Prof. Dr. jur. Josef Scherer

Rechtsanwalt, Leitung des Internationalen Instituts für Governance, Management, Risk und Compliance und der Stabsstelle ESGRC der Technischen Hochschule Deggendorf. Mitglied diverser ISO- / DIN- / ASI-Normungsausschüsse und Beirat bei FIRM.

1.6.2026[1]

Legalitätspflicht als Kardinalpflicht und der Albtraum von Führungskräften, auch im Kontext von KI-Einsatz

- Managerenthaftung, Kardinalpflichten, Risikofrüherkennung und D&O-Versicherung im Lichte aktueller Rechtsprechung

#Managersicherheitspaket #Top Risks für Führungskräfte #Kardinalpflichten #IDW S 16 neu #Megatrends #Haftungsgefahren #KI-Einsatz

#Einsatzbereitschaft #Sicherheit #Erfolg #Verlässlichkeit #Struktur #Antifraglilität

[1] Diesen Artikel widme ich meinem Bruder zu seinem runden Geburtstag. Er schaffte es, als erfolgreicher CEO ohne Managerhaftungsfall wohlverdient in den Ruhestand zu gehen.

Einleitung / Summary

Nachfolgender Artikel[2] behandelt u.a. Megatrends, die aktuelle Lage in den Organisationen und den Wunsch der Führungskräfte[3], sicherer und erfolgreicher zu werden. Außerdem werden die Top Risks 2026 ff. und die Pain, aber auch die Governance-Pflichten der Führungskräfte dargestellt. Risikobasiertes Management, um die wichtigen Dinge richtig zu machen, könnte den steigenden Zahlen von Managerhaftungsfällen entgegenwirken. Die Entwicklung höchstrichterlicher Rechtsprechung[4] zum Thema „*Kardinalpflichten von Führungskräften, wissentliche Pflichtverletzung und Auswirkung auf (D&O-)Versicherungen*“ und die neuen Anforderungen an Risikofrüherkennung verschärfen die Lage. Jüngst wurde seitens der Rechtsprechung festgestellt, dass die *Beachtung der Legalitätspflicht, also von Compliance, zu den „wesentlichen Berufspflichten“ von Organen und sonstigen Führungskräften* gehört. Dies zeitigt enorme Auswirkungen auf die persönliche Haftungs-Verantwortung. Dies müssten auch die Verantwortlichen für Qualitäts-, Risiko-, Compliance-, KI- und Informationssicherheits-Managementsysteme beachten.

Führungskräfte werden derzeit im aktuellen Umfeld beruflich und privat von existenziellen Sorgen geplagt. Zukunfts- und Existenzängste[5] machen krank.[6]

Ein *Managersicherheitspaket* inkl. Absicherung des Privatvermögens[7] und ein *Integriertes (IT- / KI-) Governance-Compliance-Managementsystem* lösen effektiv und effizient die angesprochenen Probleme und bringen Sicherheit, Struktur, Resilienz, Zukunftsfähigkeit und Erfolg.

Why? Wir müssen vor die Lage kommen, sicherer und erfolgreicher werden

Unsere Organisationen, ihre Führungskräfte und sonstigen Beschäftigten müssen sicherer und erfolgreicher werden, um die Anforderungen der diversen Krisen und Transformationen zu bewältigen. Es ist effizienter, *vor die Lage* zu kommen, statt immer den aktuellen Hiobsbotschaften hinterherzujagen.

---

[2] Dieser Artikel fußt auf *Scherer, Seehaus,* Pflicht zu Governance mit Risikofrüherkennung, Resilienz, und Transformation als Kardinalpflicht von Organen und Führungskräften, ZInsO 2025, S.1515 ff., *Scherer*, Managersicherheitspaket für die Top-Risks 2026, 2026 und *Scherer, Romeike*, Vom Geschäftsrisiko zur persönlichen Haftung, 4/ 2026: alle Artikel *zum* kostenlosen Download im Internet unter https://www.risknet.de/elibrary/uebersicht/

[3] Gender-Hinweis: Zur besseren Lesbarkeit wird in diesem Text das generische Maskulinum verwendet. Es bezieht sich selbstverständlich auf Personen aller Geschlechter.

[4] Vgl. z.B. *BGH*, Urteil vom 19.11.2025, Az. IV ZR 66 / 25 („*ULLA-Versicherungsschutz-Ausschluss*“).

