76. Jahrgang 1. Juli 2025 E 5450

786207212513

VersR

Jetzt digitalen Zugang freischalten!
juris
www.juris.de/versr

Zeitschrift für Versicherungsrecht, Haftungs- und Schadensrecht

13

Aus dem Inhalt Seiten 777–840

Aufsätze

Winfried-Thomas Schneider — Unerkannt und doch relevant: Zur Rolle der Beratungsdokumentation im Versicherungsvertragsrecht **777**

Ulrich L. Göres — Aktuelle Herausforderungen für Versicherungsunternehmen – Die Compliance-Funktion vor dem Hintergrund einer verstärkten Aufsicht sowie Best-Practice-Lösungsansätzen **783**

Rechtsprechung

Ordnungsgemäßheit der drucktechnischen Gestaltung einer Widerspruchsbelehrung auch bei bloßem Teilfettdruck (OLG Dresden) **801**

Rechtsmissbräuchlichkeit eines Auskunftsbegehrens im Streit um Beitragsanpassungen (OLG Jena) **809**

Wissentliche Pflichtverletzung eines GmbH-Geschäftsführers durch Verletzung der Insolvenzantragspflicht (OLG Frankfurt) **814**

Haftung einer juristischen Person für unerlaubte Handlungen ihres Organs im Rahmen eines „Schneeballsystems“ (BGH) **816**

Fiktive Schadensabrechnung bei vollständiger sach- und fachgerechter Reparatur des Fahrzeugs in der Türkei (BGH) **828**

Beweislastverteilung bei Verletzung eines bei einem Reitverein eingestellten Pferdes (OLG Frankfurt) **830**

Beschädigung eines Anhängers als „Schaden an der versicherten Sache“ (OGH) **839**

Versicherungsrecht

Verlag Versicherungswirtschaft

*Dr. Ulrich L. Göres, Frankfurt/M.**

Aktuelle Herausforderungen für Versicherungsunternehmen

Die Compliance-Funktion vor dem Hintergrund einer verstärkten Aufsicht sowie Best-Practice-Lösungsansätzen

I. Einleitung

Die Compliance-Funktionen von Versicherungsunternehmen in Deutschland zeichnen sich derzeit häufig durch schlanke Strukturen aus, die in Aufbau und Funktionalität eher den Compliance-Funktionen in der Industrie als den komplexeren Organisationsformen für Compliance-Funktionen von Banken und anderen Finanzdienstleistungsunternehmen ähneln.

Angesichts der stetig zunehmenden regulatorischen Anforderungen, insbesondere im Bereich der Informationstechnologie (IT) sowie der Umwelt-, Sozial- und Governance-Themen (ESG), stellt sich jedoch die Frage, inwieweit dieser Ansatz langfristig tragfähig ist. Insbesondere vor dem Hintergrund verstärkter Prüfungen durch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) wird die Belastbarkeit und Anpassungsfähigkeit bestehender Compliance-Strukturen auf eine harte Probe gestellt. In vielen Fällen hat die BaFin bereits signifikante personelle und organisatorische Anpassungen eingefordert, um den gestiegenen Anforderungen gerecht zu werden. Die aufsichtsrechtlichen Erwartungen der BaFin sind in den Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo)[1] kodifiziert. Diese Anforderungen wurden zuletzt überarbeitet und befinden sich derzeit in einem Konsultationsverfahren.[2] Sie verdeutlichen den gestiegenen Anspruch an eine strukturierte, wirksame und zukunftsfähige Compliance-Organisation, die nicht nur reaktiv auf regulatorische Änderungen antwortet, sondern eine proaktive Steuerung von Compliance-Risiken gewährleistet. Die BaFin plant, insbesondere den Anwendungsbereich der MaGo auszudehnen auf Versicherungs-Holdinggesellschaften und gemischte Finanzholding-Gesellschaften, die selbst Versicherungsgeschäft betreiben, § 293 Abs. 1 S. 2 VAG. Der rechtliche Rahmen hierzu war im Gesetzesentwurf der Bundesregierung zur Verbesserung der Bekämpfung von Finanzkriminalität (Finanzkriminalitätsgesetz – FKBG) vorgesehen.[3] Zudem war geplant, dass die geldwäscherechtliche Aufsicht über alle Finanzholding-Gesellschaften und gemischte Finanzholding-Gesellschaften im Geldwäschegesetz (GwG) aufgenommen wird.[4] Hier sollte § 2 GwG um einen Verpflichtetenkreis der Finanzholding-Gesellschaften, gemischten Gesellschaften und Versicherungs-Holdingsgesellschaften erweitert werden. Ob und wann dieses Gesetz nach dem Regierungswechsel allerdings umgesetzt wird, ist derzeit noch ungewiss.

In den „Risiken im Fokus der BaFin 2024", vorgestellt am 23.1.2024 durch BaFin-Präsident *Mark Branson*, wird betont, dass die Geldwäscheaufsicht ihre Prüf- und Überwachungstätigkeit im Banken- sowie im Nichtbankensektor intensiviert.[5] Dies umfasst Sonderprüfungen und risikobasierte Erhebungen u.a. auch bei Versicherungsunternehmen.[6] Laut einem kürzlich veröffentlichten Interview mit *Carsten Sperl*, bei der BaFin zuständig für die Aufsicht über Geldwäsche und Terrorismusfinanzierung, soll der Fokus auf flexiblen Versicherungsprodukten liegen, bei denen innerhalb eines kurzen Zeitraums viele Transaktionen flexibel ein- und ausgezahlt werden können. Hervorgehoben wurden auch die Risiken der Terrorismusfinanzierung sowie die unzureichenden Überprüfungsintervalle des PeP-Status.[7]

Im Jahr 2024 hat die BaFin Versicherungsaufsicht insgesamt 74 Prüfungen bei den beaufsichtigten Unternehmen vorgenommen (2023: 72 Prüfungen; 2022: 75 Prüfungen).[8] Ziel ist es, wirksame Präventionssysteme zur Verhinderung von Geldwäsche und Terrorismusfinanzierung sicherzustellen.[9]

Dieser Aufsatz verfolgt das Ziel, einen systematischen Überblick über die gestiegenen Compliance- und geldwäscherechtlichen Anforderungen der BaFin an Versicherungsunternehmen zu geben (Abschnitt II). Aufbauend auf dieser Analyse werden Best-Practice-Beispiele präsentiert, die Lösungsansätze

* Der Autor ist Rechtsanwalt in Frankfurt/M. und CEO & Geschäftsführender Gesellschafter der TURN Advisory GmbH.

1 BaFin, Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo), abrufbar unter https://www.bafin.de/ref/19616034 (zuletzt abgerufen am 15.5.2025).

2 BaFin, Versicherungsaufsicht: BaFin stellt das überarbeitete Rundschreiben 2/2017 (VA) – Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen zur Konsultation, abrufbar unter: https://www.bafin.de/ref/19792418 (zuletzt abgerufen am 15.5.2025).

3 Entwurf eines Gesetzes zur Verbesserung der Bekämpfung von Finanzkriminalität (Finanzkriminalitätsbekämpfungsgesetz – FKBG), S. 192; abrufbar unter: https://www.bstbk.de/downloads/bstbk/recht-und-berufsrecht/gesetze-und-verordnungen/BStBK_Regierungsentwurf_Finanzkriminalitaetsbekaempfungsgesetz.pdf (zuletzt abgerufen am 15.5.2025).

4 Entwurf eines Gesetzes zur Verbesserung der Bekämpfung von Finanzkriminalität (Finanzkriminalitätsbekämpfungsgesetz – FKBG), S. 155; abrufbar unter: https://www.bstbk.de/downloads/bstbk/recht-und-berufsrecht/gesetze-und-verordnungen/BStBK_Regierungsentwurf_Finanzkriminalitaetsbekaempfungsgesetz.pdf (zuletzt abgerufen am 15.5.2025).

5 BaFin, „Risiken im Fokus 2024", 2024, S. 34.

6 BaFin, „Risiken im Fokus 2024", 2024, S. 34.

7 BaFin (2024): „BaFin fordert Versicherer zu mehr Kontrolle auf", abrufbar unter: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2024/fa_bj_0626_Interview_Sperl.html (zuletzt abgerufen am 14.5.2025).

8 BaFin Jahresbericht 2024 veröffentlicht am 7.5.2025, S. 19.

9 BaFin, „Risiken im Fokus", 2024, S. 34.

und strategische Optionen für den Umgang mit den Herausforderungen im Compliance-Management aufzeigen (Abschnitt III). Abschließend wird ein Ausblick auf künftige Entwicklungen im gesetzlichen und aufsichtsrechtlichen Umfeld und deren potenzielle Implikationen gegeben (Abschnitt IV).

II. Überblick zu Compliance und geldwäscherechtlichen Anforderungen der BaFin an Versicherungsunternehmen

In den vergangenen Jahren haben sich die regulatorischen Anforderungen an Versicherungsunternehmen erheblich verschärft, was insbesondere auf die zunehmende Komplexität und Dynamik des gesetzlichen und aufsichtsrechtlichen Umfelds zurückzuführen ist. Dieser Abschnitt bietet einen systematischen Überblick über die gestiegenen Anforderungen der BaFin, die zunehmend umfassendere Maßnahmen von Versicherungsunternehmen verlangt.

Ein besonderer Schwerpunkt liegt dabei auf zentralen Themenfeldern, die von der BaFin identifiziert und priorisiert wurden. Diese Themenfelder umfassen:

1. *Governance und allgemeines Aufsichtsrecht*: Sicherstellung einer klaren Compliance-Governance, einer angemessenen Organisationsstruktur und der Einhaltung grundlegender regulatorischer Anforderungen im Sinne der Versicherungsaufsicht (MaGo).

2. *IT-Compliance*: Sicherstellung von IT-Sicherheit, Datenintegrität und der Einhaltung regulatorischer Vorgaben im digitalen Umfeld.

3. *Finanzsanktionen*: Implementierung wirksamer Kontrollmechanismen zur Einhaltung nationaler und internationaler Sanktionsregime.

4. *Geldwäsche- und Terrorismusfinanzierungsprävention*: Aufbau und Stärkung risikobasierter Präventionssysteme zur Verhinderung von Geldwäsche und Terrorismusfinanzierung.

5. *Künstliche Intelligenz und algorithmische Verantwortung*: Regulierung und Überwachung des Einsatzes von KI-Systemen im Hinblick auf ethische und rechtliche Anforderungen.

6. *Nachhaltigkeit und ESG-Compliance*: Berücksichtigung von Umwelt-, Sozial- und Governance-Kriterien im Compliance-Management, insbesondere im Kontext der EU-Taxonomie-Verordnung[10] sowie im Rahmen der Corporate Sustainability Reporting Directive (CSRD).[11]

7. *Produkttransparenz und Verbraucherschutz*: Förderung von Transparenz und fairen Marktpraktiken zum Schutz der Versicherungsnehmer.

8. *Auslagerung und Kontrolle von Drittanbietern* (*Third-Party-Risiken*): Sicherstellung der Einhaltung aufsichtsrechtlicher Anforderungen bei der Auslagerung von wesentlichen Funktionen oder Dienstleistungen.

Dieser Überblick dient als Grundlage für die nachfolgende Analyse, die sich auf die besonderen Herausforderungen und Implikationen dieser Themen für Compliance-Funktionen in Versicherungsunternehmen konzentriert.

1. Governance Anforderungen und allgemeines Aufsichtsrecht

In den letzten Jahren wurden die generellen Anforderungen an Governance und Risikomanagement für Versicherungsunternehmen erheblich verschärft. Diese verschärften Anforderungen sollen darauf abzielen, eine robuste und transparente Unternehmensführung sowie ein effektives Risikomanagement sicherzustellen. Die wesentlichen Neuerungen und Anforderungen lassen sich in folgende Kernbereiche untergliedern:

a) Stärkere Einbindung der Unternehmensführung

Die Geschäftsleitung und der Vorstand werden stärker in die Verantwortung genommen, um sicherzustellen, dass Governance- und Risikomanagementstrukturen kontinuierlich überprüft und weiterentwickelt werden. Dazu gehört die Definition des Risikoappetits und deren regelmäßige Bewertung sowie die Implementierung geeigneter Maßnahmen zur Risikominderung. Die BaFin und die europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung (EIOPA – European Insurance and Occupational Pensions Authority) betonen die Rolle der Unternehmensführung als zentrale Instanz für die Überwachung und Steuerung dieser Prozesse.[12]

b) Strengere Anforderungen an das Risikomanagement

Versicherungsunternehmen müssen Risikomanagementsysteme implementieren, die nicht nur finanzielle Risiken, sondern auch nicht finanzielle Risiken wie Cyber-, Nachhaltigkeits- und Reputationsrisiken berücksichtigen. Die Risikoidentifikation, -bewertung und -kontrolle müssen angesichts der zunehmenden Komplexität der Risikolandschaft verstärkt werden. Diese Anforderungen basieren auf der Solvency-II-Richtlinie,[13] die eine systematische Herangehensweise an das Risikomanagement vorschreibt.[14]

c) Erhöhte Transparenzanforderungen und Berichterstattung

Die regulatorischen Vorgaben verlangen eine detailliertere und häufigere Berichterstattung über Governance- und Risikomanagementsysteme. Diese Berichte sollen den Aufsichtsbehörden und Stakeholdern eine umfassende Einschätzung der Risikopositionen sowie der ergriffenen Maßnahmen zur Risikomin-

10 Verordnung (EU) 2020/852 des Europäischen Parlaments und des Rates vom 18.6.2020 über die Einrichtung eines Rahmens zur Erleichterung nachhaltiger Investitionen und zur Änderung der Verordnung (EU) 2019/2088, ABl. Nr. L 198 vom 22.6.2020, S. 13–43.

11 Richtlinie (EU) 2022/2464 des Europäischen Parlaments und des Rates vom 14.12.2022 zur Änderung der Verordnung (EU) Nr. 537/2014 und der Richtlinien 2004/109/EG, 2006/43/EG und 2013/34/EU hinsichtlich der Nachhaltigkeitsberichterstattung von Unternehmen, ABl. Nr. L 322 vom 16.12.2022, S. 15–80.

12 EIOPA Guidelines on System of Governance, Chapter 2.

13 Solvency-II-Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates vom 25.11.2009, ABl. Nr. L 335/1 vom 17.12.2009.

