf. zu einem intensivierten Handlungsbedarf, wobei oftmals unter hohem Zeitdruck und unter rechtlicher Unsicherheit gehandelt werden muss.

---

48 Richtlinie (EU) 2016/97.

49 Einschneidendes Beispiel ist die Corona-Pandemie, die neben erheblichen Auswirkungen tatsächlicher Art zu einer Vielzahl an Rechtsänderungen mit Bedeutung für Versicherungsunternehmen führte und führt.

50 Die Analyse, Überwachung und Minimierung von Compliance-Risiken, die durch tatsächliche Umstände hervorgerufen werden, muss dabei nicht zwingend der Compliance-Funktion zugeordnet werden.

III. Compliance-Leitlinie

Die Einrichtung der Compliance-Funktion ist in einer Compliance-Leitlinie niederzulegen und zu dokumentieren (Art. 270 Abs. 1 Solva II-VO). Sie umfasst Zuständigkeiten, Befugnisse und die Berichtspflichten der Compliance-Funktion.[51] Ein solches Dokument dient der klaren Festlegung von Kompetenzen und beschreibt die konkrete Organisationsstruktur und somit zugleich die Schnittstellen zu den übrigen Governance-Funktionen. Die Leitlinie muss durch den Vorstand beschlossen werden.

Compliance-Leitlinie – Unverbindliche Checkliste:

I. Ziel der Leitlinie

- Die Compliance-Leitlinie enthält die erforderlichen Angaben zu den Zuständigkeiten, den Befugnissen und den Berichtspflichten der Compliance-Funktion.
- Die Compliance-Leitlinie verweist auf die einschlägigen Regelungen im VAG, in der Solva II-RL und in der Solva II-VO.

II. Geltungsbereich

- Solo-Unternehmen mit aufsichtsrechtlich obligatorischer Compliance-Funktion.
- Versicherungsgruppen aus Unternehmen mit aufsichtsrechtlich obligatorischer Compliance-Funktion.

III. Verfahren zur Überprüfung und Veränderung der Leitlinien

- Entscheidungsträger
- Änderungsvorschläge der Compliance-Funktion
- Regulärer Überprüfungsturnus
- Anlässe für Ad-hoc-Überprüfung

IV. Inhalte

1. Zuständigkeiten

- Aufgaben
  - Überwachung
  - Beratung
  - Frühwarnen
  - Risikokontrolle
  - Compliance-Bericht
  - Ad-hoc-Bericht
  - Zusammenarbeit mit anderen Funktionen, insbesondere Zusammenarbeit mit den Governance-Funktionen und -Bereichen
  - Compliance-Plan
  - Compliance-Assessment (Bewertung der Angemessenheit der getroffenen Maßnahmen zur Verhinderung einer Non-Compliance)
- Organisation
  - Letztverantwortung der Geschäftsleitung
  - Organisationsstruktur (zentral/dezentral)
  - Objektivität, Fairness und Unabhängigkeit
  - Ressourcen
  - Qualifikation
  - Auslagerung

2. Befugnisse

- Rechte
  - Kommunikationsmöglichkeiten
  - Informationszugang
- Pflichten
  - spiegelbildlich zu Rechten
  - Autorität, Ressourcen und Fachkunde

51 Art. 270 Abs. 1 Solva II-VO.

3. Berichtspflichten

- Adressaten
  - Verwaltungs-, Management- oder Aufsichtsorgan
  - bei dualistisch organisierten Versicherungsunternehmen: Vorstand
  - optional: Aufsichtsrat/Prüfungsausschuss
  - keine direkte Berichtspflicht gegenüber Aufsichtsbehörden
- Berichtsturnus
  - Regelbericht (jährlich)
  - Ad-hoc-Bericht bei größeren Problemen oder Verdachtsfällen
- Inhalt Regelbericht
  - Überwachungsverfahren (Angaben zu den wichtigsten Verfahren des internen Kontrollsystems)
  - Tätigkeiten während des Berichtszeitraums
  - Überprüfung eventueller signifikanter Veränderungen
  - Status Compliance-Plan
  - Compliance-Verstöße
- Form
  - keine Vorgabe
  - Dokumentationserfordernis
  - Schriftlicher Bericht (plus mündliche Erläuterung)
  - Präsentation (plus mündliche Erläuterung)

IV. Compliance-Plan

Die Aktivitäten der Compliance-Funktion erfolgen auf Basis eines Compliance-Plans. Darin sind gem. Art. 270 Abs. 1 Solva II-VO die geplanten Tätigkeiten der Compliance-Funktion, wie z. B. vorgesehene Überwachungshandlungen, unter Berücksichtigung aller relevanten Tätigkeitsbereiche und des bestehenden Compliance-Risikos darzulegen. Die wesentlichen Inhalte des Compliance-Planes sind vom Vorstand zu verabschieden.[52] Nach Auffassung der BaFin ist die Aktualität des Compliance-Planes regelmäßig zu überprüfen.[53]

Die relevanten Tätigkeits- bzw. Geschäftsbereiche sind unternehmensindividuell zu definieren. Die Auswahl der Aktivitäten sollte risikoorientiert erfolgen.[54] Das Unternehmen kann individuell eine Schwelle für „unwesentliche" Risiken festlegen. Diese sollte 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.

Die rechtlichen Vorgaben lassen Spielraum in der Planung der Aktivitäten. Sie sollten sich an den vier Aufgaben der Compliance-Funktion (Risikoanalyse, Früherkennung, Beratung, Überwachung) orientieren und zudem die „risikomindernden Maßnahmen" erfassen.

Für Aufbau und Detailtiefe des Compliance-Plans bestehen keine verbindlichen rechtlichen Vorgaben.

52 Dies folgt aus der Letztverantwortung des Vorstands für die Schlüsselfunktionen gem. Art. 268 Abs. 1 S. 2 Solva II-VO.
53 Vgl. BaFin-MaGo Rn. 94.
54 Dies folgt bereits aus dem gem. Art. 270 Abs. 1 Solva II-VO zu berücksichtigenden Compliance-Risiko.

V. Compliance-Instrumente

Die Überschrift präjudiziert keine zwingende Zuständigkeit der Compliance-Funktion. Compliance-Instrumente können im Rahmen der unternehmerischen Organisationsfreiheit auch anderen Einheiten oder Personen zugeordnet werden.

Mit welchen Mitteln die Compliance-Aufgaben wahrzunehmen sind, wird rechtlich im Einzelnen nicht vorgegeben. Beispielsweise kommen folgende übergreifende Instrumente in Betracht:

- **Compliance-Gremium**

  In Abhängigkeit von der unternehmensindividuellen Komplexität und Organisationsstruktur kann die Einrichtung eines Compliance-Gremiums hilfreich sein, in dem die Schlüsselfunktionen und die wesentlichen Fachabteilungen des Unternehmens vertreten sind.[55] Das Gremium kann dem regelmäßigen Erfahrungsaustausch dienen, aktuell auftretende Compliance-Fragen behandeln oder nach unternehmensindividuell formalisierten Regeln an Compliance-bezogenen Entscheidungen beteiligt sein.

- **Richtlinienwesen**

  Regelungen zum Umgang mit einzelnen Compliance-Risiken können in unternehmensindividuellen Richtlinien (Verhaltenskodices) adressiert werden. Mittels der Richtlinien können konkrete Verhaltensmaximen und Handlungsanweisen für die Mitarbeiter beschrieben werden. Dies kann sich für als wesentlich identifizierte Risikobereiche der Compliance empfehlen.