[5] Vgl. *Kolf* et al., „Struktureller Kollaps“ – Experten erwarten Rekord bei Großinsolvenzen, Handelsblatt.com, 8.1.2026.

[6] Vgl. *Lux* et al., Betriebliches Gesundheitsmanagement in Krisenzeiten, 2025, zum kostenlosen Download im Internet.

[7] Vgl. *Serbu, Hoffmann*, Asset Protection – Schutz für Unternehmens- und Privatvermögen, Praxis für Unternehmensnachfolge 2026, S. 17 ff. und *BGH*, Urteil vom 25.9.2025, Az. IX ZR 190 / 24, zur Insolvenzanfechtungsfestigkeit der Umwandlung einer Lebensversicherung nach § 815c Abs. 1 ZPO im Rahmen des zulässigen Höchstwerts (derzeit 7.000.- Euro pro Jahr und 340.000.- Euro Höchstbetrag. Vgl. außerdem das Urteil das LAG Köln, durch das die außerordentliche Kündigung eines Vertriebsleiters bestätigt und dieser zu 2 Jahresgehältern Schadensersatz an seinen Arbeitgeber verurteilt wurde: *LAG Köln*, Urteil vom 19.12.2024, Az. 8 Sa 830 / 22 (Back to back Vertriebsleiter), vgl. hierzu *Scherer, Romeike*, Vom Geschäftsrisiko zur persönlichen Haftung, 4/ 2026: *zum* kostenlosen Download im Internet: https://www.risknet.de/themen/risknews/vom-geschaeftsrisiko-zur-persoenlichen-haftung/

Da der hybride Krieg seitens diverser Nationen gegen Deutschland und Europa nicht mehr lediglich „Bedrohung“, sondern eingetretenes Ereignis ist,[8] sind nachfolgende Ausführungen zugleich auch ein *Beitrag zur Wehr- und Verteidigungsfähigkeit von Organisationen und Nationen*. Eine aktuelle Studie[9] des Instituts der Deutschen Wirtschaft zeigt, dass die Unternehmen nicht angemessen auf Verteidigung vorbereitet sind.

Aktuelle Lage und Top Risks 2026

Die aktuelle Lage in Zeiten multipler Krisen, diverser Transformationen aufgrund vielzähliger Megatrends[10] und zahlreicher kriegerischer Auseinandersetzungen steckt voller Risiken, wie der beispielsweise der *Global Risks Report 2026*[11], *CEO´s Annual Survey 2026*[12], *WEF Future of Growth Report 2026*[13] oder das *Allianz Risk Barometer 2026*[14] nahezu übereinstimmend zeigen. Viele neue Chancen[15] sind die Kehrseite dieser Medaille, wenn die sog. *Future Skills*[16] für *New Work, Zukunftstrends* und die Anforderungen der *Future of Jobs* frühzeitig entwickelt werden.[17]

Nach dem *Allianz Risk Barometer 2026* finden sich *Cyberrisiken, Business Continuity, Regulierung und KI* und auf den ersten vier Positionen der Unternehmens-Top Risks.[18]

Zitat: „Januar *2026: (…) In Deutschland bleiben Cyberangriffe und Geschäftsunterbrechungen auf Platz 1 und 2 – angesichts politischer und regulatorischer Unsicherheiten steigen Gesetzes- und Regulierungsänderungen auf den 3. Platz, während KI nun auf Platz 4 liegt.* (…)”[19]

Vgl. vertiefend unten Punkt 1.

---

[8] Zu hybrider Kriegsführung zählen u.a. Cyberangriffe, Spionage und Abhöraktionen, Sabotage, Desinformation und Propaganda etc., vgl. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 06.03.2025, Hybride Bedrohungen, abgerufen am 13.12.2025.

[9] Institut der Deutschen Wirtschaft (IW), Die Rolle der Privatwirtschaft in der Gesamtverteidigung Deutschlands, 2025, zum kostenlosen Download im Internet.

[10] Vgl. beispielhaft die Megatrend-Map des *Zukunftsinstituts* mit New Work, Future of Jobs, etc., 2025, zum kostenlosen Download im Internet.

[11] Zum kostenlosen Download im Internet.

[12] Zum kostenlosen Download im Internet.

[13] Zum kostenlosen Download im Internet.

[14] Zum kostenlosen Download im Internet.