14 Solvency-II-Richtlinie (Fn. 13), Art. 45.

derung ermöglichen. Dazu gehören auch spezifische Berichte über wesentliche Risiken sowie präventive Maßnahmen, die zur Sicherstellung der Stabilität des Unternehmens ergriffen wurden.

d) Proportionalitätsprinzip und Risiko-Profil-Spezifizierung

Die verschärften Anforderungen berücksichtigen das Proportionalitätsprinzip, welches es kleineren oder weniger komplexen Versicherungsunternehmen ermöglicht, die Maßnahmen entsprechend ihrem individuellen Risikoprofil umzusetzen. Dennoch wird erwartet, dass alle Versicherer angemessene Mechanismen und Kontrollen etablieren, die den individuellen Risiken des Unternehmens Rechnung tragen.[15]

e) Einhaltung internationaler Standards

Die verschärften Anforderungen basieren auf der europäischen Solvency-II-Richtlinie sowie zunehmend auf internationalen Standards wie denen der International Association of Insurance Supervisors (IAIS). Diese Standards wurden in den nationalen aufsichtsrechtlichen Rahmen der BaFin integriert und dienen als Grundlage für die Weiterentwicklung der Governance- und Risikomanagementstrukturen in Versicherungsunternehmen.

Diese (regulatorischen) Anpassungen fordern Versicherungsunternehmen auf, ihre Governance- und Risikomanagementsysteme kontinuierlich zu evaluieren und anzupassen, um den steigenden Anforderungen an Transparenz, Stabilität und Verbraucherschutz gerecht zu werden.

2. IT-Compliance

Die regulatorischen Anforderungen an Versicherungsunternehmen im Bereich der IT-Compliance sind in den letzten Jahren angesichts der fortschreitenden Digitalisierung und den damit verbundenen Risiken signifikant gestiegen. (Verwaltungs-) Vorschriften wie die Versicherungsaufsichtlichen Anforderungen an die IT (VAIT),[16] der Digital Operational Resilience Act (DORA) der EU[17] und der am 21.5.2024 verabschiedete EU AI Act[18] verdeutlichen den steigenden Druck auf Versicherer, ihre IT-Systeme und Prozesse den signifikant gestiegenen regulatorischen Vorgaben anzupassen. Da die aufsichtsrechtlichen Anforderungen an die IT im Wesentlichen von der EU-Verordnung DORA abgedeckt werden, hat die BaFin jüngst das Rundschreiben zur VAIT zum 16.1.2025 aufgehoben.[19]

Der nachfolgende Überblick über die aktuell geltenden regulatorischen Anforderungen konzentriert sich insbesondere auf den Datenschutz, die IT-Sicherheit und das Notfallmanagement:

a) Mindestanforderungen an die IT-Sicherheit

Die EU-Verordnung DORA definiert spezifische Standards für die IT-Governance, das Risikomanagement und das Informationssicherheitsmanagementsystem.[20] Diese beinhalten Vorgaben zum Schutz gegen Cyberangriffe, Manipulationen und Datenverlust sowie regelmäßige Überprüfungen und Aktualisierungen der Sicherheitsvorkehrungen. Der Fokus soll hierbei auf einer Stärkung der Resilienz von IT-Systemen liegen.[21]

b) Datenschutz- und Datensicherheitsanforderungen

Die Datenschutz-Grundverordnung (DS-GVO) verlangt von Versicherungsunternehmen die Einhaltung strenger Anforderungen an die Verarbeitung und Sicherung personenbezogener Daten. Hierbei sind insbesondere die Prinzipien der Datenminimierung, Integrität und Verfügbarkeit zu gewährleisten.[22]

c) Business Continuity Management (BCM)

Versicherer sind verpflichtet, Maßnahmen zur Sicherstellung der Geschäftskontinuität zu implementieren.[23] Hierzu zählen Notfallpläne und Wiederherstellungskonzepte, die eine rasche Wiederaufnahme betrieblicher Abläufe nach Störungen ermöglichen sollen.[24]

d) IT-Risikomanagement

Die Identifikation, Bewertung und Steuerung von IT-Risiken sind integraler Bestandteil eines umfassenden Risikomanagements.[25] Regelmäßige Berichte an die Geschäftsführung sind dabei obligatorisch, um eine adäquate Entscheidungsfindung sicherzustellen.

e) Auslagerungsmanagement

Regulatorische Anforderungen an das Auslagerungsmanagement[26] umfassen die Risikoanalyse und die umfassende Dokumentation ausgelagerter IT-Prozesse.[27] Ziel ist es sicherzustellen, dass auch externe Dienstleister den regulatorischen Standards entsprechen.

---

15 Solvency-II-Richtlinie (Fn. 13), Art. 29.

16 BaFin Rundschreiben 10/2018 – Versicherungsaufsichtliche Anforderungen an die IT (VAIT) i.d.F. vom 3.3.2022, abrufbar unter: https://www.bafin.de/ref/19615902 (zuletzt abgerufen am 15.5.2025).

17 Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14.12.2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011, ABl. Nr. L 333 vom 27.12.2022, S. 1–79.

18 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13.6.2024 – Verordnung über künstliche Intelligenz, ABl. L, 2024/1689 vom 12.7.2024, abrufbar unter: https://data.europa.eu/eli/reg/2024/1689/oj (zuletzt abgerufen am 15.5.2025).

19 BaFin, Mitteilung vom 10.1.2025, DORA kommt: Änderungen bei den aufsichtlichen Anforderungen an die IT, abrufbar unter: https://www.bafin.de/ref/19779986 (zuletzt abgerufen am 15.5.2025).

20 EU DORA-Verordnung (Fn. 17), Art. 5 f.

21 BaFin, Interview vom 17.1.2025, Vorbereitung auf DORA, Interview mit Jens Obermöller, Leiter IT-Aufsicht der BaFin, abrufbar unter: https://www.bafin.de/ref/19789986 (zuletzt abgerufen am 15.5.2025).

22 Art. 5 und Art. 32 DSGVO, BaFin VAIT (Fn. 16), Abschn. 4, S. 12.

23 EU DORA-Verordnung (Fn. 17), Art. 11.

24 EU DORA-Verordnung (Fn. 17), Art. 11.

25 EU DORA-Verordnung (Fn. 17), Art. 6.

26 S. auch unter 8. Auslagerung und Kontrolle von Drittanbietern, S. 3.

27 EU DORA-Verordnung (Fn. 17), Art. 28 f.

f) IT-Compliance-Audits und Prüfungen

Die BaFin verlangt regelmäßige IT-Audits, um die Einhaltung von IT-Compliance-Vorgaben zu überprüfen.[28] Diese Audits sollen die Effektivität der implementierten Sicherheitsmaßnahmen sicherstellen und Optimierungsbedarfe aufdecken.

Die BaFin hebt insbesondere die zunehmenden Bedrohungen durch Cyberangriffe hervor, die sowohl IT-Systeme als auch kritische Finanzmarktinfrastrukturen betreffen.[29] Solche Angriffe werden als potentielle Gefahr für die Stabilität des Finanzmarkts bewertet.[30] Versicherungsunternehmen werden daher aufgefordert, ihre IT-Sicherheitsmaßnahmen konsequent zu stärken und im Fall schwerwiegender Betriebs- oder Sicherheitsvorfälle unverzüglich eine Meldung an die BaFin vorzunehmen.[31]

Im Rahmen von IT-Prüfungen hat die BaFin in der Vergangenheit teils erhebliche Mängel festgestellt, insbesondere in den Bereichen Informationsrisiko-, Berechtigungs- und Auslagerungsmanagement.[32] In zwei Fällen wurden Versicherungsunternehmen aufgrund dieser Verstöße Kapitalaufschläge auf die Solvabilitätskapitalanforderung (SCR) auferlegt, verbunden mit der Auflage, die festgestellten Defizite innerhalb einer festgelegten Frist zu beheben.[33]

3. Finanzsanktionen

Die regulatorischen Anforderungen an Versicherungsunternehmen im Bereich Finanzsanktionen haben in den letzten Jahren erheblich zugenommen. Diese Entwicklung ist auf die zunehmende geopolitische Dynamik, die steigende Bedeutung globaler Sanktionsregelungen und die intensivere Durchsetzung durch nationale und internationale Aufsichtsbehörden zurückzuführen. Der Schwerpunkt liegt dabei auf der Verhinderung von Geschäftsbeziehungen mit sanktionierten Personen, Organisationen oder Staaten sowie der Sicherstellung umfassender Compliance mit internationalen Sanktionsvorgaben. Die zentralen Aspekte lassen sich wie folgt zusammenfassen:

- *Umsetzung zunehmender internationaler Sanktionsregelungen*: Versicherungsunternehmen in der EU sind verpflichtet, die von der EU verhängten Sanktionen strikt einzuhalten.[34]
- *Erweiterung der Sorgfaltspflichten*: Versicherungsunternehmen sind verpflichtet, sowohl bei der Begründung von Geschäftsbeziehungen als auch während der Laufzeit der Geschäftsbeziehung regelmäßige Prüfungen durchzuführen, um Transaktionen mit sanktionierten Parteien zu verhindern.[35] Dies hat nach den Anforderungen der Bundesbank insbesondere zu erfolgen durch:
- *Screening-Systeme:* IT-gestützte Abgleiche von Kundendaten mit internationalen Sanktionslisten[36]
- *Transaktionsmonitoring*: Kontinuierliche Überwachung finanzieller Aktivitäten, um mögliche Verstöße frühzeitig zu erkennen[37]
- *IT-gestützte Compliance-Systeme*: Der Einsatz automatisierter Screening-Software hat sich nach Auffassung der zuständigen Stellen als obligatorisch etabliert, um die Vielzahl und Dynamik internationaler Sanktionslisten effizient zu bewältigen.[38] Zudem wird die Notwendigkeit korrekter, vollständiger und aktueller Daten betont, um die Effektivität der Systeme sicherzustellen.[39]
- *Meldepflichten und Zusammenarbeit mit Behörden*: Die Finanzsanktionsverordnungen sehen umfangreiche Mitwirkungs- und Informationspflichten vor, wonach etwa Informationen über eingefrorene Konten und Beträge unverzüglich den zuständigen Behörden der Mitgliedstaaten (betreffend Gelder und Finanzmittel/Finanzhilfen in Deutschland, in der Regel also der Bundesbank) zu übermitteln sind und mit diesen Behörden bei der Überprüfung der Informationen zusammenzuarbeiten ist.[40] Während die Bundesbank grundsätzlich zuständig ist für die Entgegennahme von Meldungen, soweit sich diese auf Gelder im sanktionsrechtlichen Sinn beziehen, ist das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) grundsätzlich zuständig für die Entgegennahme von Meldungen, die sich auf Güter, technische Hilfe oder sonstige wirtschaftliche Ressourcen beziehen.[41]
- *Erhöhte Haftungsrisiken und Sanktionen*: Die verstärkte Überwachung durch Aufsichts- und Strafverfolgungsbehörden hat die Haftungsrisiken bei Verstößen deutlich erhöht. Sanktionen können Bußgelder, strafrechtliche Konsequenzen und erhebliche Reputationsschäden umfassen.[42] Auch Vorstände und Compliance-Beauftragte können persönlich haftbar gemacht werden.[43]
- *Integration in die Compliance-Funktion*: Finanzsanktionen müssen als zentrales Element in die Compliance-Funktion integriert werden. Dies umfasst klare Verantwortlichkeiten, regelmäßige Schulungen und die kontinuierliche Überprüfung der Effektivität der implementierten Maßnahmen.

---

28 EU DORA-Verordnung (Fn. 17), Art. 6.

29 S. Pressebericht „Weltweite IT-Störung aufgrund eines Updates: Diese Banken sind betroffen", IT Finanzmagazin vom 19.7.2024, abrufbar unter: https://www.it-finanzmagazin.de/weltweite-it-stoerung-aufgrund-von-cloud-problemen-diese-banken-sind-betroffen-und-das-koennte-helfen-213227/ (zuletzt abgerufen am 15.5.2025); Bundesamt für Sicherheit in der Informationstechnik (BSI), CrowdStrike: „Welche Folgen der IT-Ausfall für deutsche Unternehmen hatte vom 19.9.2024", abrufbar unter: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/240919_BSI-bitkom_Crowdstrike-Umfrage.html#:~:text=Bei%20den%20direkt%20betroffenen%20Unternehmen,nicht%20verfügbar%20(58%20Prozent) (zuletzt abgerufen am 15.5.2025).

30 BaFin, Jahresbericht 2023, S. 14.

31 BaFin, Jahresbericht 2023, S. 14.

32 BaFin, Jahresbericht 2023, S. 22.

33 BaFin, Jahresbericht 2023, S. 22. Diese Feststellungen setzten sich in 2024 fort, s. hierzu BaFin, Jahresbericht 2024, S. 22.

34 EU-Vertrag, Art. 215; EU-Ratsverordnungen zu spezifischen Sanktionen, z.B. VO (EU) 833/2014 für Russland.

35 Bundesbank, Merkblatt Finanzsanktionen, Merkblatt zur Einhaltung von Finanzsanktionen vom 5.7.2024, S. 17 f.

36 Bundesbank, Merkblatt Finanzsanktionen (Fn. 35), S. 16.

37 Bundesbank, Merkblatt Finanzsanktionen (Fn. 35), S. 16.

38 Bundesbank, Merkblatt Finanzsanktionen (Fn. 35), S. 16.

39 Bundesbank, Merkblatt Finanzsanktionen (Fn. 35), S. 18.

40 Bundesbank, Merkblatt Finanzsanktionen (Fn. 35), S. 11.

41 Bundesbank, Merkblatt Finanzsanktionen (Fn. 35), S. 11.

42 Vgl. § 56 GwG.

43 Vgl. OLG Frankfurt v. 10.4.2018 – 2 Ss-OWi 1059/17, ECLI:DE:OLGHE:2018:0410.2SS.OWI1059.17.00, VersR 2019, 878.

Die Sensibilisierung von Mitarbeitern und die Etablierung einer Unternehmenskultur, die die Einhaltung von Sanktionen priorisiert, sind essenziell.