- **Berichtswesen**

  Zur effektiven Erfüllung der Compliance-Aufgaben ist eine geregelte Kommunikation im Unternehmen mittels eines Berichtswesens vorzusehen. Es ist in Leitlinien festzulegen, dass die relevanten organisatorischen Einheiten die Compliance-Funktion über die Sachverhalte unterrichtet, die zur Erfüllung ihrer Pflichten erforderlich sind.[56] Zu den erforderlichen bzw. empfehlenswerten Berichtswegen siehe näher unter D.VI.

- **Hinweisgebersystem**

  Für die Aufdeckung von Compliance-relevanten Fehlentwicklungen und Verstößen können Hinweise von Mitarbeitern oder auch Dritten relevant sein. Versicherungsunternehmen müssen gem. § 23 Abs. 6 VAG einen Prozess vorsehen, der es Mitarbeitern unter Wahrung ihrer Vertraulichkeit ermöglicht, potenzielle und tatsächliche Rechtsverstöße zu melden. Der sachliche Anwendungsbereich ist allerdings eingeschränkt.[57] Vorgaben zur Einrichtung von internen Kanälen und Verfahren zur Meldung von bestimmten Verstößen gegen das EU-Recht macht zudem die EU-Whistleb-

---

55 *Schlierenkämper* in: Bürkle, Compliance in Versicherungsunternehmen, 3. Aufl. 2020, § 11 Rn. 187.
56 EIOPA-Leitlinien zum Governance-System, Rn. 1.34.
57 Erfasst sind Verstöße gegen das VAG, auf dem VAG beruhenden Rechtsverordnungen, gegen die Marktmissbrauchsverordnung (VO (EU) 596/2014), PRIIP-VO (VO (EU) 1286/2014) sowie etwaige strafbare Handlungen innerhalb des Unternehmens.

lowing-Richtlinie.[58] Daneben existiert eine Vielzahl weiterer Vorgaben zu Hinweisgebersystemen, die auch Versicherungsunternehmen betreffen können.[59]

Solche Hinweise können aus Compliance-Sicht eine erhebliche Erkenntnisquelle darstellen. Im Rahmen der unternehmerischen Organisationsfreiheit kann daher eine Öffnung des Hinweisgebersystems über den rechtlich vorgegebenen Anwendungsbereich hinaus für andere Verstöße sinnvoll sein.

- **Interne Ermittlungen**

  Unternehmensinterne Ermittlungen (internal investigations) dienen der Abklärung von Verdachtsmomenten, um mögliche Compliance-Verstöße auszuschließen oder aufdecken, abstellen, sanktionieren und für die Zukunft vermeiden zu können. Sie können daher die Wahrnehmung der Compliance-Aufgaben unterstützen. Eine eigenständige Aufklärung von Compliance-Verstößen kann sich zudem positiv auf eine ordnungswidrigkeiten- oder strafrechtliche Haftung auswirken.[60] Die Durchführung von internen Untersuchungen kann komplexe Fragestellungen aufwerfen, etwa hinsichtlich der Mitwirkungspflicht von Mitarbeitern, des Datenschutzes, der betrieblichen Mitbestimmung und der Beschlagnahmefähigkeit der Untersuchungsergebnisse durch Verfolgungsbehörden.

---

58 Richtlinie (EU) 2019/1937. Die Richtlinie muss (in wesentlichen Teilen) bis zum 17. Dezember 2021 in nationales Recht umgesetzt werden. Sie erfasst beispielsweise auch Verstöße gegen die Vorgaben der Solva II-RL und der Solva II-VO.

59 Z. B. § 6 Abs. 5 GwG, Art. 32 Abs. 3 MAR.

60 Siehe dazu auch den Regierungsentwurf eines Verbandssanktionengesetzes (Gesetzentwurf der BReg eines Gesetzes zur Stärkung der Integrität in der Wirtschaft v. 16.06.2020, Bundestags-Drucks. 19/23568), das eine obligatorische Milderung der neu einzuführenden Verbandssanktion vorsieht, wenn das Unternehmen durch verbandsinterne Untersuchungen wesentlich zur Aufklärung der Verbandstat und -verantwortlichkeit beiträgt, § 17; siehe hierzu auch unter E.

D. Organisatorische Anforderungen

Die unter B. und C. skizzierten (aufsichts-)rechtlichen Vorgaben haben Auswirkungen darauf, wie die Compliance-Funktion in den Versicherungsunternehmen ausgestaltet werden muss.

I. Allgemeine Prinzipien

- **Gestaltungsfreiheit im Rahmen der allgemeinen Organisationspflicht**

  Die Organisationsform bzw. die konkreten Prozessabläufe der Compliance-Funktion sind nicht detailliert vorgegeben. Die Solva II-RL verfolgt den Ansatz einer prinzipienbasierten Regulierung. Es obliegt deshalb der Entscheidung der Unternehmen, wie die in der Richtlinie vorgegebenen Ziele erreicht werden sollen. Im Rahmen der nationalen Umsetzung und der delegierten Rechtsakte besteht eine weitgehende Freiheit im Hinblick auf die Ausgestaltung ihrer Corporate Governance.[61] Nachfolgend sollen praktische Hinweise für die Umsetzung gegeben werden.

- **Proportionalitätsgrundsatz**

  Bei der Aufgabenwahrnehmung durch die Compliance-Funktion ist der **aufsichtsrechtliche Proportionalitätsgrundsatz** (Art. 41 Abs. 2 Solva II-RL) zu beachten. Danach hängen die Anforderungen an die organisatorischen Maßnahmen zur Erfüllung der Compliance-Funktion wesentlich von der Art und Umfang sowie der Komplexität der Geschäftstätigkeit und des damit verbundenen Risikos ab. Zu beachten ist, dass sich der Proportionalitätsgrundsatz nach umstrittener Ansicht der BaFin nicht auf das „Ob" der Aufgabenwahrnehmung durch die Compliance-Funktion, sondern immer nur auf deren Reichweite und Tiefe („Wie") auswirkt.[62] Des Weiteren haben die Größe des Unternehmens, die Art, Umfang und regionale Ausdehnung des betriebenen Versicherungsgeschäfts, die angebotenen Produkte, 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.

- **Ausreichende Befugnisse und Unabhängigkeit**

  Bei der Organisation der Compliance-Funktion sind die **zur Aufgabenerfüllung notwendigen Befugnisse und die gebotene Unabhängigkeit** sicherzustellen.[63] Die Compliance-Funktion ist so einzurichten, dass sie frei von Einflüssen ist, die eine objektive, faire und unabhängige Aufgabenerfüllung beeinträchtigen können.[64]

  Zu den notwendigen Kompetenzen gehört insbesondere der Zugang zu Informationen und Mitarbeitern. Ferner muss der Compliance-Funktion das Recht auf Durchführung von Untersuchungen möglicher Compliance-Verstöße eingeräumt sein; in

61 Vgl. Erwägungsgrund 31 der Solva II-RL.
62 Vgl. BaFin-MaGo, Rn. 13, die sich auf Ausführungen zum „Wie" beschränken.
63 Vgl. hierzu Art. 268 Solva II-VO.
64 Art. 268 Abs. 1 Satz 1 Solva II-VO und hierzu BaFin-MaGo, Rn. 78.

schwerwiegenden Fällen auch unter Hinzuziehung von internen oder externen Sachverständigen. Essenziell ist schließlich im Rahmen der dafür vorgesehenen Berichtslinien der uneingeschränkte Zugang zur Geschäftsleitung bzw. zum Aufsichtsgremium.