[15] Nach dem neuen IDW S 16 (9/2025) zur Prüfung des Krisenfrüherkennungssystems nach § 1 StaRUG sind auch *Chancen* in die Unternehmensplanung aufzunehmen. Diese können u.U. auch Risiken im Rahmen der Bewertung der Risikotragfähigkeit kompensieren: *„(…) 45 In die Unternehmensplanung sind alle relevanten und wesentlichen künftigen Entwicklungen einzubeziehen. Das bedeutet, dass sowohl mögliche Chancen als auch Risiken adäquat in der Planung berücksichtigt werden müssen, um den Gesamtrisikoumfang des Unternehmens analysieren zu können. (…)*“.

[16] Vgl. *Stifterverband*, Future Skills 2030, 2025, zum kostenlosen Download im Internet.

[17] Infos zu diesen Themen finden sich im Internet.

[18] Vgl. *Scherer, Pothorn*, Integriertes IT- (KI-) Governance-Compliance-Managementsystem, 2026, zum kostenlosen Download im Internet.

[19] Allianz Risk Barometer 2026, zum kostenlosen Download im Internet.

Pain und Governance-Pflichten der Führungskräfte

Die Gefahren und Chancen angemessen zu identifizieren und zu bewerten und daraus angemessene Transformationsmaßnahmen abzuleiten, um langfristig die Existenz bzw. Resilienz der Organisation und ihrer Beschäftigten zu sichern,[20] gehört zu den *wesentlichen Governance-Pflichten*, die häufig unbekannt sind oder vernachlässigt werden.

Vgl. vertiefend unten Punkt 6.

Risikobasiertes Vorgehen, um die wichtigen Dinge richtig zu machen

Geschäftsführer, Vorstände, Aufsichtsräte, Abschlussprüfer, Revisoren, Compliance- und Risikomanager, IKS-Verantwortliche (sowie weitere Lines of Defense-Funktionen), sonstige Führungskräfte u.v.m. kümmern sich in Zeiten multipler Krisen und Transformation oft zu wenig um die wirklich wichtigen Dinge, weil sie nicht risikobasiert vorgehen.

Auch die (Arbeitssicherheits-, Umwelt-, Informationssicherheits-, Qualitäts-, Nachhaltigkeits-, Energieeffizienz- etc.-) Managementsystem-Verantwortlichen nebst deren Auditoren und Zertifizierern haben noch nicht zwingend realisiert, dass angemessene Governance mit Compliance- und Risikomanagement auch für das von ihnen betreute System die primäre und unverzichtbare Anforderung darstellt.[21]

Dies verursacht bei den betroffenen Organisationen häufig finanzielle Schäden, bringt sie nicht selten in vermeidbare existenzielle Schwierigkeiten und wird zumeist haftungsbewehrtes Missmanagement[22] der vielen verantwortlichen Führungskräfte darstellen. Dafür werden sich die genannten Funktionen bei Problemfällen in ihrem Verantwortungsbereich zu verteidigen haben.

Vgl. vertiefend unten Punkte 2 und 3.

Steigende Zahlen von Managerhaftungsfällen, Kardinalpflichten und Gefährdung des Versicherungsschutzes nach aktueller Rechtsprechung

Die Zahl der Managerhaftungsfälle steigt nach Auskunft des *Gesamtverbandes der Deutschen Versicherungswirtschaft* enorm.[23]

---

[20] Vgl. *Scherer*, Nachhaltige Führung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, Kapitel 6.11: Langfristige Existenzsicherung und Leistung.

[21] Vgl. *Scherer,* Das gefährliche (alte) Neue an der ISO 9001:2026 (Qualitäts-Managementsystem), 2026, zum kostenlosen Download im Internet.

[22] Vgl. *Scherer*, Das interessiert Kapitalgeber: Antifragilität und der „Achilleskörper" des Ordentlichen Kaufmanns, 2019, zum kostenlosen Download im Internet.

[23] Vgl. *Gesamtverband der Versicherer* (GDV), Haftungsrisiken für Manager und Berater steigen, 13.11.2025, zum kostenlosen Download im Internet.

Neben des nachgewiesen drastisch steigenden Risikos der persönlichen Haftung droht aufgrund des von aktueller Rechtsprechung[24] angenommenen Vorwurfs der „*Verletzung von Kardinalpflichten*“ und der daraus abgeleiteten Indikation[25] einer „*wissentlicher Pflichtverletzung*“ der Verlust des Versicherungsschutzes für Manager und Führungskräfte.