Die gestiegenen Anforderungen im Bereich Finanzsanktionen stellen Versicherungsunternehmen vor erhebliche Herausforderungen. Die Komplexität internationaler Regelungen, die Ausweitung von Prüfpflichten und die zunehmenden Haftungsrisiken machen den Einsatz moderner Compliance-Technologien, eine robuste Governance-Struktur sowie eine umfassende Sensibilisierung von Mitarbeitenden unerlässlich.

4. Geldwäsche- und Terrorismusfinanzierungsprävention

Die Anforderungen zur Prävention von Geldwäsche (Anti-Money Laundering – AML) und Terrorismusfinanzierung haben sich in den letzten Jahren für Versicherungsunternehmen in Deutschland und Europa erheblich verschärft. Diese Entwicklung resultiert aus strengeren gesetzlichen Vorgaben wie etwa der Umsetzung der EU-Geldwäscherichtlinien und einer intensivierten Überwachung durch die BaFin. Zudem hat der Rat der Europäischen Union ein weiteres Gesetzespaket (AML-Paket) angenommen.[44] Das AML-Paket umfasst:

- eine Verordnung zur Errichtung einer neuen EU-Behörde zur Bekämpfung der Geldwäsche[45] (AMLA-VO), die befugt sein wird, Sanktionen und Geldstrafen zu verhängen. Die AMLA-VO ist am 26.6.2024 in Kraft getreten und gilt bis auf wenige Ausnahmen ab dem 1.7.2025. Die AMLA wird ihren Sitz in Frankfurt haben.
- eine Verordnung zur Neufassung der Verordnung über Geldtransfers[46] (GTVO 2023), die darauf abzielt, Kryptowertetransfers transparenter und vollständig rückverfolgbar zu machen. Die GTVO 2023 ist am 29.6.2023 in Kraft getreten und gilt bereits ab dem 30.12.2024.
- Eine Verordnung über die Verpflichtungen des privaten Sektors zur Bekämpfung der Geldwäsche[47] (EU-Geldwäscherichtlinie) ist am 9.7.2024 in Kraft getreten und wird für die Verpflichteten unter der Aufsicht der BaFin ab dem 10.7.2027 unmittelbar anwendbar sein.
- Eine Richtlinie über die Mechanismen zur Bekämpfung der Geldwäsche auf nationaler Ebene[48] (AMLD) ist am 9.7.2024 in Kraft getreten. Die AMLD muss überwiegend bis zum 10.7.2027 unmittelbar anwendbar sein.

Der folgende Überblick fasst die aktuell geltenden Anforderungen zusammen:

a) Risikobasierter Ansatz

Die Einführung eines stärker differenzierten, risikobasierten Ansatzes hat die Bedeutung der Risikoanalyse erheblich gesteigert. So hat auch die BaFin-Exekutivdirektorin Abwicklung und Geldwäscheprävention, *Birgit Rudolphe*, in der Keynote bei der Fachtagung „Prävention von Geldwäsche und Terrorismusfinanzierung" die Risikoanalyse als „das Kernstück der Prävention" bezeichnet.[49]

„Jeder Verpflichtete müsse eine individuell passende Risikoanalyse für seine eigene Geschäftstätigkeit erstellen und diese regelmäßig aktualisieren. Zu den Sicherungsmaßnahmen gehörten klare interne Grund-sätze, Verfahren und Kontrollen sowie die Funktion des Geldwäschebeauftragten."[50]

Entscheidend ist hierbei, dass die jeweiligen Versicherungsunternehmen eine Bewertung der in ihrem Eigentum befindlichen Gesellschaften dahin gehend vornehmen, inwieweit diese welchen regulatorischen Vorschriften unterliegen und diese dann klassifizieren (sog. Konsolidierungskreis). Versicherungsunternehmen sind verpflichtet, Geschäftsbereiche und Kundenprofile anhand spezifischer Risikofaktoren zu bewerten und Präventionsmaßnahmen gezielt auf risikoreiche Bereiche auszurichten.[51] Ziel ist es, Ressourcen effizient einzusetzen und Risiken wirksam zu minimieren.[52]

b) Kundenidentifizierung und Sorgfaltspflichten

Die Erweiterung der Identifikationspflichten durch die fünfte EU-Geldwäscherichtlinie hat den Rahmen für die Kundenüberprüfung erheblich ausgeweitet.[53] Versicherer müssen nun insbesondere bei hohen Transaktionsvolumina und komplexen Geschäftsbeziehungen die wirtschaftlich Berechtigten identifizieren, deren Daten systematisch dokumentieren und regelmäßige Aktualisierungen vornehmen.[54]

c) Verdachtsmeldungen

Die Meldepflichten im Zusammenhang mit verdächtigen Aktivitäten wurden verschärft. Bereits bei geringfügigen Anhaltspunkten sind Verdachtsmeldungen an die Financial Intelligence Unit (FIU) verpflichtend.[55] Eine Unterlassung dieser Meldungen kann zu erheblichen Sanktionen und auch durch

---

44 Pressemitteilung des Rates der Europäischen Union vom 30.5.2024, Bekämpfung von Geldwäsche: Rat nimmt Paket von Vorschriften an.

45 Verordnung (EU) 2024/1620 des Europäischen Parlaments und des Rates vom 31.5.2024 zur Errichtung der Behörde zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung und zur Änderung der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010, ABl. L, 2024/1620 vom 19.6.2024.

46 Verordnung (EU) 2023/1113 des Europäischen Parlaments und des Rates vom 31.5.2023 über die Übermittlung von Angaben bei Geldtransfers und Transfers bestimmter Kryptowerte und zur Änderung der Richtlinie (EU) 2015/849, ABl. Nr. L 150 vom 9.6.2023, S. 1–39.

47 Verordnung (EU) 2024/1624 des Europäischen Parlaments und des Rates vom 31.5.2024 zur Verhinderung der Nutzung des Finanzsystems für Zwecke der Geldwäsche oder der Terrorismusfinanzierung, ABl. L, 2024/1624 vom 19.6.2024.

48 Richtlinie (EU) 2024/1640 des Europäischen Parlaments und des Rates vom 31.5.2024 über die von den Mitgliedstaaten einzurichtenden Mechanismen zur Verhinderung der Nutzung des Finanzsystems für Zwecke der Geldwäsche oder der Terrorismusfinanzierung, zur Änderung der Richtlinie (EU) 2019/1937 und zur Änderung und Aufhebung der Richtlinie (EU) 2015/849, ABl. L, 2024/1640 vom 19.6.2024.

49 Die Rede ist abrufbar unter: https://www.bafin.de/ref/19693640 (zuletzt abgerufen am 15.5.2025).

50 Die Rede ist abrufbar unter: https://www.bafin.de/ref/19693640 (zuletzt abgerufen am 15.5.2025).

51 2017 mit der Umsetzung der vierten EU-Geldwäscherichtlinie (AMLD4) in § 5 GwG umgesetzt.

52 S. hierzu BaFin, Auslegungs- und Anwendungshinweise zum Geldwäschegesetz (AuA), S. 13 f., abrufbar unter: https://www.bafin.de/ref/19598312 (zuletzt abgerufen am 15.5.2025).

53 2020 mit der Umsetzung der fünften EU-Geldwäscherichtlinie (AMLD5) in §§ 10 ff. GWG umgesetzt.

54 BaFin, AuAs (Fn. 52), S. 40 f.

55 BaFin, AuAs (Fn. 52), S. 82 f., 2020 mit der Umsetzung der fünften EU-Geldwäscherichtlinie (AMLD5) in § 43 GwG umgesetzt.

eine entsprechende Veröffentlichung des Sachverhalts durch die BaFin führen, was die Überwachungspflichten von Versicherungsunternehmen weiter intensiviert.[56] Die Anzahl der von Versicherungsunternehmen abgegebenen und bei der FIU eingegangenen Verdachtsmeldungen ist mit 269 (Vorjahr 2022: 252; 2021: 222) und damit 0,08 % der durch die Verpflichteten des Finanzsektors abgegebene Verdachtsmeldungen weiterhin auf einem äußerst niedrigen Niveau.[57]

d) Geldwäschebeauftragte

Die Anforderungen an die Qualifikation und Unabhängigkeit des Geldwäschebeauftragten haben sich verschärft.[58] Die BaFin fordert, dass Geldwäschebeauftragte über ausreichende Fachkenntnisse und Handlungsspielräume verfügen.[59] Zudem wird ihre Unabhängigkeit betont, um eine objektive und wirksame Überwachung zu gewährleisten.[60]

e) Schulungen und Sensibilisierung

Die Notwendigkeit regelmäßiger und umfassender Schulungen wurde erhöht, um sicherzustellen, dass Mitarbeitende in relevanten Bereichen über geldwäscherechtliche Risiken und Präventionsmaßnahmen informiert sind.[61]

f) Dokumentation und Aufbewahrungspflichten

Die verschärften Dokumentationspflichten verlangen eine umfassende und systematische Erfassung aller AML-Maßnahmen, einschließlich der Protokollierung von Risikoanalysen, Verdachtsfällen und internen Entscheidungen.[62] Diese Dokumentationen dienen der Nachvollziehbarkeit und erleichtern die Überprüfungen durch Aufsichtsbehörden.[63]

g) Interne Überwachung und Kontrolle

Die Anforderungen an die internen Kontrollsysteme wurden erhöht, um sicherzustellen, dass AML-Maßnahmen effektiv und angepasst an aktuelle Bedrohungen sind. Versicherungsunternehmen müssen regelmäßige Überprüfungen und Tests ihrer Compliance-Maßnahmen durchführen, um sich auf neue Risiken einzustellen.[64]

Die gestiegenen Anforderungen sollen nicht nur die Wirksamkeit von Präventionsmaßnahmen erhöhen, sondern auch die Eigenverantwortung von Versicherungsunternehmen im Bereich Geldwäscheprävention stärken.

Mit dem Schreiben „Sensibilisierung zur Prävention von Terrorismusfinanzierung" vom 15.1.2024 hat die BaFin zudem betont, dass Risikoanalysen nicht allein auf Geldwäsche ausgerichtet sein dürfen.[65] Vielmehr seien auch Risiken der Terrorismusfinanzierung zu berücksichtigen, die aus legalen Quellen stammen können.[66] Dies erfordere eine umfassende Betrachtung der institutsspezifischen Risiken, einschließlich geografischer Faktoren, Transaktionsarten und Kundenprofilen.[67] Im Ergebnis muss von den Verpflichteten jeweils eine eigenständige Risikoanalyse für die Säulen Geldwäscheprävention und Prävention von Terrorismusfinanzierung erstellt werden.

5. Künstliche Intelligenz und algorithmische Verantwortung

Mit dem Inkrafttreten der europäischen Verordnung über künstliche Intelligenz (EU AI Act) am 1.8.2024 und ihrer schrittweisen Anwendung innerhalb der nächsten zwei Jahre stehen Versicherungsunternehmen vor neuen regulatorischen Herausforderungen.[68]

Diese betreffen insbesondere die Compliance im Umgang mit künstlicher Intelligenz (KI) und maschinellen Lernverfahren (ML). Die BaFin hat bereits klare Anforderungen formuliert, die den Fokus auf den Schutz vor ungerechtfertigter Diskriminierung sowie die Sicherstellung einer fairen und transparenten Nutzung von KI-Systemen im Finanzsektor legen.[69] Die BaFin Exekutivdirektorin *Julia Wiens* betonte kürzlich in einer Rede zu KI in der Versicherungsbranche, dass es der BaFin wichtig sei, dass die Versicherungsunternehmen „eine angemessene Governance für ihre KI-Anwendungen etablieren".[70] Darüber hinaus sollten sie Technologien in den Blick nehmen, die gerade erst entstehen, wie das Quantencomputing, von dem bereits heute Risiken ausgingen.[71]

a) Diskriminierungsvermeidung und Überprüfungsprozesse

Versicherungsunternehmen sind verpflichtet, Mechanismen zur Vermeidung unzulässiger Diskriminierung zu implementieren.[72] Dies erfordert die Einrichtung von Prozessen zur Identifizierung potenzieller Diskriminierungsquellen, insbesondere

56 BaFin, AuAs (Fn. 52), S. 88 f.

57 S. FIU Jahresbericht 2023, S. 66, abrufbar unter https://www.zoll.de/DE/FIU/Fachliche-Informationen/Jahresberichte/jahresberichte_node.html (zuletzt abgerufen am 15.5.2025).

58 BaFin, AuAs (Fn. 52), S. 20 f.; 2020 mit der Umsetzung der fünften EU-Geldwäscherichtlinie (AMLD5) in § 7 GwG umgesetzt.

59 BaFin, AuAs (Fn. 52), S. 22.

60 BaFin, AuAs (Fn. 52), S. 22.

61 BaFin, AuAs (Fn. 52), S. 28.

62 BaFin, AuAs (Fn. 52), S. 17.

63 BaFin, AuAs (Fn. 52), S. 17.

64 BaFin, Rundschreiben 2/2017 (VA) (Fn. 1), Abschn. 12 (zuletzt abgerufen am 15.5.2025).

65 BaFin Schreiben vom 15.1.2024, nicht öffentlich zugänglich.

66 BaFin Schreiben vom 15.1.2024 (Fn. 65); s. auch Typologiepapier der FIU aus April 2024 zur Terrorismusfinanzierung.

67 BaFin Schreiben vom 15.1.2024 (Fn. 65); s. auch Typologiepapier der FIU aus April 2024 zur Terrorismusfinanzierung.

68 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13.6.2024 – Verordnung über künstliche Intelligenz, ABl. L, 2024/1689 vom 12.7.2024.

69 *Albers/Fahrenwaldt/Kuhn-Stojic/Schneider*, KI bei Banken und Versicherern: Automatisch Fair, BaFinJournal vom 1.8.2024, abrufbar unter: https://www.bafin.de/ref/19755884 (zuletzt abgerufen am 15.5.2025).

70 *Wiens*, KI in der Versicherungsbranche: „Die Verantwortung liegt bei den Unternehmen", Rede beim Vorlesungstag des Instituts für Versicherungswissenschaften e.V. an der Universität zu Leipzig, 6.3.2025, abrufbar unter: https://www.bafin.de/ref/19801662 (zuletzt abgerufen am 15.5.2025).