- **Gruppendimensionale Ausgestaltung**

  Bei der Ausgestaltung der Compliance-Funktion in Unternehmensgruppen sind die Anforderungen in Art. 246 Solva II-RL sowie die nationale Umsetzung in § 275 Abs. 1 VAG zu berücksichtigen. Danach muss die Compliance-Funktion (wie auch die übrigen Schlüsselfunktionen) auf Gruppenebene eingerichtet und entsprechend gemeinsamer Mindeststandards gruppenweit gesteuert werden.[65]

II. Zentrale oder dezentrale Organisation

1. Organisationsfreiheit[66]

Die Compliance-Funktion setzt keine eigenständige Compliance-Abteilung voraus. Dennoch ist es den Unternehmen möglich, ihr Governance-System so auszugestalten, dass Compliance-Funktion und Compliance-Abteilung identisch sind. 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 Bestellung eines Verantwortlichen für die Compliance-Funktion (verantwortlicher Schlüsselfunktionsinhaber) durch die Geschäftsleitung erforderlich.

2. Dezentrale Organisation mit Compliance-Beauftragten

Bei dieser Organisationsstruktur sind die mit einzelnen Compliance-Aufgaben und Verantwortlichkeiten beauftragten Mitarbeiter den verschiedenen Bereichen zugeordnet (z. B. Compliance-Beauftragte). Welche Stellen im Unternehmen die Compliance-Funktion wahrnehmen, ist in der Compliance-Leitlinie zu definieren. Jedoch muss auch bei diesem Ansatz ein zentral verantwortlicher Schlüsselfunktionsinhaber benannt sein. Dieser ist regelmäßig bzw. ad hoc über die Tätigkeit der Compliance-Beauftragten zu informieren.[67]

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 verantwortlichen Schlüsselfunktionsinhaber in der Regel nicht disziplinarisch, aber fachlich unterstellt, sondern nehmen ihre Com-

65 Siehe hierzu näher unter D. VII.
66 Organisationsfragen und deren praktische Behandlung behandelt EIOPA, Peer review of key functions: superviso-ry practices and application in assessing key functions, 2018.
67 Vgl. zu den Berichtswegen unten D. VI.

pliance-Aufgabe im Rahmen ihres jeweiligen Ressorts wahr und berichten dort anfallende Compliance-Themen auch an die jeweils zuständigen Vorstandsmitglieder. Eine zusätzliche Berichtslinie an den verantwortlichen Schlüsselfunktionsinhaber – insbesondere zu aktuellen Compliance-Fällen – ist jedoch erforderlich.

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 verantwortlichen Schlüsselfunktionsinhabers 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.

Zu gruppenweiten Organisation siehe auch unter D. VII.

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 Verband ein Diskussionspapier mit detaillierten Hinweisen veröffentlicht.[68]

Gegebenenfalls kann die Überlegung sinnvoll sein, 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.

Nach den europäischen Vorgaben soll es in kleinen und weniger komplexen Unternehmen möglich sein, mehr als eine Funktion auf eine Person oder Organisationseinheit zu vereinen.[69] 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.[70] Dies kann auch durch flankierende Maßnahmen (die sich unternehmensindividuell wieder am Risikoprofil und Proportionalitätsgrundsatz zu orientieren haben) ausgestaltet

68 GDV-Diskussionspapier „Governance-Funktionen unter Solvency II: Kernaufgaben und Schnittstellen".
69 Erwägungsgrund 32 der Solva II-RL.
70 Art. 268 Abs. 1 Solva II-VO.

werden. 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. Eine Kombination mit der internen Revisionsfunktion ist nur ausnahmsweise unter den engen Voraussetzungen des Art. 271 Abs. 2 Solva II-VO zulässig.

Hingegen ist nach Ansicht der BaFin eine Zuweisung der Verantwortung für eine Schlüsselfunktion an mehrere Personen generell unzulässig.[71]

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

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

  Die Überschneidung der Aufgaben der Compliance-Funktion mit der Rechtsabteilung ist naturgemäß hoch, da es im Kern um die Sicherstellung rechtmäßigen Verhaltens geht. Im Vergleich zur klassischen Aufgabenstellung einer Rechtsabteilung gibt es jedoch Unterschiede. Hervorzuheben ist die systematisch präventive und überwachende Funktion von Compliance. Diese bedingt eine entsprechende Ausrichtung und eine engere operative Einbindung der mit Compliance-Aufgaben betrauten Mitarbeiter. Die Rechtsabteilung ist keine der zwingend durch Solva II vorgesehenen Schlüsselfunktionen, kann aber unternehmensindividuell als „andere Schlüsselaufgabe" definiert werden. 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.

  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 D. I.). Ferner muss die Verantwortung für die Erfüllung dieser Aufgaben eindeutig geklärt sein. Sofern der verantwortliche 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.

- **Verhältnis der Compliance-Funktion zu Unternehmensbeauftragten**

  Für bestimmte Tätigkeitsbereiche sind spezielle Unternehmensbeauftragte gesetzlich vorgeschrieben. Hierzu zählen insbesondere Geldwäsche- und Datenschutzbeauftragte (dazu näher sogleich).

71 BaFin-MaGo, Rn. 81.

Die Unternehmen haben einen weiten Gestaltungsspielraum, wie sie das Verhältnis der Compliance-Funktion zu Unternehmensbeauftragten ausgestalten. Unternehmensbeauftragte können z. B. in die Compliance-Funktion eingegliedert werden, soweit deren spezifischen Aufgaben und Vorgaben dem nicht entgegenstehen.

Unternehmensbeauftragte können daneben auch unabhängig von der Compliance-Funktion organisiert sein. Die insoweit betroffenen Rechtsbereiche sind dann ggf. auch Gegenstand der Aufgaben der Compliance-Funktion (Überwachung, Beratung, Risikokontrolle und Frühwarnung). Die BaFin führt insoweit in Rn. 89 MaGo aus, dass auch solche Rechtsbereiche, für die Unternehmensbeauftragte vorgesehen sind, nicht vollständig aus dem Aufgabenbereich der Compliance-Funktion fallen. Bei Rechtsbereichen, die mit wesentlichen Risiken verbunden sind, habe die Compliance-Funktion mindestens zu überwachen, ob die Unternehmensbeauftragten ihre gesetzlich vorgeschriebenen Aufgaben wahrnehmen.

Auch wenn Unternehmensbeauftragte unabhängig von der Compliance-Funktion agieren, besteht ein weiter Spielraum, Gegenstand und Intensität der Aufgabenwahrnehmung der Compliance-Funktion gegenüber den Unternehmensbeauftragten und den diesen zukommenden Rechtsbereichen festzulegen. Eine vollständige Doppelung ist weder erforderlich noch sachgerecht. Kriterien für die Identifizierung wesentlicher Rechtsbereiche, die auch Gegenstand der Compliance-Funktion sind, dürften die Wesentlichkeit, Risikoorientierung und Verhältnismäßigkeit/Proportionalität sein. Es sollte festgelegt werden, inwieweit eine Überwachung stattfindet und welche Berichtspflichten der Unternehmensbeauftragten gegenüber der Compliance-Funktion (Gegenstand, Turnus, ggf. ad hoc-Berichtspflichten) bestehen. Es bietet sich auch ein Austausch oder Zusammenarbeit über Methoden, Techniken, Vorgehensweisen u. ä. an.