Nach der neuesten Entscheidung des *BGH*[26] bleiben die Ausführungen der bisherigen Judikatur zu Haftung von Führungskräften bei Pflichtverletzungen unberührt:

Zum einen kann ein Organ (Vorstand / Geschäftsführer) aus unterschiedlichen Gründen persönlich auf Schadensersatz haften, wenn er keine angemessene Risiko- oder Krisenfrüherkennung betreibt und dadurch die Gesellschaft schädigt (§§ 43 GmbHG, 93 AktG, etc.). Hier reicht bereits Fahrlässigkeit.

Eine neue Entscheidung des 5. Senats des *OLG Frankfurt*[27] führte unlängst aus, *jede Verletzung des Legalitätsprinzips* stelle eine *Kardinalpflichtverletzung* dar.[28]

Damit wurde die Compliance und das nach ständiger Rechtsprechung[29] verpflichtende Compliance-Managementsystem zur *haftungsbewährten* „*wesentlichen Berufspflicht*“ von Geschäftsführern und Vorständen, deren Befolgung Aufsichtsräte, Lines of Defense-Funktionen, u.U. auch Abschlussprüfer und sonstige Überwachungsfunktionen oder -Behörden ebenfalls haftungsbewährt zu überwachen haben.

Falls der Geschäftsführer / Vorstand nicht über eine D&O- (Managerhaftpflicht-Versicherung) verfügt, muss er persönlich den Schaden ersetzen (und kann so oder so gekündigt werden).

Sofern er versichert ist, stellte sich nun die Frage, ob die Versicherung die Zahlung unter Verweis auf einen Risikoausschluss in den Versicherungsbedingungen „*wegen wissentlicher Gesetzes- oder sonstiger Pflichtverletzung*“ verweigern kann.

Der *BGH* widersprach insoweit jüngst lediglich der Ansicht des 7. Senats des *OLG Frankfurt*, dass bei wissentlichen Pflichtverletzungen generell sogleich ein Risikoausschluss gemäß der Allgemeinen D&O-AGB *ULLA*[30] vorliege. Es müsse schon ein *wissentlicher* Pflichtverstoß *bzgl. einer konkret bezeichneten* Pflicht im Sinne eines direkten Vorsatzes oder gar Absicht[31] vorliegen.

---

[24] Vgl. *Scherer, Seehaus,* Pflicht zu Governance mit Risikofrüherkennung, Resilienz, und Transformation als Kardinalpflicht von Organen und Führungskräften, ZInsO 2025, S.1515 ff., zum kostenlosen Download im Internet.

[25] Vgl. hierzu *Seehaus*, Kurzanalyse des Urteils des BGH vom 19.11.2025 – IV ZR 66 / 25, ZInsO 2026, S. 899 ff..:

[26] *BGH*, Urteil vom 19.11.2025, Az. IV ZR 66 / 25 („*ULLA-Versicherungsschutz-Ausschluss*“).

[27] *OLG Frankfurt*, Urteil vom 20.11.2025, Az. 5 U 15 / 25 („*Verstoß gegen Legalitätsprinzip ist Kardinalpflichtverletzung und rechtfertigt außerordentliche Kündigung eines Geschäftsführers*“).

[28] […] und rechtfertige im konkreten Fall eine außerordentliche Kündigung des Geschäftsführers.

[29] Vgl. *LG München* (Neubürger), *OLG Nürnberg* (Tankstellenpächter) und diverse *BGH*-Entscheidungen, kommentiert in *Scherer,* Compliance-Managementsystem nach DIN ISO 37301, DIN Media, 2022, Kapitel Einleitung.

[30] ULLA: Versicherungsbedingungen für die Vermögensschadenshaftpflichtversicherung von Unternehmensleitern und Leitenden Angestellten

[31] Dolus directus 2. Grades (Wissentlichkeit) oder 1. Grades (Absicht).

Fahrlässigkeit oder ein bloßes „für-möglich-halten-und-sich-damit-abfinden“[32] reiche nicht.