71 *Wiens*, KI in der Versicherungsbranche: „Die Verantwortung liegt bei den Unternehmen", Rede beim Vorlesungstag des Instituts für Versicherungswissenschaften e.V. an der Universität zu Leipzig, 6.3.2025, abrufbar unter: https://www.bafin.de/ref/19801662 (zuletzt abgerufen am 15.5.2025).

bei der Nutzung von KI- und ML-Anwendungen.[73] Die BaFin betont die Notwendigkeit, nicht nur präventive Maßnahmen zu ergreifen, sondern auch laufende Prüfungen durchzuführen, um Diskriminierung im Betrieb zu erkennen und zu beheben.[74] Eine solche Anforderung erfordert ein hohes Maß an Transparenz und Effektivität in den Verfahren zur Daten-Governance und -Verwaltung.[75]

b) Daten-Governance und Datenverwaltung

Eine zuverlässige und transparente Daten-Governance ist ein Schlüssel zur Vermeidung diskriminierender Ergebnisse in KI-Anwendungen.[76] Die BaFin fordert von Versicherungsunternehmen, die Qualität und den Ursprung der verwendeten Daten sicherzustellen und die Nachvollziehbarkeit der Datenverarbeitung zu gewährleisten.[77] Dies beinhaltet die Verpflichtung, Datenverwaltungssysteme so zu gestalten, dass eine faire Behandlung aller VN sichergestellt wird.[78] Besonders wichtig ist dabei die klare Zuordnung von Verantwortlichkeiten für die Auswahl, Pflege und Aktualisierung der Datengrundlagen, die Grundlage für KI-gestützte Entscheidungen sind.

c) Menschliche Aufsicht und Verantwortung

Die BaFin hebt die Bedeutung menschlicher Aufsicht bei der Nutzung von KI hervor.[79] Versicherungsunternehmen müssen sicherstellen, dass ihre KI-Systeme kontinuierlich von qualifiziertem Personal überwacht werden, um potenzielle technische Unzulänglichkeiten und Datenlücken auszugleichen.[80] Die menschliche Aufsicht dient zudem als Kontrollinstanz, um sicherzustellen, dass Entscheidungen der KI den rechtlichen und ethischen Vorgaben entsprechen. Dies ist insbesondere wichtig, um unvorhergesehene negative Auswirkungen auf benachteiligte Gruppen zu vermeiden.[81]

d) BaFin-Maßnahmen bei Verstößen

Verstöße gegen das Diskriminierungsverbot oder andere regulatorische Anforderungen im Zusammenhang mit KI-Anwendungen können zu strengen Maßnahmen der BaFin führen.[82] Dies schließt die Modifikation oder Abschaltung von KI-Systemen ein, wenn Missstände festgestellt werden. Versicherungsunternehmen sind daher angehalten, proaktiv mögliche Diskriminierungsrisiken zu analysieren und entsprechende Compliance-Maßnahmen zu entwickeln, um regulatorische Sanktionen zu vermeiden.[83]

Die Anforderungen der BaFin verdeutlichen die Notwendigkeit eines mehrschichtigen Compliance-Rahmenwerks für den Einsatz von KI in der Versicherungsbranche, um eine diskriminierungsfreie und verantwortungsvolle Nutzung von KI-gestützten Anwendungen zu gewährleisten. Dieses Rahmenwerk umfasst eine robuste Governance, präventive Überprüfungsprozesse, transparente Daten- und Systemkontrollen sowie organisatorische Maßnahmen zur Sicherstellung regulatorischer und ethischer Konformität.

6. Nachhaltigkeit und ESG-Compliance

Die zunehmende Bedeutung von Nachhaltigkeit spiegelt sich insbesondere auch in regulatorischen Anforderungen wider, die Versicherungsunternehmen zur Offenlegung und Einhaltung von ESG-Kriterien (Environmental, Social, Governance) verpflichten. Die EU-Taxonomieverordnung[84] und die Offenlegungsverordnung[85] (SFDR) zielen darauf ab, Transparenz in der Bewertung nachhaltigkeitsbezogener Risiken für Kapitalanlagen und angebotene Produkte zu schaffen. Versicherungsunternehmen stehen vor der Herausforderung, diese Anfor-

72 *Wiens*, KI in der Versicherungsbranche: „Die Verantwortung liegt bei den Unternehmen", Rede beim Vorlesungstag des Instituts für Versicherungswissenschaften e.V. an der Universität zu Leipzig, 6.3.2025, abrufbar unter: https://www.bafin.de/ref/19801662 (zuletzt abgerufen am 15.5.2025).

73 *Wiens*, KI in der Versicherungsbranche: „Die Verantwortung liegt bei den Unternehmen", Rede beim Vorlesungstag des Instituts für Versicherungswissenschaften e.V. an der Universität zu Leipzig, 6.3.2025, abrufbar unter: https://www.bafin.de/ref/19801662 (zuletzt abgerufen am 15.5.2025).

74 *Wiens*, KI in der Versicherungsbranche: „Die Verantwortung liegt bei den Unternehmen", Rede beim Vorlesungstag des Instituts für Versicherungswissenschaften e.V. an der Universität zu Leipzig, 6.3.2025, abrufbar unter: https://www.bafin.de/ref/19801662 (zuletzt abgerufen am 15.5.2025).

75 *Wiens*, KI in der Versicherungsbranche: „Die Verantwortung liegt bei den Unternehmen", Rede beim Vorlesungstag des Instituts für Versicherungswissenschaften e.V. an der Universität zu Leipzig, 6.3.2025, abrufbar unter: https://www.bafin.de/ref/19801662 (zuletzt abgerufen am 15.5.2025).

76 *Wiens*, KI in der Versicherungsbranche: „Die Verantwortung liegt bei den Unternehmen", Rede beim Vorlesungstag des Instituts für Versicherungswissenschaften e.V. an der Universität zu Leipzig, 6.3.2025, abrufbar unter: https://www.bafin.de/ref/19801662 (zuletzt abgerufen am 15.5.2025).

77 *Wiens*, KI in der Versicherungsbranche: „Die Verantwortung liegt bei den Unternehmen", Rede beim Vorlesungstag des Instituts für Versicherungswissenschaften e.V. an der Universität zu Leipzig, 6.3.2025, abrufbar unter: https://www.bafin.de/ref/19801662 (zuletzt abgerufen am 15.5.2025).

78 *Wiens*, KI in der Versicherungsbranche: „Die Verantwortung liegt bei den Unternehmen", Rede beim Vorlesungstag des Instituts für Versicherungswissenschaften e.V. an der Universität zu Leipzig, 6.3.2025, abrufbar unter: https://www.bafin.de/ref/19801662 (zuletzt abgerufen am 15.5.2025).

79 *Wiens*, KI in der Versicherungsbranche: „Die Verantwortung liegt bei den Unternehmen", Rede beim Vorlesungstag des Instituts für Versicherungswissenschaften e.V. an der Universität zu Leipzig, 6.3.2025, abrufbar unter: https://www.bafin.de/ref/19801662 (zuletzt abgerufen am 15.5.2025).

80 *Wiens*, KI in der Versicherungsbranche: „Die Verantwortung liegt bei den Unternehmen", Rede beim Vorlesungstag des Instituts für Versicherungswissenschaften e.V. an der Universität zu Leipzig, 6.3.2025, abrufbar unter: https://www.bafin.de/ref/19801662 (zuletzt abgerufen am 15.5.2025).

81 *Wiens*, KI in der Versicherungsbranche: „Die Verantwortung liegt bei den Unternehmen", Rede beim Vorlesungstag des Instituts für Versicherungswissenschaften e.V. an der Universität zu Leipzig, 6.3.2025, abrufbar unter: https://www.bafin.de/ref/19801662 (zuletzt abgerufen am 15.5.2025).

82 *Wiens*, KI in der Versicherungsbranche: „Die Verantwortung liegt bei den Unternehmen", Rede beim Vorlesungstag des Instituts für Versicherungswissenschaften e.V. an der Universität zu Leipzig, 6.3.2025, abrufbar unter: https://www.bafin.de/ref/19801662 (zuletzt abgerufen am 15.5.2025).

83 *Wiens*, KI in der Versicherungsbranche: „Die Verantwortung liegt bei den Unternehmen", Rede beim Vorlesungstag des Instituts für Versicherungswissenschaften e.V. an der Universität zu Leipzig, 6.3.2025, abrufbar unter: https://www.bafin.de/ref/19801662 (zuletzt abgerufen am 15.5.2025).

84 Verordnung (EU) 2020/852 des Europäischen Parlaments und des Rates vom 18.6.2020 über die Einrichtung eines Rahmens zur Erleichterung nachhaltiger Investitionen und zur Änderung der Verordnung (EU) 2019/2088, ABl. Nr. L 198 vom 22.6.2020.

85 Verordnung (EU) 2019/2088 des Europäischen Parlaments und des Rates vom 27.11.2019 über nachhaltigkeitsbezogene Offenlegungspflichten, ABl. Nr. L 317 vom 9.12.2019, S. 1–16.

derungen in ihre bestehenden Strukturen und Prozesse zu integrieren.

Die BaFin hat bereits im Jahr 2020 ein Merkblatt zum Umgang mit Nachhaltigkeitsrisiken veröffentlicht, das als Orientierungshilfe für beaufsichtigte Unternehmen dient.[86] Dieses Merkblatt unterstützt die Umsetzung der Empfehlung 1 b) des Network for Greening the Financial System (NGFS), klimabezogene Risiken in die Aufsicht zu integrieren und klare Erwartungen zu formulieren.[87] Die Hinweise der BaFin sind ausdrücklich als Good-Practice-Ansätze konzipiert, die unter Berücksichtigung des Proportionalitätsprinzips angewendet werden können.[88] Dies erlaubt eine differenzierte Umsetzung, die sich an der Größe, Komplexität und dem Risikoprofil des jeweiligen Unternehmens orientiert.

Der Begriff „Nachhaltigkeitsrisiko" bezeichnet nach Art. 1 Nr. 55c der Delegierten Verordnung (EU) 2015/35[89]

„ein Ereignis oder eine Bedingung in den Bereichen Umwelt, Soziales oder Unternehmensführung (Environmental, Social, Governance – ESG), dessen bzw. deren Eintreten tatsächlich oder potenziell negative Auswirkungen auf den Wert der Investition oder auf den Wert der Verbindlichkeit haben könnte."

In Bezug auf die Compliance-Funktion betont die BaFin im Merkblatt unter Ziff. 5.9 die Bedeutung einer Anpassung an die Anforderungen der MaGo, d.h. die Mindestanforderungen an die Geschäftsorganisation.[90] Die Compliance-Funktion soll rechtliche und regulatorische Vorgaben im Bereich Nachhaltigkeit berücksichtigen.[91] Auf dieser Grundlage lassen sich die zentralen Aufgaben der Compliance-Funktion im Bereich der Nachhaltigkeit wie folgt strukturieren:

a) Integration in bestehende Strukturen

Nachhaltigkeitsrisiken sollen in bestehende Compliance-Aufgaben und -Prozesse integriert werden, um eine ganzheitliche Betrachtung aller relevanten Nachhaltigkeitsrisiken sicherzustellen. Nachhaltigkeitsrisiken sind ausweislich des BaFin-Merkblatts „Ereignisse oder Bedingungen aus den Bereichen Umwelt, Soziales oder Unternehmensführung, deren Eintreten tatsächlich oder potenziell negative Auswirkungen auf die Vermögens-, Finanz- und Ertragslage sowie auf die Reputation eines beaufsichtigten Unternehmens haben können".[92]

b) Überwachung

Die Compliance-Funktion trägt die Verantwortung für die Überwachung der Einhaltung von Gesetzen, Vorschriften und internen Richtlinien im Zusammenhang mit Nachhaltigkeitsrisiken.

c) Beratung

Die Compliance-Funktion soll die Geschäftsleitung und relevante Geschäftsbereiche in Bezug auf Nachhaltigkeitsrisiken beraten.

d) Schulungen

Die regelmäßige Durchführung von Schulungen zu Nachhaltigkeitsrisiken und deren regulatorischen Anforderungen dient der Sensibilisierung und dem Kompetenzaufbau bei Mitarbeitenden.

e) Risikoanalyse

Nachhaltigkeitsrisiken müssen systematisch in die regelmäßige Risikoanalyse einbezogen werden, um potenzielle Bedrohungen frühzeitig zu erkennen und angemessen darauf zu reagieren.

f) Berichterstattung

Die Compliance-Funktion ist verpflichtet, wesentliche Erkenntnisse zu Nachhaltigkeitsrisiken und deren Handhabung regelmäßig an die Geschäftsleitung zu berichten.

Ein zunehmend wichtiger Aspekt der ESG-Compliance ist die Vermeidung von sog. Greenwashing. Dabei handelt es sich um die irreführende Darstellung von Produkten, Dienstleistungen oder Unternehmenspraktiken als nachhaltiger, als sie tatsächlich sind.[93] Versicherungsunternehmen stehen vor der Herausforderung, Transparenz in ihren ESG-Aktivitäten zu gewährleisten und gleichzeitig regulatorischen Anforderungen wie der EU-Offenlegungsverordnung (SFDR) gerecht zu werden.

Maßnahmen zur Vermeidung von Greenwashing umfassen:

- *Transparente Berichterstattung*: ESG-bezogene Angaben müssen auf überprüfbaren und konsistenten Daten basieren, um eine klare Abgrenzung zu rein marketingorientierten Aussagen sicherzustellen.
- *Standardisierte Offenlegungsprozesse*: Einheitliche Vorgaben und ein klarer Rahmen für ESG-Daten erleichtern die Überprüfung und Kommunikation der Nachhaltigkeitsbemühungen.
- *Unabhängige Audits*: Regelmäßige Überprüfungen durch externe Prüfer stärken die Glaubwürdigkeit der ESG-Berichterstattung und beugen falschen Darstellungen vor.

---

86 BaFin, Merkblatt zum Umgang mit Nachhaltigkeitsrisiken vom 13.1.2020, abrufbar unter: https://www.bafin.de/ref/19598538 (zuletzt abgerufen am 15.5.2025).