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

  Der Geldwäschebeauftragte ist ein durch das Geldwäschegesetz (GwG) vorgeschriebener Unternehmensbeauftragter, der auf „Führungsebene“[72] zu bestellen ist. Seine gesetzlich zugewiesenen Befugnisse sollen dem Allgemeinwohlinteresse dienen. Er ist unmittelbar dem Vorstand nachgeordnet (vgl. § 7 Abs. 1 Satz 3 GwG), dem er unmittelbar zu berichten hat (§ 7 Abs. 5 Satz 4 GwG).[73]

  Die originäre Aufgabe des Geldwäschebeauftragten, die Einhaltung der GwG-Vorschriften sicherzustellen, ist grundsätzlich mit der Stellung als Compliance-Beauftragtem vereinbar und kann mit der Compliance-Funktion verbunden werden.[74] Auch hier ist aber sicherzustellen, dass es nicht zu Interessenkonflikten kommt. Diese könnten sich beispielhaft ergeben, wenn die Geldwäscheorganisation vom Complian-

72 Vgl. zum Begriff § 1 Abs. 15 GwG.
73 Näher zu den Erwartungen der BaFin an die Stellung und Berichtspflichten des Geldwäschebeauftragten BaFin, Auslegungs- und Anwendungshinweise zum Geldwäschegesetz, Mai 2020 (AuA-AT), 3.2 (S. 16 ff.); für Versicherungsunternehmen hinsichtlich Berichtspflichten an das Kontrollgremium (Aufsichtsrat) spezieller zudem AuA für Versicherungsunternehmen (AuA-BT/VU), II.3 (S. 7).
74 Vgl. näher BaFin-AuA-AT, 3.2 (S. 19).

ce-Beauftragten überwacht 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 Art. 38 DSGVO 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; grob gesagt, benötigt die Compliance möglichst viele Daten, während der Datenschutz hier einen sparsamen Umgang fordert. 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 Interessenkonflikte 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.

- **Einrichtung einer Vertriebsfunktion**

  Gem. § 48 Abs. 1 und 2 VAG müssen Versicherungsunternehmen sicherstellen, dass Versicherungsvermittler und Angestellte des Versicherungsunternehmens bestimmte Anforderungen an den Versicherungsvertrieb im Hinblick auf die Qualifikation erfüllen. Zu diesem Zweck ist eine Funktion einzurichten, § 48 Abs. 2a Satz 2 VAG. Aus Sicht des Verbandes lässt die Regelung Raum im Rahmen der Organisationsfreiheit, die Funktion im operativen Vertrieb zu verorten oder die Compliance-Funktion mit dieser Aufgabe zu betrauen.[75]

- **Informationssicherheitsbeauftragter**

Die BaFin erwartet die Einrichtung der Funktion des Informationssicherheitsbeauftragten.[76] Die Erwartung geht über die zwingenden Anforderungen der

75 Siehe zur Rolle der Compliance auch EIOPA, EIOPA's approach to the supervision of product oversight and governance (08.10.2020), abrufbar unter *https://www.eiopa.europa.eu/content/eiopa-approach-supervision-product-oversight-and-governance_en* (zuletzt abgerufen: Februar 2021).

76 BaFin, Rundschreiben 10/2018 zu Versicherungsaufsichtsrechtlichen Anforderungen an die IT (VAIT), Rn. 28.

Solva II-RL, der Solva II-VO und des VAG hinaus. Sofern eine solche Funktion eingerichtet wird, kann sie nach Auffassung der BaFin mit der Compliance-Funktion gekoppelt werden.[77] Eine etwaige Kopplung wirft verschiedene Folgefragen, etwa hinsichtlich erforderlicher Kompetenzen, Qualifikation und Berichtspflichten auf.

IV. Outsourcing der Compliance-Funktion

1. Rechtliche Vorgaben

Ein Outsourcing (Ausgliederung) liegt vor, wenn die Compliance-Funktion durch einen externen Dienstleister (auch gruppenintern) übernommen wird.[78] Als Schlüsselfunktion handelt es sich bei der Compliance-Funktion um eine wichtige und kritische Funktion,[79] sodass für ihre Ausgliederung die strengeren Anforderungen gem. **§ 32 Abs. 3 VAG** bzw. **Art. 274 Abs. 5 Solva II-VO** gelten: Dies betrifft insbesondere die Auswahl des Dienstleisters sowie die Gestaltung der vertraglichen Beziehungen. Für den Inhalt des Ausgliederungsvertrags selbst macht Art. 274 Abs. 4 Solva II-VO konkrete Vorgaben. Nach Art. 41 Abs. 3 Solva II-RL sowie Art. 274 Abs. 1 Solva II-VO haben die Unternehmen zudem **schriftliche Leitlinien zur Ausgliederung** zu erstellen und mindestens jährlich zu überprüfen. Bereits im Rahmen der schriftlichen Leitlinien zum Outsourcing ist daher auszuführen, welche unternehmensinternen Kontrollprozesse vorgesehen sind, um die ordnungsgemäße Leistungserbringung durch den Dienstleister sicherzustellen. So ist auch sicherzustellen, dass das Risikomanagement und das interne Kontrollsystem des Dienstleisters in der Lage sind, eine ordnungsgemäße Leistungserbringung zu gewährleisten.[80] Weiter muss eine angemessene Einbindung in das eigene Risikomanagementsystem und das interne Kontrollsystem im Unternehmen erfolgen. Erforderlich ist zudem, dass der Dienstleister über angemessene finanzielle Ressourcen[81] und Notfallpläne[82] verfügt.

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 Versicherungsunternehmen 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.

Ausgliedernde Versicherungsunternehmen bleiben gem. § 32 Abs. 1 VAG für die Einhaltung der aufsichtsrechtlichen Vorgaben bei dem Dienstleister verantwortlich.[83]

---

77 Vgl. BaFin, VAIT Rn. 2, wonach eine Kopplung mit anderen Funktionen im Unternehmen möglich ist, wenn dies dem Risikoprofil entspricht.
78 Zur Definition vgl. Art. 13 Nr. 28 Solva II-RL; § 7 Nr. 2 VAG.
79 Erwägungsgrund 33 Solva II-RL.
80 Art. 274 Abs. 5 Solva II-VO.
81 Art. 274 Abs. 5 lit. c) Solva II-VO.
82 Art. 274 Abs. 5 lit. d) Solva II-VO.
83 Art. 49 Abs. 1 Solvency II-Richtline.

Art. 49 Abs. 3 Solva II-RL sieht vor, dass die Unternehmen das Outsourcing kritischer oder wichtiger Funktionen oder Tätigkeiten und wesentliche Änderungen anzeigen. Auch sieht Leitlinie 14, Ziffer 1.47 der EIOPA-Leitlinien zum Governance-System vor, dass eine Person in dem Versicherungsunternehmen benannt werden muss, welche die Gesamtverantwortung für die ausgegliederte Schlüsselfunktion trägt.

2. Aufsichtsbehördliche Erwartungen

Die BaFin verlangt, dass Versicherungsunternehmen beim Outsourcing von Schlüsselfunktionen einen Ausgliederungsbeauftragten benennen, der die operative Verantwortung für eine ordnungsgemäße Durchführung der ausgegliederten Aufgabe trägt.[84] Dafür gibt es keine Rechtsgrundlage in den Vorgaben der Solva II-RL, der Solva II-VO oder im VAG.