Zu den Kardinalpflichten führte der *BGH* nichts aus. Somit bleibt es bei der Rechtsprechung, dass eine Kardinalpflichtverletzung eine wissentliche Pflichtverletzung indiziert.[33]

Streitigkeiten mit dem Versicherer und das Risiko, dass der Versicherer sich erfolgreich – oder sogar zu Unrecht unter Vorspiegelung einer falschen Rechtslage, was leider immer wieder mal passiert - auf einen Risikoausschluss beruft, sollten vermieden werden.

Wenn die Organe und Führungskräfte über ein angemessenes (u.U. sogar zertifiziertes) Compliance-Managementsystem mit fortschrittlichem Rechtskataster und kompetenter externer Unterstützung darlegen können, dass sie zum einen ihre Pflichten kennen und über Implementierung von entsprechenden Aktivitäten in die Prozesse auch beachten wollen, wird sich ein Versicherer schwer tun, eine *wissentliche* Pflichtverletzung nachzuweisen.

Vgl. vertiefend unten Punkt 13.

Verantwortliche Führungskräfte im Fokus von Ermittlungen: Fallbeispiele

Es gibt zahllose Fälle mit Verurteilungen von Organen, Führungskräften, aber auch unterhalb der Führungsebene bis hin zu Werkstudenten, Azubis und Praktikanten, die beweisen, dass hier nicht nur theoretische Probleme erörtert werden.

Im Fall „*Müller Brot*" wurden im Münchner Raum laut Medien strafrechtlich Ermittlungen auch gegen den *Qualitätsmanagement-Beauftragten* und den *Produktionsverantwortlichen* geführt.[34]

Beim „*Love-Parade*“-Fall wurde gemeldet, dass auch gegen die *Vorgesetzten der verantwortlichen Mitarbeiter* der Stadt wegen unterlassener Überwachung ermittelt werde.[35]

Auch der „*Transrapid*“-Fall[36] zeigte, dass bei entsprechenden Vorkommnissen (fehlende Prozessbeschreibungen!) nicht nur einzelne direkte Verursacher, sondern gleich mehrere Verantwortliche, insbesondere auch einfache *Vorgesetzte*, im Fokus von Ermittlungen, Anklagen und Verurteilungen stehen.

---

[32] Dolus eventualis.
[33] Vgl. hierzu *Seehaus,* Kurzanalyse des Urteils des BGH vom 19.11.2025 – IV ZR 66 / 25, ZInsO 2026, S. 899 ff..
[34] Vgl. *Ehrenstein*, Wenn "Gier und Preisdruck" über die Hygiene siegen, Welt, 12.02.2012, abrufbar unter https://www.welt.de/dieweltbewegen/article13864527/Wenn-Gier-und-Preisdruck-ueber-die-Hygiene-siegen.html.
[35] Vgl. *Puppe/Grosse-Wilde*, Die Legende von der Unaufklärbarkeit einer Katastrophe, Legal Tribune Online, 27.07.2020, abrufbar unter https://www.lto.de/recht/hintergruende/h/loveparade-prozess-fehler-gutachten-nicht-eingefuehrt-kausalitaet-schuld.
[36] Vgl. *Werner*, Transrapid-Unfall 2006: Bewährungsstrafen für zwei Fahrdienstleiter, Mitteldeutsche Zeitung, 03.03.2011, abrufbar unter https://www.mz.de/panorama/transrapid-unfall-2006-bewahrungsstrafen-fur-zwei-fahrdienstleiter-2268246.

Im Fall des eingestürzten „*Kölner Stadtarchivs*“ mit zwei Toten wurde das Verfahren 15 Jahre nach dem Einsturz vom *LG Köln* im August 2024 gegen die verbliebenen vier Angeklagten gegen Zahlung von Geldauflagen eingestellt.[37] Hauptverantwortlich seien zwei einstige Mitangeklagte, ein Baggerfahrer und ein Polier, gewesen, die aber nicht mehr verfolgt werden könnten, da der eine verhandlungsunfähig geworden und der andere verstorben sei.

Es reicht alleine, in die Maschinerie von Ermittlungen und behördlicher Verfahren nebst medialer Begleitung zu kommen, um am Ende – noch längst vor einem Urteil – psychisch und wirtschaftlich vernichtet zu sein.

Da hilft nur, bereits im Falle eines Verdachts aufgrund rechtssicherer Organisation nebst Dokumentation „per Knopfdruck“ beweisen zu können, sich zumindest bemüht zu haben, „*das Wichtige und Richtige richtig gemacht*“ zu haben.