87 BaFin, Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo) (Fn. 1), S. 8.

88 BaFin, Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo) (Fn. 1), S. 8.

89 Delegierte Verordnung (EU) 2015/35 der Kommission vom 10.10.2014 zur Ergänzung der Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit (Solvabilität II), ABl. Nr. L 12 vom 17.1.2015, S. 1–797. „Nachhaltigkeitsrisiko" ist „ein Ereignis oder eine Bedingung in den Bereichen Umwelt, Soziales oder Unternehmensführung, dessen bzw. deren Eintreten tatsächlich oder potentiell wesentliche negative Auswirkungen auf den Wert der Investition haben könnte." Auch im Wertpapierbereich wird die gleichlautende Definition verwendet. S. hierzu Art. 2 Nr. 22 der Verordnung (EU) 2019/2088 des Europäischen Parlaments und des Rates vom 27.11.2019 über nachhaltigkeitsbezogene Offenlegungspflichten im Finanzdienstleistungssektor, ABl. Nr. L 317/1 ff. vom 9.12.2019.

90 BaFin, Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo) (Fn. 1).

91 BaFin, Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGO) (Fn. 1), S. 23.

92 BaFin-Merkblatt Nachhaltigkeit (Fn. 86), S. 18.

93 Vgl. Richtlinie (EU) 2024/825 des Europäischen Parlaments und des Rates vom 28.2.2024 zur Änderung der Richtlinien 2005/29/EG und 2011/83/EU hinsichtlich der Stärkung der Verbraucher für den ökologischen Wandel durch besseren Schutz gegen unlautere Praktiken und durch bessere Informationen, ABl. L, 2024/825 vom 6.3.2024, Rz. 11.

- *Interne Schulungen*: Mitarbeitende müssen für die Risiken und Konsequenzen von Greenwashing sensibilisiert werden, um Fehler und irreführende Aussagen zu vermeiden.

Die Umsetzung dieser Anforderungen erfolgt unter Beachtung des Proportionalitätsprinzips, das eine Anpassung an die individuellen Gegebenheiten des Unternehmens ermöglicht.[94] Dies bedeutet, dass die Maßnahmen in Abhängigkeit von Größe, Komplexität und Risikoprofil eines Unternehmens ausgestaltet werden müssen.

Die stärkere Einbindung der Compliance-Funktion in Nachhaltigkeitsthemen wird durch die überarbeitete und zur Konsultation stehende Fassung des MaGo-Rundschreibens der BaFin vom 26.4.2024 zusätzlich hervorgehoben.[95] Hier wird insbesondere die kontinuierliche Beobachtung und Nachverfolgung von Entwicklungen im Bereich Nachhaltigkeit sowie deren Umsetzung in die Unternehmensprozesse betont.[96] Diese Anforderungen verdeutlichen die wachsende Bedeutung einer umfassenden ESG-Compliance und die Notwendigkeit, Nachhaltigkeitskriterien systematisch bei der Unternehmensführung zu berücksichtigen.

7. Produkttransparenz und Verbraucherschutz

Auch die regulatorischen Anforderungen an Versicherungsunternehmen im Bereich Produkttransparenz und Verbraucherschutz wurden in den vergangenen Jahren erheblich verschärft.[97] Diese Entwicklungen spiegeln den verstärkten Fokus der Aufsichtsbehörden auf den Schutz der Versicherungsnehmer sowie die Verbesserung der Transparenz in Bezug auf Versicherungsprodukte und -dienstleistungen wider. Die zentralen Aspekte lassen sich wie folgt zusammenfassen:

a) Erhöhte Transparenzanforderungen

Versicherungsunternehmen sind zunehmend verpflichtet, ihre Produkte und die damit verbundenen Kosten klar, verständlich und nachvollziehbar darzustellen.[98] Verlangt werden insbesondere eine transparente Darstellung aller wesentlichen Produktmerkmale sowie potenzieller Risiken, um den Verbrauchern eine fundierte Entscheidungsfindung zu ermöglichen.

b) Verbesserte Informationspflichten

Die Ausweitung der Informationspflichten zielt darauf ab, Versicherungsnehmer frühzeitig und umfassend über ihre Rechte und Pflichten aufzuklären.[99] Dazu gehören insbesondere die Vertragsbedingungen, Leistungsversprechen, Laufzeiten sowie Kündigungsfristen.[100] Die Einführung standardisierter Produktinformationsblätter soll sicherstellen, dass wesentliche Informationen übersichtlich und leicht verständlich präsentiert werden.[101] Dies unterstützt Verbraucher bei der Vergleichbarkeit und Bewertung von Versicherungsprodukten.

c) Schutz vor missbräuchlichen Produkten und Praktiken

Die BaFin überwacht verstärkt die Entwicklung und den Vertrieb von Versicherungsprodukten, um missbräuchliche Praktiken zu verhindern.[102] Produkte, die unverhältnismäßige Kosten verursachen oder schwer verständlich sind, stehen dabei besonders im Fokus.[103] Versicherungsunternehmen sind verpflichtet sicherzustellen, dass ihre Produkte den Bedürfnissen und Interessen der Zielgruppen entsprechen und keine versteckten Kosten oder übermäßigen Risiken beinhalten. Dies erfordert eine ethische und kundenorientierte Vertriebsstrategie sowie die kontinuierliche Überprüfung von Vertriebspraktiken.[104] In einer EIOPA-koordinierten Mystery-Shopping-Aktion testete die BaFin 2024 den Vertrieb von Versicherungs anlageprodukten. Es ging dabei um Lebens- und Ren tenversicherungen, deren Wert von Marktschwankungen abhängig ist. Bei der Aktion standen Beratungs- und Informationspflichten im Vordergrund.[105]

d) Stärkung des Widerrufs- und Kündigungsrechts

Die Rechte der Verbraucher in Bezug auf Widerruf und Kündigung wurden umfassend gestärkt, um eine größere Flexibilität und Schutz vor langfristigen Verpflichtungen zu gewährleisten. Versicherungsunternehmen sind verpflichtet, diese Informationen klar in Vertragsunterlagen hervorzuheben und Verbraucher über ihre Widerrufs- und Kündigungsmöglichkeiten umfassend aufzuklären.[106]

---

94 BaFin, Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo) (Fn. 1), S. 11.

95 Entwurf einer überarbeiteten Fassung der MaGo für Solvency II Versicherungsunternehmen vom 26.4.2024, Ziff. 10.2.

96 Entwurf einer überarbeiteten Fassung der MaGo für Solvency II Versicherungsunternehmen vom 26.4.2024, Ziff. 10.2.

97 BaFin, Schwerpunkte der Versicherungsaufsicht 2025 vom 20.11.2024, Rede von Julia Wiens, Exekutivdirektorin Versicherungs- und Pensionsfondsaufsicht, bei der Jahrestagung der Versicherungsaufsicht, abrufbar unter: https://www.bafin.de/ref/19774138 (zuletzt abgerufen am 15.5.2025).

98 BaFin, Schwerpunkte der Versicherungsaufsicht 2025 vom 20.11.2024, Rede von *Julia Wiens*, Exekutivdirektorin Versicherungs- und Pensionsfondsaufsicht, bei der Jahrestagung der Versicherungsaufsicht, abrufbar unter: https://www.bafin.de/ref/19774138 (zuletzt abgerufen am 15.5.2025).

99 BaFin, Welche Verbraucherinformationen muss der Versicherer dem Versicherungsnehmer bei Abschluss eines Versicherungsvertrags zur Verfügung stellen?, 5.5.2023, abrufbar unter: https://www.bafin.de/ref/19628494 (zuletzt abgerufen am 15.5.2025).

100 BaFin, Welche Verbraucherinformationen muss der Versicherer dem Versicherungsnehmer bei Abschluss eines Versicherungsvertrags zur Verfügung stellen?, 5.5.2023, abrufbar unter https://www.bafin.de/ref/19628494 (zuletzt abgerufen am 15.5.2025).

101 EIOPA, Editable Template for the Insurance Product Information Document, abrufbar unter: https://www.eiopa.europa.eu/browse/regulation-and-policy/insurance-distribution-directive-idd/editable-template-insurance-product-information-document-ipid_en). (zuletzt abgerufen am 15.5.2025

102 BaFin, Versicherungsvertrieb: Auswirkungendes geplanten Umsetzungsgesetzes auf die Aufsicht, abrufbar unter: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2017/fa_bj_1703_Versicherungsvertrieb.html (zuletzt abgerufen am 15.5.2025).

103 BaFin, Versicherungsvertrieb: Auswirkungendes geplanten Umsetzungsgesetzes auf die Aufsicht, abrufbar unter: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2017/fa_bj_1703_Versicherungsvertrieb.html (zuletzt abgerufen am 15.5.2025).

104 Vgl. IDD Art. 25 und 30.

105 BaFin, Jahresbericht 2024, S. 31.

106 Die rechtliche Grundlage dafür bietet das VVG (§§ 8, 9).

e) Verpflichtungen im Rahmen der Produktüberwachung und -kontrolle

Die kontinuierliche Produktüberwachung und -kontrolle, auch bekannt als „Product Oversight and Governance" (POG), gehört zu den wesentlichen regulatorischen Anforderungen.[107] Über die gesamte Lebensdauer eines Produkts hinweg müssen Versicherungsunternehmen sicherstellen, dass die Produkte weiterhin den Bedürfnissen und Erwartungen der Zielgruppe entsprechen. Anpassungen sind erforderlich, wenn dies nicht mehr gewährleistet ist. Die BaFin überprüft, ob diese Prozesse ordnungsgemäß implementiert und durchgeführt werden, und legt dabei besonderen Wert auf die langfristige Marktgängigkeit und Eignung der Produkte.[108] Die BaFin hat hierbei als ein wichtiges Thema den Wandel von klassischen Lebensversicherungen mit Garantien hin zu flexibleren Versicherungsprodukten identifiziert.[109] Diese relativ neuen Produkte zeichnen sich durch die kurzfristige Verfügbarkeit der angelegten Gelder aus. Im Gegensatz zur herkömmlichen Lebensversicherung, bei der regelmäßige und gleichbleibende Prämienzahlungen erfolgen, führen flexible Ein- und Auszahlungsmöglichkeiten zu vielen Transaktionen innerhalb eines relativ kurzen Zeitraums in einem Vertrag. Diese zusätzlichen unregelmäßigen Zahlungen machen es komplizierter, die Mittelzu- bzw. -abflüsse zu überwachen. Auch die vielen banknahen Geschäfte der Versicherungsunternehmen, wie beispielsweise Tagesgelder oder Darlehensgeschäfte, bringen zusätzliche Herausforderungen für die Geldwäscheprävention mit sich, da hier die Gefahr, dass illegale Gelder durch Transaktionen verschleiert und in den legalen Wirtschaftskreislauf integriert werden, ähnlich hoch ist wie bei einem Kreditinstitut. Es empfiehlt sich, dass die Compliance-Funktion generell zwingend in die Prüfung und Freigabe von neuen oder modifizierten Produkten frühzeitig eingebunden wird. Für den Bereich Geldwäsche ist dies ohnehin zwingend vorgeschrieben.

Zusammengefasst ist zu erkennen, dass sich die regulatorischen Anforderungen an Versicherungsunternehmen im Bereich der Produkttransparenz und des Verbraucherschutzes erheblich erhöht haben. Ziel dieser Maßnahmen ist es, die Kundenorientierung und Fairness im Versicherungssektor zu stärken, Transparenz über Produkte und Kosten zu schaffen und letztlich den Schutz der Verbraucherinnen und Verbraucher in einer zunehmend komplexen und digitalisierten Versicherungslandschaft sicherzustellen.

8. Auslagerung und Kontrolle von Drittanbietern (Third-Party-Risiken)

Die regulatorischen Anforderungen an die Auslagerung wesentlicher Funktionen und Dienstleistungen haben sich in den letzten Jahren erheblich verschärft. Die BaFin hat aktuell mit der Überarbeitung der Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen klare Vorgaben zur Steuerung und Überwachung von Outsourcing-Prozessen formuliert.[110] Dabei steht insbesondere die Risikosteuerung und Kontrolle von Drittanbietern (Third-Party-Risiken) im Fokus. Versicherungsunternehmen sind verpflichtet sicherzustellen, dass auch ausgelagerte Prozesse und Dienstleistungen den aufsichtsrechtlichen Anforderungen entsprechen und jederzeit effektiv überwacht werden.[111]

Die zentralen Anforderungen im Bereich Auslagerungsmanagement lassen sich wie folgt zusammenfassen:

a) Risikobewertung und Dokumentation von Auslagerungen

Versicherungsunternehmen müssen eine umfassende Risikoanalyse durchführen, bevor eine Funktion oder Dienstleistung ausgelagert wird.[112] Dies umfasst eine systematische Bewertung, ob die Auslagerung wesentliche Geschäftsprozesse betrifft und inwieweit dadurch die Risikoexposition des Unternehmens erhöht wird.[113] Zudem fordert die BaFin, dass alle wesentlichen Auslagerungen sorgfältig zu dokumentieren und regelmäßig zu überprüfen sind.[114]

b) Vertragliche Mindestanforderungen und Steuerung der Dienstleister

Die Verträge mit externen Dienstleistern müssen spezifische aufsichtsrechtliche Mindestanforderungen erfüllen. Diese betreffen insbesondere die Regelung von Kontrollrechten, Informationspflichten, Datenzugriffen sowie Notfallvorsorge.[115] Die BaFin fordert zudem, dass Unternehmen jederzeit die Verantwortung und Steuerung für ausgelagerte Prozesse behalten und ein funktionierendes Notfallmanagement sicherstellen müssen.[116]

c) Laufendes Monitoring und Überwachung

Ein wirksames Überwachungssystem ist erforderlich, um die Einhaltung der vertraglichen und regulatorischen Vorgaben durch den Dienstleister fortlaufend zu kontrollieren.[117] Dazu zählen regelmäßige Berichterstattungen, Audits und Risikobewertungen.

d) IT-Auslagerungen und Cloud-Computing

Besondere Anforderungen gelten für IT-bezogene Auslagerungen, insbesondere im Bereich Cloud-Computing. Die BaFin

107 BaFin, Versicherungsvertrieb: Auswirkungen des geplanten Umsetzungsgesetzes auf die Aufsicht, abrufbar unter: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2017/fa_bj_1703_Versicherungsvertrieb.html (zuletzt abgerufen am 15.5.2025).