EIOPA hat die aufsichtsrechtlichen Anforderungen an das Outsourcing in ihren **Leitlinien zum Governance-System** näher erläutert.[85] Auch hier sind besondere Anforderungen für **kritische oder wichtige operative Funktionen oder Tätigkeiten** vorgesehen.

3. Gruppeninternes Outsourcing

Bei der Auslagerung auf ein gruppenangehöriges Unternehmen sind gem. Art. 274 Abs. 2 Solva II-VO grundsätzlich dieselben Anforderungen zu erfüllen wie bei dem Outsourcing auf einen externen Dienstleister. Nach den EIOPA-Leitlinien zum Governance-System soll das zuständige Unternehmen – sofern Schlüsselfunktionen innerhalb der Gruppe ausgelagert werden – dokumentieren, welche 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.[86] Danach müssen die Zuständigkeiten/Verantwortlichkeiten innerhalb des VU klar geregelt werden.

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

1. Betroffener Personenkreis

Personen, die ein Versicherungsunternehmen tatsächlich leiten oder andere Schlüsselaufgaben wahrnehmen, müssen gem. § 24 Abs. 1 Satz 1 VAG zuverlässig und fachlich geeignet sein.[87] Art. 42 Abs. 1 Solva II-RL stellt allerdings nicht auf Personen ab, die Schlüsselaufgaben wahrnehmen, sondern enger auf solche, die Schlüsselaufgaben innehaben. Die Compliance-Funktion ist als Schlüsselaufgabe nach Solva II von den Qualifikations- und Zuverlässigkeitsanforderungen erfasst.

---

84 BaFin-MaGo Rn. 267; BaFin, VAG-Merkblatt Verantwortliche Personen für Schlüsselfunktionen (v. 06.12.2018), I.2.b) (S. 6).
85 EIOPA, Leitlinien zum Governance-System, Leitlinien 14, 60–64.
86 EIOPA-Leitlinien zum Governance-System, Leitlinie 62 Ziff. 1.115.
87 Vgl. Art. 42 Solva II-RL.

Nach Ansicht des Verbandes gelten die besonderen Anforderungen nur für den Leiter bzw. verantwortlichen Inhaber der Schlüsselfunktion. Erfasst sein dürften darüber hinaus auch Stellvertreter, sofern diese vom Unternehmen freiwillig dauerhaft benannt und mit entsprechenden Rechten und Pflichten ausgestattet sind.[88]

Für weitere Personen gelten innerhalb der Compliance-Funktion (nur) die allgemeinen Anforderungen im Sinne von Art. 258 Abs. 1 lit. e) Solva II-VO, sodass sie über Fähigkeiten, Kenntnisse und Fachkunde verfügen müssen, die zur ordnungsgemäßen Erfüllung der ihnen übertragenen Aufgaben erforderlich sind. Insoweit führt auch die BaFin aus, dass sich die Anforderungen an die fachliche Qualifikation nach den jeweiligen Verantwortlichkeiten, Tätigkeiten und Zuständigkeiten der Person richten.[89]

Weitergehend fordert die BaFin, dass auch die für Schlüsselfunktionen tätigen Personen *zuverlässig* sind.[90]

2. Qualifikationsanforderungen gem. Art. 42 Solva II-RL („Fit")

Die Bewertung der erforderlichen Qualifikationen für Personen, die Schlüsselfunktionen innehaben, erfolgt nach Art. 273 Abs. 2 Solva II-VO hinsichtlich der drei Kriterien Berufsqualifikation, Kenntnisse und Erfahrungen im Versicherungssektor, anderen Finanzsektoren oder anderen Unternehmen. Bei Festlegung der Qualifikationsanforderungen sind die Pflichten der jeweiligen Person zu berücksichtigen.[91]

Konkrete Vorgaben an die Qualifikation des verantwortlichen Inhabers der Compliance-Funktion sind weder in der Solva II-RL, der Solva II-VO noch dem VAG enthalten. Eine Wahrnehmung der Funktion durch Juristen liegt aufgrund der Rechtsbezogenheit der Aufgaben nahe, ist aber keine rechtliche Voraussetzung.[92] Entscheidend ist die Beurteilung der fachlichen Qualifikation im konkreten Einzelfall, die auch außerhalb eines volljuristischen Studiengangs, etwa im Rahmen spezieller Compliance-Studiengänge oder beruflicher Erfahrung erworben werden könnte.

3. Zuverlässigkeitsanforderungen gem. Art. 42 Solva II-RL („Proper")

Nach Art. 273 Abs. 4 Solva II-VO soll die persönliche Zuverlässigkeit eines Mitarbeiters anhand seiner persönlichen Redlichkeit und finanziellen Zuverlässigkeit bewertet werden. Dabei sind strafrechtliche, finanzielle und aufsichtsrechtliche Aspekte zu berücksichtigen.

---

88 Vgl. auch BaFin, VAG-Merkblatt Verantwortliche Personen für Schlüsselfunktionen (v. 06.12.2018), unter II.1 b) (S. 14).
89 BaFin, VAG-Merkblatt Verantwortliche Personen für Schlüsselfunktionen (v. 06.12.2018), unter II.1 b) (S. 14).
90 BaFin, VAG-Merkblatt Verantwortliche Personen für Schlüsselfunktionen (v. 06.12.2018), unter II.2.b) (S. 15).
91 Art. 273 Abs. 2 Solva II-VO.
92 Strikter allerdings *Bürkle*, Compliance in Versicherungsunternehmen, 3. Aufl. 2020, § 2 Rn. 219 f; Prölss/Dreher/*Dreher*, VAG, 13. Aufl. 2018, § 24 Rn. 71; Kaulbach/Bähr/Pohlmann/*Pohlmann*, VAG, 6. Aufl. 2019, § 24 Rn. 73, § 29 Rn. 44.

Nach Ansicht der BaFin findet der Proportionalitätsgrundsatz hier keine Anwendung.[93] Eines positiven Nachweises der Zuverlässigkeit bedarf es nicht. Die BaFin unterstellt die Zuverlässigkeit, wenn keine Tatsachen erkennbar sind, die die Unzuverlässigkeit begründen.[94]

4. Anzeigepflicht

Gem. Art. 42 Abs. 2 und Abs. 3 Solva II-RL haben Versicherungsunternehmen der Aufsichtsbehörde zu melden, wenn es relevante Änderungen bei von den Qualifikations- und Zuverlässigkeitsvorgaben betroffenen Personen gibt.

Gem. § 47 Nr. 1 VAG ist (über die Solva II-RL hinausgehend) bereits die „vorgesehene Bestellung" der Personen, die für Schlüsselaufgaben verantwortlich sind, der Aufsichtsbehörde unverzüglich anzuzeigen. Für weitere Personen, die für die Schlüsselfunktion tätig sind, besteht keine Anzeigepflicht.[95]

Die BaFin erwartet, dass der Absichtsanzeige bestimmte Unterlagen, wie Lebenslauf, eine „persönliche Erklärung mit Angaben zur Zuverlässigkeit", ein Führungszeugnis und ein Auszug aus dem Gewerbezentralregister beigefügt werden.[96]

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**[97]

  Die Compliance-Funktion muss nach Art. 268 Solva II-VO regelmäßig und – wenn ein Anlass gegeben ist – auch ad hoc an den Vorstand berichten.[98] 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.[99] Die Aufsichtsbehörde hat ihre Erwartungen in der MaGo konkretisiert.[100]

  Es ist in jedem Fall sicherzustellen, dass der Vorstand die notwendigen Mindestinformationen hat, um seine Pflichten wahrzunehmen.[101] In welcher Periodik die Be-

---

93 BaFin, VAG-Merkblatt Verantwortliche Personen für Schlüsselfunktionen (v. 06.12.2018), unter Nr. II. (S. 13).
94 BaFin, VAG-Merkblatt Verantwortliche Personen für Schlüsselfunktionen (v. 06.12.2018), unter Nr. II.2 (S. 14).
95 BaFin, VAG-Merkblatt Verantwortliche Personen für Schlüsselfunktionen (v. 06.12.2018), unter Nr. I.2 (S. 6).
96 Vgl. im Einzelnen BaFin, VAG-Merkblatt Verantwortliche Personen für Schlüsselfunktionen (v. 06.12.2018), unter Nr. I.2 (S. 6).
97 Vorstand steht hier stellvertretend für die Geschäftsleitung.
98 Vgl. Art. 268 Abs. 1 S. 2 und Abs. 3 Solva II-VO.
99 Vgl. hierzu oben B.
100 Vgl. BaFin-MaGo Rn. 95 und 84.
101 Vgl. oben B. I.2.

richterstattung 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.[102]

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 wesentlichen Compliance-Risiken und der durchgeführten bzw. durchzuführenden Maßnahmen zur Risikoreduzierung (Stichproben, Reviews, ggf. Monitoring-Systeme);[103]
- 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;[104]
- Ergebnis der Bewertung der Angemessenheit der Vorkehrungen zur Verhinderung von Rechtsverstößen;
- der Vorstand sollte zudem über Entwicklungen und allgemeine Trends des Rechtsumfeldes informiert werden,[105] damit dieser entsprechende Vorkehrungen und Maßnahmen einleiten kann.

Darüber hinaus hat der Compliance-Verantwortliche dem Vorstand erhebliche Feststellungen unverzüglich mittels eines anlassbezogenen **Ad-hoc-Berichts** mitzuteilen.[106] 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-Funktion anlässlich jeder Berichterstattung, ob eine Berichterstattung auch an die übergeordnete Compliance-Funktion innerhalb des Unternehmensverbunds erforderlich ist.

- **Aufsichtsrat**

  Konkrete rechtliche Vorgaben zur Kommunikation zwischen dem Inhaber der Compliance-Funktion und dem Aufsichtsrat bestehen nicht. Der Aufsichtsrat hat sich im Rahmen seiner Überwachungspflicht allerdings auch mit relevanten Compliance-Sachverhalten zu befassen und entsprechende Informationen einzuholen. Unternehmensindividuell sollte eine Regelung der Kommunikation zwischen dem Compliance-Beauftragten und dem Aufsichtsrat getroffen werden. Es ist festzulegen, in welchen

102 So auch BaFin-MaGo Rn. 95.
103 Vgl. auch BaFin-MaGo Rn. 96.
104 Vgl. dazu auch BaFin-MaGo, Rn. 63.
105 Vgl. oben C. II.1. a.
106 Art. 268 Abs. 3 Solva II-VO.

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.[107]

Sofern der Aufsichtsrat einen Prüfungsausschuss eingerichtet hat,[108] wird in dessen Sitzungen regelmäßig auch über Compliance-relevante Sachverhalte berichtet. Auch ein Recht des Compliance-Beauftragten, sich im Eskalationsfall unmittelbar an den Aufsichtsrat zu wenden, sollte geregelt werden.

- **Behörden**

  Es besteht keine allgemeine rechtliche Pflicht, Compliance-Verdachtsfälle oder -Verstöße außerhalb des Unternehmens mitzuteilen oder zur Anzeige zu bringen.[109]

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 Unternehmensbeauftragte**

  Sind Compliance-Beauftragte in einzelnen Unternehmensteilen installiert, sollten diese auf regelmäßiger Basis über ihre Aktivitäten und Feststellungen an den verantwortlichen 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 unterstützen. Auch bei besonderen Unternehmensbeauftragten, wie etwa dem Geldwäsche- oder dem Datenschutzbeauftragten, bietet es sich an, entsprechend vorzugehen.

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

  - Einschätzung der Wirksamkeit implementierter Präventionsmaßnahmen;
  - behördliche Verfahren (zu Compliance-relevanten Themen, insbesondere Anfragen, Prüfungen und Untersuchungen von Aufsichts- und Strafverfolgungsbehörden);
  - schwerwiegende Verstöße gegen Gesetze und andere Rechtsvorschriften sowie gegen interne Vorschriften (wie z. B. Verhaltenskodizes, Compliance-Richtlinien) einschließlich Verdachtsfälle;
  - die Unternehmen können individuell weitere Themen für die Berichterstattung vorsehen.

---

107 Vgl. den Grundsatz 15 des Deutschen Corporate Governance Kodex (zur Geltung des DCGK s. Fn. 24).
108 Vgl. hierzu die Empfehlung unter Ziffer D. 3 des Deutschen Corporate Governance Kodex (zur Geltung des DCGK s. Fn. 24).
109 Eine Ausnahme ist § 138 StGB. Danach ist die Nichtanzeige bestimmter geplanter Straftaten strafbar.

- **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 möglicherweise Compliance-relevanten Berichtsausschnitte der Internen Revision erhalten, die für ihre Aufgabenerfüllung notwendig sind, die Risikokontrollfunktion sollte alle Informationen an die Compliance-Funktion weiterleiten, die Compliance-Risiken betreffen. Ebenso sollte festgelegt werden, in welchen Fällen die Compliance-Funktion Informationen an die anderen Schlüsselfunktionen geben sollte.

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

  Zusätzlich müssen den Mitarbeitern Möglichkeiten eingeräumt werden, Verstöße freiwillig unter Wahrung der Vertraulichkeit ihrer Identität zu melden. Es muss sichergestellt sein, dass derartige Meldungen auch die vorgesehene Stelle in der Compliance-Funktion[110] erreichen.

  Unternehmensindividuell muss entschieden werden, ob in diesem Zusammenhang auch allen Mitarbeitern die Pflicht zur Meldung bestimmter, schwerer Verstöße auferlegt wird.[111]

- **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.

VII. Gruppen-Compliance

Die versicherungsaufsichtsrechtliche Anforderung einer übergreifenden Compliance-Organisation auf Gruppenebene (Art. 246 Abs. 1 Solva II-RL, § 275 Abs. 1 S. 2 VAG)[112] führt zu Herausforderungen in der praktischen Umsetzung. Zwar wird verbreitet (auch

---

110 Die Hinweisgeberstelle muss nicht zwingend auf Ebene der Compliance-Funktion angesiedelt sein. Demgemäß sind bei anderer organisatorischer Ausgestaltung andere Berichtswege zu beachten.

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

112 Siehe dazu schon oben D. I. Die BaFin greift dies in Rn. 80 der MaGo auf. Danach hat das für die Erfüllung der Governance-Anforderungen auf Gruppenebene zuständige Unternehmen für die zusätzliche Einrichtung der Schlüsselfunktionen auf Gruppenebene Sorge zu tragen.