108 BaFin, Versicherungsvertrieb: Auswirkungen des geplanten Umsetzungsgesetzes auf die Aufsicht, abrufbar unter: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2017/fa_bj_1703_Versicherungsvertrieb.html (zuletzt abgerufen am 15.5.2025).

109 BaFin (2024): „BaFin fordert Versicherer zu mehr Kontrolle auf", abrufbar unter: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2024/fa_bj_0626_Interview_Sperl.html (zuletzt abgerufen am 15.5.2025).

110 BaFin, Versicherungsaufsicht: BaFin stellt das überarbeitete Rundschreiben 2/2017 (VA) – Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen zur Konsultation (MaGo) (Fn. 1), Kap. 13.

111 BaFin, MaGo (Fn. 1), Kap. 13.3.

112 BaFin, MaGo (Fn. 1), Kap. 13.3.

113 BaFin, MaGo (Fn. 1), Kap. 13.3.

114 BaFin, MaGo (Fn. 1), Kap. 13.3.

115 BaFin, MaGo (Fn. 1), Kap. 13.3.

116 BaFin, MaGo (Fn. 1), Kap. 13.3.

117 BaFin, MaGo (Fn. 1), Kap. 13.3.

verweist auf den EU-Digital Operational Resilience Act (DORA), der spezifische Vorgaben für IT-Sicherheit, Datenzugriff, Systemverfügbarkeit und Notfallmanagement enthalten.[118] Nach DORA müssen Versicherungsunternehmen sicherstellen, dass Cloud-Dienstleister die gleichen Sicherheits- und Compliance-Standards erfüllen wie interne IT-Systeme.[119]

e) Notfallpläne und Exit-Strategien

Versicherungsunternehmen sind verpflichtet, Notfallpläne und Exit-Strategien für alle wesentlichen Auslagerungen zu entwickeln.[120] Diese müssen sicherstellen, dass das Unternehmen im Fall von Leistungsstörungen oder der Insolvenz eines Dienstleisters die ausgelagerten Prozesse schnell und ohne erhebliche Beeinträchtigungen wieder in die eigene Organisation zurückholen oder an alternative Anbieter überführen kann.[121]

f) Meldepflichten und aufsichtsrechtliche Anforderungen

Die BaFin verpflichtet Versicherungsunternehmen, eine fortlaufende Bewertung der ausgelagerten Funktionen vorzunehmen und wesentliche Auslagerungen der Aufsicht zu melden.[122]

Die steigenden Anforderungen an das Auslagerungsmanagement zwingen Versicherungsunternehmen dazu, strukturiertere und umfassendere Kontrollmechanismen für externe Dienstleister zu implementieren. Ein effektives Risikomanagement, klare vertragliche Regelungen und eine kontinuierliche Überwachung sind essenziell, um die Einhaltung aufsichtsrechtlicher Anforderungen sicherzustellen und operationelle Risiken zu minimieren. Die zunehmende Digitalisierung und der verstärkte Einsatz von Cloud-Lösungen erfordern zudem erweiterte Kontrollmechanismen, um IT-Sicherheitsrisiken und regulatorische Vorgaben konsequent zu erfüllen.

III. Lösungsansätze und Best-Practice-Beispiele für Compliance-Funktionen

Die steigende Komplexität und Vielfalt regulatorischer Anforderungen zwingt Versicherungsunternehmen, ihre Compliance-Funktionen kontinuierlich weiterzuentwickeln. Dabei stellt sich die Frage, wie diese Herausforderungen effizient und nachhaltig bewältigt werden können, ohne unverhältnismäßig große Strukturen aufzubauen. Angesichts unterschiedlicher Geschäftsmodelle, Unternehmensgrößen und internationaler Ausrichtungen gibt es keinen universellen „One-Size-Fits-All"-Ansatz. Individuelle und passgenaue Lösungen sind daher essenziell.

Eine flexible, strategische Verteilung der Compliance-Aufgaben ist dabei entscheidend. Dezentrale Strukturen und die Förderung von Eigenverantwortung in anderen Abteilungen können die Effizienz steigern, während eine zentrale Steuerungsfunktion die Einhaltung von Governance-Vorgaben gewährleistet und fortlaufend kontrolliert und überwacht. Die Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo) sowie bewährte Best Practices aus dem Bankensektor bieten hierfür wertvolle Orientierungspunkte, um nachhaltige und wirksame Compliance-Strukturen zu gestalten.

1. Einheitliche Risikoanalyse und Compliance-Methodik

Wie von der BaFin betont, bildet die Risikoanalyse das Kernstück einer effektiven Compliance-Organisation und Prävention. Versicherungsunternehmen sollten daher eine ganzheitliche, standardisierte Methodik für Risikoanalysen entwickeln, die sämtliche Compliance-Aufgabenbereiche abdeckt. Diese Methodik hat sich insbesondere im Bankensektor bewährt und bietet auch für Versicherungsunternehmen zahlreiche Vorteile. Sie sollte sämtliche relevante Compliance-Themen umfassen und innerhalb der Versicherungsunternehmen idealerweise auf internationaler Ebene, ggf. unter Ergänzung lokaler Vorschriften, anwendbar sein.

Eine standardisierte Methodik ermöglicht nicht nur eine konsistente Bewertung von Risiken, sondern schafft auch eine Grundlage für die Implementierung globaler Compliance-Standards. Ein zentralisiertes und standardisiertes Reporting ergänzt diese Methodik und ist ein wesentlicher Erfolgsfaktor. Ein solches Reporting sollte sämtliche relevanten Compliance-Aufgabenbereiche konsolidieren, um Transparenz, Vergleichbarkeit und Nachvollziehbarkeit zu gewährleisten. Dies erleichtert die Berichterstattung an die Geschäftsleitung und fördert die Einhaltung gesetzlicher und aufsichtsrechtlicher Vorgaben. Besonders ESG-Risiken stehen im Fokus, da sie aufgrund steigender regulatorischer Anforderungen zunehmend eine zentrale Rolle spielen. Eine systematische und konsistente Herangehensweise an ESG-Themen ermöglicht nicht nur die Erfüllung rechtlicher Vorgaben, sondern unterstützt auch die strategische Ausrichtung des Unternehmens in Richtung Nachhaltigkeit.

Darüber hinaus eröffnet ein konsistenter Ansatz in der Risikoanalyse und Berichterstattung die Möglichkeit, präventiv zu handeln, Risiken und etwaige Schwachstellen frühzeitig zu identifizieren und geeignete Maßnahmen und Kontrollen zu ergreifen. Eine enge Verzahnung von Risikoanalyse, Reporting und Maßnahmenplanung ist essenziell, um sowohl interne Anforderungen als auch die Erwartungen von Aufsichtsbehörden effektiv zu erfüllen.

2. Integration von ESG-Kriterien

Im Anschluss an die Risikoanalyse ist die Integration von ESG-Kriterien ein zentraler Schritt, um den regulatorischen Anforderungen gerecht zu werden und die Nachhaltigkeitsstrategie eines Versicherungsunternehmens zu stärken. Die Etablierung eines klar strukturierten ESG-Frameworks bildet dabei die Grundlage für eine systematische Umsetzung. Ein solches Framework sollte Richtlinien, Monitoring-Systeme und ein zentrales Berichtsformat umfassen, wie sie beispielsweise in der EU-Taxonomieverordnung (Art. 8) und im BaFin-Merkblatt zu Nachhaltigkeitsrisiken vom 13.1.2020 gefordert werden.

118 EU DORA-Verordnung (s. Fn. 17).
119 EU DORA-Verordnung (s. Fn. 17), Art. 28.
120 BaFin, MaGo (s. Fn. 1), Kap. 14.
121 BaFin, MaGo (s. Fn. 1), Kap. 14.
122 BaFin, MaGo (s. Fn. 1), Kap. 14.

Ein bewährter Best-Practice-Ansatz aus dem Bankensektor ist die Integration von ESG-Compliance in Kredit- und Investmentrichtlinien. Versicherungsunternehmen können diesen Ansatz auf ihre Kapitalanlageprozesse und die Gestaltung von Versicherungsprodukten übertragen. Die Bewertung von Kapitalanlagen anhand ESG-relevanter Kriterien trägt nicht nur zur Erfüllung regulatorischer Vorgaben bei, sondern ermöglicht es Versicherern auch, potenzielle Risiken frühzeitig zu erkennen und die langfristige Rentabilität ihrer Investitionen zu sichern. Im Bereich der Produktgestaltung kann ESG-Compliance dazu beitragen, innovative und nachhaltige Produkte zu entwickeln, die den Erwartungen von Aufsichtsbehörden und Kunden gleichermaßen entsprechen.

Ein weiterer essenzieller Aspekt ist die Förderung des Bewusstseins für Nachhaltigkeitsrisiken auf allen Unternehmensebenen. Regelmäßige ESG-bezogene Schulungen sollten ein integraler Bestandteil der Weiterbildungsmaßnahmen sein, um sicherzustellen, dass Mitarbeitende die Bedeutung von ESG-Risiken und deren Management verstehen. Diese Sensibilisierung stärkt nicht nur die Compliance-Kultur im Unternehmen, sondern trägt auch dazu bei, ESG-Aspekte in operative Entscheidungen zu integrieren. Ein Beispiel hierfür sind gezielte Kommunikationsmaßnahmen, die Mitarbeitende und Führungskräfte gleichermaßen einbinden und ESG-Themen in den Arbeitsalltag integrieren.

Die Kombination aus einem robusten ESG-Framework, der Integration in bestehende Prozesse und einer gezielten Schulungsstrategie schafft die Grundlage für ein zukunftsorientiertes Compliance-Management. Darüber hinaus wird die aktive Einbindung von ESG-Kriterien in die Unternehmensstrategie zunehmend zu einem Wettbewerbsfaktor, der sowohl die regulatorischen Risiken minimiert als auch die Reputation des Unternehmens stärkt.

3. Zentralisierte Compliance-Beratung (sog. Compliance Advisory)

Die zunehmende Komplexität regulatorischer Anforderungen erfordert eine strukturierte und zentralisierte Compliance-Beratung (sog. Compliance Advisory) innerhalb eines Versicherungsunternehmens. Eine zentrale Beratungsstruktur ermöglicht es, die spezifischen Risiken einzelner Gesellschaften oder Geschäftsfelder gezielt zu analysieren und effektive Maßnahmen zur Risikominderung zu entwickeln. Insbesondere bei international tätigen Versicherungsunternehmen kann diese Herangehensweise dazu beitragen, die Einhaltung globaler und lokaler Anforderungen effizient zu steuern.

Ein bewährter Ansatz aus dem Bankensektor ist die Zuordnung von spezialisierten Compliance-Officern zu einzelnen Gesellschaften oder Geschäftseinheiten. Diese Ansprechpartner fungieren als Schnittstelle zwischen den zentralen Compliance-Funktionen und den operativen Geschäftsbereichen. Durch die enge Zusammenarbeit mit den jeweiligen Geschäftsleitungen können sie spezifische Risiken präzise identifizieren und maßgeschneiderte Lösungen entwickeln. Dies ist insbesondere im Bereich der Geldwäscheprävention relevant, die als zentraler Bestandteil der Compliance-Beratung einheitlich koordiniert werden sollte.

Ein weiterer Vorteil dieser Struktur ist die Möglichkeit, differenzierte Anforderungen einzelner Geschäftsmodelle oder geografischer Regionen zu berücksichtigen, ohne die Einheitlichkeit der übergeordneten Compliance-Strategie zu gefährden. Eine bewährte Best Practice ist dabei die doppelte Funktion eines Compliance-Officers, der gleichzeitig als Geldwäschebeauftragter für die jeweilige Gesellschaft fungiert. Diese Kombination stärkt die operative Effizienz und gewährleistet eine klare Verantwortlichkeit, da der Funktionsinhaber dieser Position formal bei den zuständigen Aufsichtsbehörden anzuzeigen ist.

Zusätzlich trägt eine zentralisierte Beratungsstruktur dazu bei, Fragestellungen einheitlich zu beantworten, Ressourcen effizienter zu nutzen und Synergieeffekte zwischen den Gesellschaften zu schaffen. So können beispielsweise Erfahrungen und Best Practices aus einer Gesellschaft systematisch auf andere übertragen werden. Der regelmäßige Austausch zwischen den Compliance-Officern und der zentralen Compliance Funktion fördert zudem die Harmonisierung von Standards und Prozessen, was nicht nur regulatorische Anforderungen erfüllt, sondern auch die Resilienz der gesamten Compliance-Organisation stärkt.

Die zentrale Compliance-Beratung kombiniert damit die Vorteile einer einheitlichen Steuerung mit der Flexibilität dezentraler Anpassungen. Sie schafft die Grundlage für ein effizientes und risikobasiertes Compliance-Management, das den Anforderungen einer zunehmend regulierten und komplexen Versicherungswelt gerecht wird.