über das Versicherungsaufsichtsrecht hinaus) im Rahmen der Legalitätspflicht eine konzernweite Compliance-Verantwortung der Muttergesellschaft angenommen. Ein Spannungsverhältnis kann gleichwohl zu gesellschafts- bzw. konzernrechtlichen Vorgaben bestehen.[113]

Eine eigene aufsichtsrechtliche Kompetenz für gruppenweite Maßnahmen des übergeordneten Unternehmens besteht nicht. Die aufsichtsrechtlichen Anforderungen sind daher im Rahmen des gesellschaftsrechtlich Möglichen umzusetzen. Die BaFin führt insoweit aus, dass „das für die Erfüllung dieser Anforderungen zuständige Unternehmen und die gruppenzugehörigen Unternehmen [...] angemessene Maßnahmen ergreifen [müssen], um die Erfüllung der Anforderungen sicherzustellen. Zu diesem Zweck hat das für die Erfüllung der Anforderungen auf Gruppenebene zuständige Unternehmen die vorhandenen Einwirkungsmöglichkeiten angemessen zu nutzen. Alle der Gruppenaufsicht unterworfenen Unternehmen haben bei der Erfüllung der Governance-Anforderungen auf Gruppenebene mitzuwirken (§ 246 Abs. 3 VAG)."[114]

Abhängig von der Art der Konzernierung im Einzelfall dürften verschiedene Mittel für die Gestaltung der Gruppen-Compliance in Betracht kommen.[115] Bei Vertragskonzernen bestehen weitgehende Weisungsrechte des herrschenden Unternehmens (§ 308 AktG), die eine Einwirkung auf die Ausgestaltung der Compliance in untergeordneten Unternehmen ermöglichen. Im faktischen Konzern mag die tatsächliche Einflussmöglichkeit über die Personalhoheit des übergeordneten Unternehmens ausreichend sein, um eine übergreifende Compliance zu ermöglichen.[116] Im Übrigen kommen Vereinbarungen zwischen den gruppenangehörigen Unternehmen in Betracht, die eine Mitwirkung bei gruppenbezogenen Compliance-Maßnahmen tatsächlich sicherstellen.

Zur Ermöglichung einer gruppenweiten Compliance sollte sich die Compliance-Organisation in den gruppenangehörigen Unternehmen an einheitlichen Kriterien ausrichten.[117] Gleichwohl kann es erforderlich oder sinnvoll sein, hinsichtlich der Intensität der Einbindung von Einzelgesellschaften und hinsichtlich den jeweiligen Compliance-Anforderungen zu differenzieren. Differenzierungskriterien können z. B. die Art der Gesellschaft (Versicherungsunternehmen oder Gesellschaften anderer Branchen ohne oder mit abweichenden aufsichtsrechtlichen Vorgaben), Risikoträgereigenschaften, abweichende gesetzliche Compliance-Vorgaben (z. B. abweichende Vorgaben des KWG; abweichende Vorgaben in Drittstaaten) sowie ggf. unterschiedliche Reputationsrisken sein.[118]

Die Unternehmen haben entsprechend ihrer Compliance-Gestaltung festzulegen, wie und welche Berichtswege aus den einzelnen Unternehmen gruppenweit auszugestalten sind. Bei Mischformen von zentralen/dezentralen Organisationen mit einer eigenstän-

---

113 Vgl. BaFin-MaGo Rn. 23; Prölss/Dreher/*Krämer*, VAG, 13. Aufl. 2018, § 275 Rn. 6 ff.; *Hemeling*/Lange, VersR 2014, 1238.
114 BaFin-MaGo Rn. 23.
115 Vgl. ausführlich zur Compliance in Versicherungsgruppen und -konzernen *Kruchen*, in Bürkle, Compliance in Versicherungsunternehmen, 3. Aufl. 2020, § 3.
116 Kaulbach/Bähr/Pohlmann/*Lemmer*, VAG, 6. Aufl. 2019, § 275 Rn. 7.
117 Kaulbach/Bähr/Pohlmann/*Lemmer*, VAG, 6. Aufl. 2019, § 275 Rn. 4.
118 Vgl. dazu Prölss/Dreher/*Krämer*, VAG, 13. Aufl. 2018, § 275 Rn. 12.

digen Compliance-Abteilung in der Muttergesellschaft und einer dezentralen Struktur auf der Tochterebene ist 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.

E. Haftung von Unternehmen, Organen und Compliance-Beauftragten

Compliance-Verstöße können – neben einer persönlichen Verantwortung und Haftung der handelnden Mitarbeiter – zu einer Haftung des Unternehmens, der Organe und ggf. des Compliance-Beauftragten führen. Eine wirksame Compliance trägt dazu bei, Rechtsverstöße zu verhindern und eine Haftung damit von vornherein auszuschließen. Sollten trotz einer wirksamen Compliance Rechtsverstöße aus dem Unternehmen vorliegen, können die getroffenen Maßnahmen den Schaden- und Haftungsumfang beschränken.[119]

Rechtsverstöße können ggf. **zivilrechtliche Ansprüche** wie Schadenersatz- oder bereicherungsrechtliche Ansprüche auslösen.

Ordnungswidrigkeitenrechtlich können gegen **Leitungspersonen**, wie insbesondere **Vorstandsmitglieder**, Geldbußen verhängt werden, wenn sie schuldhaft die Aufsichtspflichten verletzt haben, die erforderlich sind, um unternehmensbezogene Straftaten oder Ordnungswidrigkeiten der Mitarbeiter zu verhindern (§§ 9 Abs. 1 Nr. 1, 130 OWiG). Dieser Haftung können auch die **Inhaber der Compliance-Funktion** im Rahmen der ihnen in eigener Verantwortung übertragenen Aufgaben unterliegen (§§ 9 Abs. 2 Nr. 2, 130 OWiG).[120]

Auch gegen **das Unternehmen** kann ordnungswidrigkeitenrechtlich anknüpfend an eine Aufsichtspflichtverletzung von Leitungspersonen eine Geldbuße verhängt werden, wenn durch die Straftaten oder Ordnungswidrigkeiten Pflichten des Unternehmens verletzt worden sind oder eine Bereicherung des Unternehmens erreicht wurde oder werden sollte (§ 30 OWiG).

Die Bundesregierung hat zudem den Entwurf eines Verbandssanktionengesetzes eingebracht, das eine erhebliche Ausweitung der Haftung von Unternehmen für unternehmensbezogene Straftaten vorsieht.[121] Anstelle des Opportunitätsprinzips des OWiG ist eine Verfolgungspflicht (Legalitätspflicht) vorgesehen. Der Entwurf hebt die Bedeutung von Compliance-Maßnahmen hervor und berücksichtigt diese bei einer Sanktionierung. Bewusst sind keine Vorgaben an die Ausgestaltung der Compliance vorgesehen.

Aufsichtsrechtlich kann zudem die BaFin im Rahmen der Missstandsaufsicht gem. § 298 Abs. 1 S. 1 VAG Maßnahmen zur Beseitigung eines Missstandes ergreifen.[122] Auch die Einsetzung eines Sonderbeauftragten durch die Aufsicht kommt in Betracht (§ 307 Abs. 1 VAG). Zudem kann unter Umständen eine Abberufung eines Geschäftsleiters oder des Inhabers der Compliance-Funktion verlangt werden (§ 303 Abs. 2 Nr. 1 VAG).

---

119 Zur bußgeldmindernden Wirkung eines Compliance-Management-Systems s. BGH, Urteil v. 09.05.2017, 1 StR 265/16; s. zudem den Entwurf eines Gesetzes zur Stärkung der Integrität in der Wirtschaft, Bundestags-Drucks. 19/23568, mit dem Verbandssanktionengesetz als Kern, das die Berücksichtigung von Compliance-Maßnahmen bei einer Sanktionierung vorsieht (§ 15 Abs. 3 Nr. 6 und 7).