4. Anti-Financial Crime (AFC): Bündelung und Spezialisierung

Die Einrichtung einer spezialisierten Abteilung „Anti-Financial Crime" (AFC) hat sich im Bankensektor als effektive Maßnahme zur Bekämpfung von Finanzkriminalität etabliert. Diese kann Teil einer bestehenden Compliance-Funktion sein oder als eigenständige Funktion neben ihr etabliert werden. Versicherungsunternehmen können diesen bewährten Ansatz adaptieren, indem sie relevante Aufgaben und Kompetenzen in einer solchen zentralen AFC-Einheit bündeln. Eine solche Struktur ermöglicht die systematische Bearbeitung komplexer Herausforderungen und leistet einen entscheidenden Beitrag zur Erfüllung regulatorischer Anforderungen sowie zum Schutz der Unternehmensreputation.

a) Kernthemen einer AFC-Abteilung

Die Aufgabenfelder einer AFC-Abteilung umfassen in der Regel folgende Aufgabenschwerpunkte:

- *Geldwäscheprävention und Bekämpfung der Terrorismusfinanzierung* (*AML/CTF*): Entwicklung und Überwachung von Maßnahmen zur Identifikation und Verhinderung verdächtiger Transaktionen
- *Finanzsanktionen:* Sicherstellung der Einhaltung nationaler und internationaler Sanktionsregelungen, einschließlich automatisierter Screening-Prozesse
- *Betrugsprävention* (*Anti-Fraud, AF*): Identifikation und Minimierung von betrügerischen Aktivitäten, sowohl intern als auch extern

- *Bekämpfung von Bestechung und Korruption (Anti-Bribery & Corruption, AB&C)*: Entwicklung und Durchsetzung von Richtlinien zur Verhinderung korrupter Praktiken, ergänzt durch Schulungs- und Monitoring-Programme
- *Investigations und Whistleblowing*[123]

b) Aufgaben und Verantwortlichkeiten

Die zentrale AFC-Abteilung übernimmt Schlüsselaufgaben, die eine effektive Bekämpfung von Finanzkriminalität gewährleisten:

- *Standardisierung*: Entwicklung einheitlicher Standards und Richtlinien für alle Gesellschaften des Unternehmens, die eine konsistente Umsetzung sicherstellen
- *Fachexpertise*: Bereitstellung spezialisierter Unterstützung für lokale Compliance-Officer und Abteilungen, insbesondere bei komplexen internationalen Fragestellungen oder Verdachtsfällen
- *Überwachung und Kontrolle*: Zentrale Überwachung und Berichterstattung über finanzkriminalitätsbezogene Risiken und Maßnahmen, um Transparenz und Nachvollziehbarkeit zu gewährleisten

c) Best Practices und praktische Umsetzung

Ein zentraler Erfolgsfaktor ist die Anwendung eines risikobasierten Ansatzes, um Ressourcen gezielt auf Bereiche mit erhöhtem Risiko zu konzentrieren. Darüber hinaus spielen technologische Innovationen eine Schlüsselrolle:

- *Automatisierte Systeme*: Einsatz von KI-gestützten Screening-Tools zur Analyse von Kundenprofilen und Transaktionen. Diese Systeme verbessern die Effizienz und reduzieren die Fehleranfälligkeit manueller Prozesse.
- *Schulungsprogramme*: Regelmäßige Schulungen für Mitarbeitende sensibilisieren für Risiken im Bereich Finanzkriminalität und erhöhen das Bewusstsein für regulatorische Anforderungen.
- *Interdisziplinäre Zusammenarbeit*: Einbindung von Experten aus Compliance, IT und Recht zur Entwicklung ganzheitlicher Lösungen und zur Stärkung der Kontrollmechanismen.

d) Vorteile einer AFC-Abteilung für Versicherungsunternehmen

Die Bündelung aller relevanten Aufgaben in einer zentralen AFC-Abteilung oder einer eigenständigen Funktion bietet zahlreiche Vorteile:

- *Effizienz*: Risiken können frühzeitig identifiziert und priorisiert werden, wodurch Maßnahmen gezielt und schnell umgesetzt werden können.
- *Transparenz*: Die klare Strukturierung und zentrale Berichterstattung schaffen Vertrauen bei Aufsichtsbehörden, Geschäftspartnern und Kunden.
- *Wettbewerbsvorteil*: Die effektive Bekämpfung von Finanzkriminalität stärkt die Integrität des Unternehmens und schützt vor erheblichen finanziellen und reputationsbezogenen Schäden.

Die Übernahme des bewährten AFC-Modells aus dem Bankensektor bietet Versicherungsunternehmen eine praxisnahe und nachhaltige Möglichkeit, den gestiegenen Anforderungen im Bereich Finanzkriminalität gerecht zu werden. Eine spezialisierte AFC-Abteilung bildet nicht nur die Grundlage für die Einhaltung regulatorischer Vorgaben, sondern trägt auch maßgeblich zur langfristigen Stabilität und Integrität eines Unternehmens bei.

5. IT-Compliance: Digitalisierung und regulatorische Anforderungen

Die Einrichtung einer spezialisierten IT-Compliance-Abteilung stellt eine weitere zukunftsweisende Best Practice dar, um den wachsenden gesetzlichen und aufsichtsrechtlichen Anforderungen im digitalen Umfeld Rechnung zu tragen. Regulatorische Vorgaben wie die Versicherungsaufsichtlichen Anforderungen an die IT (VAIT), der Digital Operational Resilience Act (DORA) und der EU AI Act verdeutlichen die Notwendigkeit, Kompetenzen und Ressourcen gezielt zu bündeln. Eine solche Abteilung kann nicht nur die Einhaltung dieser Vorgaben sicherstellen, sondern auch digitale Kompetenzen beinhalten, um die Compliance-Funktion nachhaltig zu stärken und auf zukünftige Entwicklungen auszurichten.

a) Aufgaben und Schwerpunkte der IT-Compliance-Abteilung

Eine spezialisierte IT-Compliance-Abteilung hat mehrere zentrale Funktionen:

- *Umsetzung regulatorischer Anforderungen*: Die Abteilung gewährleistet die Einhaltung von Standards in den Bereichen IT-Governance, Informationssicherheit und Risikomanagement gemäß VAIT, DORA und EU AI Act. Dazu gehören u.a. die Implementierung von Notfallplänen, der Schutz vor Cyberangriffen und die Sicherstellung der Datenintegrität.
- *Digitale Kompetenzentwicklung*: Aufbau und Förderung digitaler Fähigkeiten innerhalb der Compliance-Funktion, um den Herausforderungen einer zunehmend technologisierten Versicherungsbranche gerecht zu werden.
- *Integration moderner Technologien*: Nutzung fortschrittlicher IT-Tools und Systeme zur Videoüberwachung und Berichterstattung. Solche Systeme unterstützen die Risikoidentifikation, -bewertung und -steuerung in Echtzeit und steigern die Effizienz der Compliance-Arbeit.

b) Praktische Umsetzung und Vorteile

- *Spezialisierte Teams*: Die Einrichtung spezialisierter IT-Compliance-Teams, die sich auf die Überwachung technologischer Vorgaben konzentrieren, fördert die Expertise und Effektivität in diesem Bereich.

123 S. unter 9. Investigations und Hinweisgebersystem.

- *Schulungen und Wissensaufbau*: Entwicklung von Programmen zur Fortbildung der Mitarbeitenden, die nicht nur die regulatorischen Anforderungen, sondern auch technologische Grundlagen und Trends vermitteln.

- *Strategische Verknüpfung*: Enge Zusammenarbeit zwischen IT-Compliance, IT-Abteilung und anderen Compliance-Bereichen ermöglicht Synergien und fördert die konzernweite Verankerung digitaler Kompetenzen.

- *Proaktive Überwachung*: Implementierung automatisierter Monitoring-Systeme zur frühzeitigen Erkennung von Risiken und Abweichungen sowie zur effizienten Einhaltung regulatorischer Vorgaben

Die Verbindung von technologischem Know-how mit regulatorischer Expertise schafft die Grundlage für eine zukunftsfähige Compliance-Funktion. Eine IT-Compliance-Abteilung kann nicht nur bestehende Anforderungen erfüllen, sondern auch innovative Technologien wie künstliche Intelligenz oder maschinelles Lernen in die Compliance-Prozesse integrieren. Diese Innovationen erhöhen die Effizienz, stärken die Prävention und eröffnen neue Möglichkeiten, Risiken proaktiv zu managen.

Eine spezialisierte IT-Compliance-Abteilung ist daher mehr als eine Reaktion auf die steigenden regulatorischen Anforderungen – sie ist eine strategische Investition in die Zukunftsfähigkeit des Unternehmens. Die Kombination aus technologischem Fortschritt und regulatorischer Konformität bietet Versicherungsunternehmen die Möglichkeit, sich in einer zunehmend digitalisierten und regulierten Branche erfolgreich zu positionieren.

6. Compliance international

Für international tätige Versicherungsunternehmen bietet die Einrichtung einer spezialisierten Abteilung „Compliance International" eine strategische Lösung, um die Einhaltung regulatorischer Vorgaben in ausländischen Gesellschaften effizient zu steuern. Diese Struktur ermöglicht eine zentrale und ganzheitliche Betreuung der ausländischen Compliance-Funktionen, während sie gleichzeitig lokale Besonderheiten berücksichtigt. Sofern das Versicherungsunternehmen seine weltweiten Geschäftsaktivitäten in Regionen unterteilt hat,[124] können diese unter der Abteilung Compliance International abgebildet werden. Mit einem solchen Ansatz können globale Themen wie Anti-Financial-Crime (AFC) und ESG-Compliance konsistent überwacht und gesteuert werden, ohne die Flexibilität und Expertise der lokalen Einheiten einzuschränken.

a) Hauptaufgaben einer Compliance-international-Abteilung

Die Hauptaufgabe einer solchen Abteilung liegt in der Steuerung und Koordination der Compliance- und Geldwäschebeauftragten in den internationalen Gesellschaften.

b) Verantwortlichkeiten einer Compliance-international-Abteilung

Dabei verfolgt sie einen hybriden Ansatz:

- *Lokale Verantwortung*: Die dezentralen Einheiten unter der Leitung eines lokalen Compliance- und Geldwäschebeauftragten bleiben für die Umsetzung und Überwachung nationaler Vorgaben verantwortlich. Dies gewährleistet, dass lokale regulatorische Anforderungen effektiv erfüllt werden und das spezifische Wissen vor Ort optimal genutzt wird.

- *Zentrale Steuerung*: Die zentrale Abteilung übernimmt die Harmonisierung von Prozessen, die Entwicklung einheitlicher Standards und die Überwachung der Einhaltung internationaler Compliance-Vorgaben. Zudem stellt sie Unterstützung bei der Implementierung konzernweiter Compliance-Strategien bereit.

7. Vorteile und praktische Umsetzung

- *Harmonisierung und Standardisierung*: Eine solche Abteilung „Compliance international" ermöglicht die Implementierung einheitlicher Standards und Methodiken, wodurch Prozesse über alle Standorte hinweg vergleichbar und steuerbar werden. Dies ist insbesondere bei globalen Themen wie ESG-Compliance, Finanzsanktionen und Geldwäsche- und Terrorismusfinanzierungsprävention von Vorteil bzw. unerlässlich, da diese Bereiche häufig internationale Dimensionen aufweisen. Gleichzeitig bleibt ausreichend Raum für die Berücksichtigung lokaler Besonderheiten, um regulatorische Risiken zu minimieren.

- *Effiziente Kommunikation*: Eine zentrale Koordination verkürzt die Kommunikationswege zwischen den internationalen Einheiten und der Konzernzentrale. Dies erleichtert die schnelle Anpassung an regulatorische Änderungen und sorgt für eine effiziente Weitergabe von Informationen und Entscheidungen.

- *Best-Practice-Transfer*: Durch den systematischen Austausch zwischen den lokalen Gesellschaften und der zentralen Einheit können Erfahrungen und bewährte Ansätze gezielt genutzt werden. Dies fördert die kontinuierliche Verbesserung der Compliance-Prozesse und stärkt die Gesamtleistung des Unternehmens.

- *Unterstützung bei aufsichtsrechtlichen Prüfungen*: Die zentrale Organisation erleichtert die Vorbereitung und Durchführung von Prüfungen durch lokale und internationale Aufsichtsbehörden. Konsolidierte und transparente Informationen ermöglichen eine kohärente Darstellung der Einhaltung regulatorischer Vorgaben und reduzieren den Aufwand für die lokalen Einheiten.

Eine Abteilung „Compliance international" verbindet zentrale Steuerung und ein einheitliches Reporting mit lokaler Expertise und schafft dadurch eine effiziente und flexible Organisationsstruktur. Sie gewährleistet nicht nur die Einhaltung globaler

124 Geläufig sind hier insbesondere Europa, EMEA, Asien, (Süd-, Mittel- und Nord) Amerika und Afrika.

und nationaler Compliance-Anforderungen, sondern stärkt auch die Resilienz und Wettbewerbsfähigkeit international tätiger Versicherungsunternehmen. Diese Struktur ist ein zentraler Baustein, um den Herausforderungen eines zunehmend globalisierten regulatorischen Umfelds gerecht zu werden und die strategische Positionierung des Unternehmens nachhaltig zu sichern.

8. Compliance-Monitoring: Etablierung eines einheitlichen Kontrollrahmens

Ein effektives Compliance-Monitoring[125] ist ein weiterer zentraler Bestandteil moderner Compliance-Funktionen. Versicherungsunternehmen stehen zunehmend vor der Herausforderung, eine systematische und standardisierte Überwachung zu etablieren, die regulatorischen Anforderungen gerecht wird und gleichzeitig Effizienz und Präzision gewährleistet. Ein solches Monitoring-System ermöglicht es, die in der MaGo[126] vorgeschriebenen Überwachungsaufgaben sowohl für inländische als auch internationale Gesellschaften nach einheitlichen Standards zu erfüllen. Der Fokus liegt dabei auf einem ganzheitlichen und risikobasierten Kontrollrahmen, der die Einhaltung interner und externer Vorgaben sicherstellt.

a) Wesentliche Elemente des (aufsichts-)rechtlichen und internen Compliance-Monitorings

Ein gut strukturiertes Compliance-Monitoring umfasst die systematische Überprüfung der Einhaltung von Gruppenvorgaben, externen regulatorischen Anforderungen und spezifischen Compliance-Normen. Die Integration konzernweiter Standards erleichtert die Vergleichbarkeit und Steuerung der Compliance-Performance. Wesentliche Vorteile eines solchen Rahmens sind:

- *Einheitliche Überwachungsstandards:* Vergleichbare Kontrollmechanismen über alle Standorte hinweg fördern die Konsistenz und Transparenz.
- *Ressourcenoptimierung:* Eine risikobasierte Steuerung der Überwachungsintensität ermöglicht die effiziente Allokation von Ressourcen und berücksichtigt den Proportionalitätsgrundsatz.
- *Frühzeitige Risikoerkennung:* Ein strukturierter Kontrollansatz deckt Schwachstellen und potentielle Abweichungen frühzeitig auf, wodurch präventive Maßnahmen proaktiv ergriffen werden können.

b) Praktische Umsetzung

Die erfolgreiche Umsetzung eines zentralisierten Compliance-Monitorings erfordert spezifische Maßnahmen und Technologien:

- *Zentralisiertes Monitoring*: Entwicklung eines einheitlichen Überwachungs-frameworks, das alle relevanten Compliance-Bereiche, einschließlich Finanzsanktionen, Geldwäsche- und Terrorismusfinanzierungsprävention, ESG-Compliance und Produkttransparenz, abdeckt.
- *Automatisierte Tools und Systeme*: Einsatz digitaler Lösungen zur Echtzeit-Überwachung und Erstellung standardisierter Berichte, um Effizienz und Genauigkeit zu steigern
- *Regelmäßige Reviews*: Durchführung periodischer Reviews und Überprüfungen, die zentrale Risikobereiche fokussieren und den lokalen Einheiten unterstützend zur Seite stehen
- *Normenkontrolle*: Sicherstellung der Einhaltung gruppenweiter Vorgaben, die gleiche Qualitätsstandards in allen Einheiten gewährleisten

Ein strukturiertes Compliance-Monitoring bietet Versicherungsunternehmen die Möglichkeit, regulatorische Anforderungen systematisch und risikobasiert zu überwachen. Durch die Harmonisierung von Prozessen und die Integration automatisierter Technologien können Ressourcen effizient genutzt und Risiken frühzeitig adressiert werden. Ein einheitlicher Kontrollrahmen, inspiriert durch Best Practices aus dem Bankensektor, gewährleistet die notwendige Flexibilität und stärkt gleichzeitig die Resilienz der gesamten Compliance-Funktion.