120 BeckOK VAG/*Michael/Kübler*, 10. Ed. 01.09.2020, VAG § 29 Rn. 68; zur strafrechtlichen Garantenpflicht von Compliance-Officern, „im Zusammenhang mit der Tätigkeit des Unternehmens stehende Straftaten von Unternehmensangehörigen zu verhindern", bei tatsächlicher Übernahme eines entsprechenden Pflichtenkreises siehe (obiter dictum) BGH, Urteil vom 17.07.2009 – 5 StR 394/08, Rn. 27.

121 Gesetzentwurf eines Gesetzes zur Stärkung der Integrität in der Wirtschaft, Bundestags-Drucks. 19/23568.

122 Restriktiv hinsichtlich der Voraussetzungen VGH Kassel, Urteil v. 30.04.2020 – 6 A 2158/18, VersR 2020, 819, nicht rechtskräftig.

F. Ausblick

Auch der umfassend überarbeitete und aktualisierte Leitfaden stellt insbesondere hinsichtlich der Beschreibung des relevanten Rechtsumfelds nur eine Momentaufnahme dar. Bereits heute zeichnen sich auf nationaler und europäischer Ebene regulatorische Entwicklungen ab, die neue Herausforderungen für die Compliance mit sich bringen werden.

National lenkt der Gesetzentwurf zur Stärkung der Integrität in der Wirtschaft[123] den branchenübergreifenden Blick auf die Effektivität von Compliance-Maßnahmen. Ob und ggf. wie sich der vom Gesetzgeber bezweckte Anreiz für Investitionen in Compliance-Maßnahmen auf die nach Solva II verpflichtend vorzuhaltende Compliance-Struktur in den Unternehmen auswirken wird, lässt sich zurzeit noch nicht abschließend beurteilen.

Zudem ruft der Skandal um die Insolvenz von Wirecard im Sommer 2020 den Gesetzgeber auf den Plan. Die Vorschläge des BMF und des BMJV sehen u. a. weitreichende Verschärfungen im Bilanzstraf- und -ordnungswidrigkeitenrecht sowie die Einrichtung eines angemessenen und wirksamen internen Kontrollsystems und eines entsprechenden Risikomanagementsystems für börsennotierte Aktiengesellschaften vor.[124]

Die Erkenntnisse aus der Aufklärung des Wirecard-Skandals werden sich möglicherweise auch auf die weitgehend bis zum 17. Dezember 2021 umzusetzende EU-Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden[125] auswirken. Die Bundesregierung hat ohne Verweis auf die anstehende Richtlinienumsetzung bereits eine Untersuchung angekündigt, wie Hinweise von Whistleblowern stärker genutzt werden können und wie die Anreize für Hinweisgeber verbessert werden können.

Auf europäischer Ebene wird die regulatorische Agenda vor allem durch die Themen Digitalisierung und Nachhaltigkeit bestimmt.

So werden **Environmental, Social und Governance (ESG)-Aspekte** in zunehmendem Maße auch Compliance-relevant. Zu nennen sind insbesondere die Transparenz-VO[126] und die Taxonomie-VO[127]. Weitere EU-rechtliche Vorgaben sind vorgesehen.[128] Eine Rolle spielt dies u. a. in der Kapitalanlage, der Vergütungspolitik, für Offenlegungs- und Berichtspflichten der Unternehmen sowie Beratungspflichten gegenüber Versicherungsnehmern. Verbunden sind damit wiederum (Non-)Compliance-Risiken, die von der Compliance-Organisation insbesondere im Rahmen der Überwachungs- und Beratungsaufgabe zu berücksichtigen sind.

---

123 Bundestags-Drucks. 19/23568.
124 Referentenentwurf eines Gesetzes zur Stärkung der Finanzmarktintegrität (Finanzmarktintegritätsstärkungsgesetz – FISG).
125 Richtlinie (EU) 2019/1937.
126 Verordnung (EU) 2019/2088 über nachhaltigkeitsbezogene Offenlegungspflichten im Finanzdienstleistungssektor. Betroffen sind Lebensversicherer, dagegen nicht Schaden- und Unfallversicherer.
127 Verordnung (EU) 2020/852 über die Einrichtung eines Rahmens zur Erleichterung nachhaltiger Investitionen und zur Änderung der Verordnung (EU) 2019/2088.
128 Vorschlag der EU-Kommission zur Änderung der Delegierten Verordnung im Hinblick auf Nachhaltigkeitsrisiken in der Geschäftsorganisation und im Vertrieb; EU-Kommission – Inception Impact Assessment on sustainable governance; EU-Kommission – Review of the Non-Financial Reporting Directive 2014/95/EU.

Ähnliche Fragestellungen werden sich auch im Zusammenhang mit der Regulierung der Digitalisierung ergeben. So hat die EU-Kommission unlängst einen Verordnungsentwurf zu digitaler operativer Resilienz im Finanzsektor zur Konsultation gestellt.[129] Dieser sieht umfassende Organisations-, Dokumentations-, Überwachungs- und Berichtsanforderungen vor, um Cyber-Angriffe und andere Risiken für die Informations- und Kommunikationstechnologie der Unternehmen einzudämmen.

Aus branchenspezifischer Sicht geht schließlich der Solvency II-Review im Jahr 2021 in seine entscheidende Phase. Auch hier ist mit zumindest mittelbaren Auswirkungen auf die Compliance-Funktion zu rechnen, etwa mit Blick auf die sich abzeichnende EIOPA-Empfehlung zur Schaffung eines konkreten Rechtsrahmens für die Geschäftsorganisation auf Gruppen-Ebene.[130]

Vor diesem Hintergrund bleibt auch weiterhin kontinuierlich zu beobachten, welche neuen Herausforderungen sich für die Compliance stellen und wie sie sich im Versicherungsunternehmen geeignet umsetzen lassen.

---

129 Proposal for a Regulation on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 („DORA").
130 EIOPA-Consultation Paper on the Opinion on the 2020 review of Solvency II.

G. Anhang

Verweis auf weitere GDV-Hilfestellungen

- GDV-Orientierungshilfe zur strafrechtlichen Beurteilung von Einladungen und Geschenken, 2. Aufl., August 2018;
- GDV-Diskussionspapier „Governance-Funktionen unter Solvency II: Kernaufgaben und Schnittstellenfragen“, April 2012.

Ansprechpartner

Karen Bartel
Leiterin Recht / Compliance / Verbraucherschutz
Tel. 030 / 20 20 – 52 60
E-Mail: k.bartel@gdv.de

Matthias Dzaack
Leiter Gruppe Aufsichts-, Gesellschaftsrecht und Compliance
Tel. 030 / 20 20 – 54 35
E-Mail: m.dzaack@gdv.de

Peter Glöckle
Recht / Compliance / Verbraucherschutz
Tel. 030 / 20 20 – 54 15
E-Mail: p.gloeckle@gdv.de

Aktualisierter Leitfaden für die Praxis

Compliance in Versicherungsunternehmen

Recht / Compliance / Verbraucherschutz
Ansprechpartner: Karen Bartel
E-Mail: k.bartel@gdv.de
Tel. 030/2020-5260
Fax: 030/2020-6260

Gesamtverband der Deutschen Versicherungswirtschaft e.V.

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

Tel. 030/2020-5000
Fax 030/2020-6000
berlin@gdv.de

www.gdv.de