9. Investigations und Hinweisgebersystem (sog. Whistleblowing): Effektive Aufklärung und rechtssichere Bearbeitung

Eine spezialisierte Abteilung für „Investigations" ist ein weiterer entscheidender Bestandteil eines umfassenden Compliance-Managements. Sie ermöglicht Versicherungsunternehmen, Verdachtsfälle und Hinweise aus dem Hinweisgebersystem systematisch und rechtskonform zu bearbeiten.[127]

Insbesondere bei anonymen Meldungen oder Hinweisen auf strafrechtlich relevante Sachverhalte bietet eine zentralisierte Struktur den Vorteil, Prozesse effizient und transparent zu gestalten.

a) Fokus und Aufgaben der Abteilung Investigations

Die Hauptaufgabe der Abteilung ist die Koordination und Bearbeitung aller Hinweise und Verdachtsfälle unter der Maßgabe der Rechtskonformität und einer umfassenden und gerichtsfesten Dokumentation. Die zentralen Aufgaben umfassen:

- *Koordination und Analyse*: Bündelung aller Hinweise aus internen und externen Quellen wie Hinweisgebersystemen und deren strukturierte Analyse
- *Rechtskonformität*: Sicherstellung, dass alle Ermittlungen im Einklang mit nationalen und internationalen rechtlichen Vorgaben erfolgen, einschließlich Datenschutz- und Arbeitsrecht
- *Internationale Zusammenarbeit*: Abstimmung mit lokalen Compliance- und Rechtsabteilungen, um länderspezifische Anforderungen zu berücksichtigen

125 Die Begrifflichkeiten unterscheiden sich hier. Bisweilen wird dies auch als Compliance-Assurance oder Compliance-Testing bezeichnet.

126 BaFin, Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo) (s. Fn. 1).

127 S. oben als Kernaufgabe einer AFC-Abteilung.

b) Praktische Umsetzung und Best Practices

Die effiziente Durchführung von Untersuchungen erfordert klare Strukturen und spezialisierte Werkzeuge:

- *Strategische Analyse*: Analyse des globalen Umfelds und des betroffenen Bereichs sowie Festlegung der strategischen Vorgehensweise (Was ist das Ziel der Untersuchung? Was ist der Untersuchungsgegenstand? etc.).
- *Standardisierte Prozesse*: Entwicklung eines Workflows für die Bearbeitung von Verdachtsfällen, einschließlich Eskalationsmechanismen und Nachhalten des jeweiligen Bearbeitungsstatus
- *Einsatz von Technologien*: Nutzung forensischer Analyse-Tools und digitaler Plattformen zur effizienten Dokumentation und Nachverfolgbarkeit
- *Interdisziplinäre Teams*: Einbindung von Fachkräften aus Compliance, Recht, IT und Personalwesen zur umfassenden Analyse und Bearbeitung von Verdachtsfällen
- *Berichterstattung*: Regelmäßige und transparente Berichte an die Geschäftsleitung und den Aufsichtsrat, um Vertrauen und Nachvollziehbarkeit zu fördern
- *Remediation-Prozess*: Welche Konsequenzen, Schwachstellen und Schlussfolgerungen haben sich ergeben bzw. wurden identifiziert? Auslöser der Investigation (personell oder prozessual)? Ableitung einer optimalen Zielstruktur (Ist-/Soll-Operationalisierung).

Eine spezialisierte Investigations-Abteilung schafft eine transparente und rechtskonforme Struktur zur Bearbeitung von Verdachtsfällen. Dies stärkt nicht nur die Compliance-Kultur, sondern auch das Vertrauen von Mitarbeitenden und externen Stakeholdern in die Integrität des Unternehmens. Gerade im Rahmen von Hinweisgebersystemen und internationalen Anforderungen ist eine solche Abteilung von zentraler Bedeutung, um die Reputation und rechtliche Sicherheit des Unternehmens zu gewährleisten.

10. Technologieeinsatz und Automatisierung

Der gezielte Einsatz moderner Technologien hat das Potential, die Effizienz und Effektivität von Compliance-Funktionen signifikant zu steigern. Automatisierte Screening-Tools für Finanzsanktionen, Geldwäsche- und Terrorismusfinanzierungsprävention, KI- und ML-gestützte Analysen zur Erkennung von Diskriminierungsrisiken sowie digitale Plattformen zur Überwachung von ESG-Kriterien gehören heute zu den unverzichtbaren Werkzeugen moderner Compliance-Funktionen. Der Bankensektor dient hier als Vorbild, da der technologische Fortschritt dort bereits umfassend in die Compliance-Prozesse integriert wurde.

Für Versicherungsunternehmen empfiehlt es sich, zentrale digitale Plattformen einzuführen, die alle Compliance-Bereiche integrieren. Diese Systeme sollten nicht nur Risiken identifizieren, sondern auch präventive Maßnahmen vorschlagen, deren Wirksamkeit überwachen und kontinuierlich verbessern. Automatisierung reduziert den manuellen Aufwand erheblich und ermöglicht es Compliance-Teams, sich auf strategische Kernaufgaben wie Risikoanalysen, die Entwicklung neuer Richtlinien oder die Implementierung von regulatorischen Änderungen zu konzentrieren.

Die Vorteile des Technologieeinsatzes in der praktischen Umsetzung lassen sich wie folgt zusammenfassen:

- *Automatisierung von Routineaufgaben*: Tools für Transaktionsüberwachung, Kunden-Screening und Berichterstattung verringern die Fehleranfälligkeit und beschleunigen die Prozesse.
- *Datenintegration und Echtzeitanalyse*: Digitale Plattformen erlauben eine konsolidierte Sicht auf Compliance-Risiken und fördern proaktives Handeln durch Echtzeit-Datenanalysen.
- *KI-gestützte Entscheidungsunterstützung*: Künstliche Intelligenz identifiziert Muster, die auf potentielle Risiken hinweisen, und unterstützt bei der Priorisierung von Maßnahmen.[128]
- *Effizienzsteigerung*: Durch Automatisierung werden Ressourcen freigesetzt, die auf komplexere und strategische Aufgaben ausgerichtet werden können.

11. Schulungen und kulturelle Verankerung

Neben technologischen Lösungen ist die kontinuierliche Schulung der Mitarbeitenden ein Schlüsselfaktor für eine erfolgreiche Compliance-Funktion. Schulungsprogramme sollten praxisnah gestaltet sein und sowohl klassische Themen wie Geldwäsche- und Terrorismusfinanzierungsprävention, Datenschutz und Produktsicherheit als auch neuere Bereiche wie ESG-Compliance, KI-/ML-Ethik und digitale Risiken umfassen. Best Practices zeigen, dass Unternehmen mit gut geschulten Mitarbeitenden und einer starken Compliance-Kultur weniger häufig regulatorische Verstöße begehen.

Darüber hinaus ist es essenziell, Compliance fest in der Unternehmenskultur zu verankern. Eine „Compliance-by-Design"-Philosophie stellt sicher, dass regulatorische Anforderungen bereits in der Entwicklungsphase neuer Produkte und Prozesse berücksichtigt werden. Klare Kommunikationswege, die Vorbildfunktion der Führungskräfte und ein kontinuierliches Engagement für Integrität und Transparenz fördern das Verständnis und die Akzeptanz von Compliance-Maßnahmen auf allen Ebenen des Unternehmens.

Schlüsselmaßnahmen zur Förderung der Compliance-Kultur sind insbesondere die folgenden:

- *Regelmäßige Schulungen*: Mitarbeitende auf allen Ebenen sollten kontinuierlich geschult werden, um sicherzustellen, dass sie die sich wandelnden regulatorischen Anforderungen verstehen und anwenden können.
- *Führungskräfte als Vorbilder*: Führungskräfte spielen eine zentrale Rolle bei der Etablierung einer Kultur der Integrität und Transparenz. Ihr Verhalten beeinflusst die Akzeptanz von Compliance-Maßnahmen im gesamten Unternehmen.

128 S. für Risiken beim Einsatz von KI oben unter 5. Künstliche Intelligenz und algorithmische Verantwortung.

- *Integration in die Unternehmensstrategie*: Compliance sollte nicht als isolierte Aufgabe, sondern als integraler Bestandteil der strategischen Ausrichtung des Unternehmens verstanden werden.

Die steigenden regulatorischen Anforderungen erfordern innovative und flexible Lösungen, die auf einer Kombination aus Technologie, Schulung und kultureller Verankerung beruhen. Der gezielte Einsatz von Automatisierung und modernen Technologien schafft Effizienzgewinne, während kontinuierliche Schulungsprogramme das Bewusstsein und die Kompetenzen der Mitarbeitenden stärken. Eine starke Compliance-Kultur, die von der Führung vorgelebt wird, sichert die langfristige Integration von Compliance in alle Geschäftsprozesse.

Versicherungsunternehmen, die diese Ansätze adaptieren und an ihre spezifischen Gegebenheiten anpassen, können nicht nur regulatorische Vorgaben effizient erfüllen, sondern sich auch einen Wettbewerbsvorteil in einem zunehmend anspruchsvollen Markt verschaffen. Die Balance zwischen technologischem Fortschritt und menschlichem Engagement wird dabei entscheidend sein, um die Herausforderungen der Zukunft erfolgreich zu meistern.

IV. Gesamtfazit und Ausblick

Die steigenden regulatorischen Anforderungen stellen Versicherungsunternehmen vor die Aufgabe, ihre Compliance-Funktionen effizient, flexibel und nachhaltig weiterzuentwickeln. Der Schlüssel liegt in der Kombination zentraler Steuerung und dezentraler Anpassungsfähigkeit, um die vielfältigen Herausforderungen in Bereichen wie IT-Compliance, Geldwäsche- und Terrorismusfinanzierungsprävention, ESG-Compliance und internationaler Regulierung erfolgreich zu bewältigen.

Einheitliche Risikoanalysen, zentralisierte Screening-, Beratungs- und Monitoring-Strukturen sowie spezialisierte Abteilungen wie „Anti-Financial Crime" und „Investigations" schaffen die Grundlage für eine wirksame Compliance-Organisation. Ergänzt durch moderne Technologien wie automatisierte Screening-Tools, KI- und ML-gestützte Analysen und integrierte digitale Plattformen können Versicherungsunternehmen Effizienzgewinne und damit signifikante Kosteneinsparungen erzielen, Risiken frühzeitig erkennen und regulatorische Vorgaben proaktiv umsetzen.

Gleichzeitig ist die Schulung von Mitarbeitenden und die Verankerung von Compliance in der Unternehmenskultur unverzichtbar. Regelmäßige Trainingsprogramme und die Vorbildfunktion der Führungskräfte fördern das Bewusstsein für Compliance-Themen und stärken das Engagement aller Mitarbeitenden. Eine „Compliance-by-Design"-Philosophie, bei der regulatorische Anforderungen bereits in der Entwicklungsphase neuer Produkte und Prozesse berücksichtigt werden, sichert die langfristige Einhaltung gesetzlicher und aufsichtsrechtlicher Vorgaben und die strategische Wettbewerbsfähigkeit.

Zusammengefasst ergibt sich das Bild einer modernen Compliance-Funktion, die durch klare Strukturen, technologische Innovation und eine starke Kultur der Integrität geprägt ist. Versicherungsunternehmen, die diese Elemente erfolgreich kombinieren, werden nicht nur den aktuellen regulatorischen Anforderungen gerecht, sondern positionieren sich auch als zukunftsfähige und vertrauenswürdige Marktteilnehmer.

Die regulatorischen Anforderungen an Versicherungsunternehmen werden sich in den kommenden Jahren weiterentwickeln und zunehmend dynamischer und komplexer werden. Themen wie der EU AI Act, die zunehmende Bedeutung von ESG-Standards und die weitere Digitalisierung von Geschäftsprozessen stellen sowohl Herausforderungen als auch Chancen dar.

Zukünftig wird der Einsatz innovativer Technologien wie künstlicher Intelligenz, maschinellem Lernen und Blockchain eine noch größere Rolle spielen, um Compliance effizienter und präziser zu gestalten. Gleichzeitig werden globale Standards und länderübergreifende Regelwerke an Bedeutung gewinnen, was eine noch engere Zusammenarbeit zwischen zentralen und lokalen Einheiten erfordert.

Der Fokus wird verstärkt auf proaktiven Ansätzen liegen: Prävention wird die Reaktion auf Verstöße zunehmend ersetzen. Eine stärkere Integration von Compliance in die Unternehmensstrategie wird erforderlich sein, um regulatorische Vorgaben nicht nur zu erfüllen, sondern aktiv als Wettbewerbsvorteil zu nutzen. Unternehmen, die in der Lage sind, Compliance als strategischen Werttreiber zu etablieren, werden von regulatorischen Veränderungen profitieren, statt nur auf diese reagieren zu müssen.

In diesem Kontext wird die Fähigkeit, sich schnell und agil an neue regulatorische und technologische Entwicklungen anzupassen, entscheidend sein. Versicherungsunternehmen, die auf eine Kombination aus technologischem Fortschritt, einer starken Unternehmenskultur und einem effektiven Risikomanagement setzen, werden nicht nur regulatorische Sicherheit gewährleisten, sondern sich auch als Vorreiter in einer zunehmend regulierten und digitalisierten Branche positionieren können.