Vereinfachte Grundzüge straf-, bußgeld- und zivilrechtlicher Haftung von Organisationen und Führungskräften

Manager (Organe und Führungskräfte) sowie alle sonstigen Beschäftigten können *strafrechtlich* persönlich bereits bei Fahrlässigkeit (z.B. fahrlässige Körperverletzung oder Tötung[38]) haften.

Bußgeldrechtlich können die Organisation selbst nach § 30 OWiG und Organe und exponierte Führungskräfte nach §§ 9, 130 OWiG haften.

Nach einer aktuellen Entscheidung des 31. Senats des *OLG Frankfurt* vom 21.10.2025[39], die die bisherige Linie der Rechtsprechung[40] verlässt, verschärft sich nun die oben beschriebene Bußgeldhaftung der Organisation für die Manager hin zu einer persönlichen Haftung enorm:

Wenn Organisationen nach § 30 OWiG i.V.m. Spezialgesetzen sanktioniert werden, können bzw. müssen[41] sie nach der neuen Rechtsprechung nach §§ 43 GmbHG oder 93 AktG bei Geschäftsführer oder Vorstand regressieren.

Ohne entsprechende Absicherung ist das gesamte Privatvermögen der Führungskraft im Feuer, vgl. hierzu unten Punkt 8.

Zivilrechtlich können Führungskräfte persönlich Dritten gegenüber direkt haften (Außenhaftung) oder der Organisation, in der sie tätig sind, gegenüber, wenn sie diese schädigen (Innenhaftung).[42]

---

[37] Vgl. *Fuchs*, Landgericht Köln stellt Strafverfahren gegen vier Angeklagte ein, Kölnische Rundschau, 06.08.2024, abrufbar unter https://www.rundschau-online.de/koeln/stadtarchiv-einsturz-landgericht-koeln-stellt-strafverfahren-ein-840620.

[38] Vgl. *Beck-aktuell*, Zugunglück bei Garmisch-Partenkirchen: Freispruch, 19.1.2026, zum kostenlosen Download im Internet: Selbst, wenn zum Schluss ein Freispruch rauskommt, ist das Strafverfahren mit meist begleitenden Medienberichten psychisch enorm fordernd.

[39] *OLG Frankfurt*, Urteil vom 21.10.2025, Az. 31 U 3 / 25 (BaFin-Bußgeld gegen AG (§ 30 OWiG i.V.m. 264 HGB) wegen unterlassenem Bilanzeid kann beim Vorstand (nach § 93 AktG) regressiert werden.

[40] Z.B. in Kartellsachen.

[41] So die *ARAG-Garmenbeck*-Entscheidung des *BGH*.

[42] Vgl. zu den diversen Haftungskonstellationen *Scherer*, Nachhaltige Führung von Organisationen (Governance) nach DIN ISO 37000, DIN Media Verlag, 2025, Kapitel 6.5, S. 138 ff.: Verantwortung, Delegation, Haftung.

Vgl. vertiefend unten Punkt 9.

Persönliche Haftung des Delegierenden und des Delegationsempfängers bei fehlerhafter Übertragung oder Wahrnehmung von Unternehmerpflichten (Pflichtendelegation)[43]

In der arbeitsteiligen Wirtschaftswelt wird üblicherweise von den primär- und letztverantwortlichen Organen (Vorstand / Geschäftsführer / etc.) auf Führungskräfte (Stabsstellen, Abteilungsleiter etc.) delegiert. Und diese delegieren oft weiter.

Auch auf Externe (Berater[44], Lieferanten, Auftragsdatenverarbeiter, Assembler, Veredler, verlängerte Werkbanken, etc.) wird häufig delegiert, wobei die nachfolgend dargestellten Grundsätze weitgehend auch hier gelten.

Bei Delegation wandelt sich die primäre Ausführungspflicht in eine Auswahl-, Instruktions- und *Überwachungs*pflicht bzgl. des Delegationsempfängers.

Deshalb umfasst der Begriff Governance neben Führung auch *Überwachung*.

Werden bei der sogenannten Pflichtendelegation Fehler gemacht, kann das zu einer Haftung sowohl des Delegationsempfängers als auch der Organisation und des Leitungsorgans führen (vgl. §§ 130, 9, 30 OWiG). Auch der *Aufsichtsrat*, der den Vorstand zu überwachen hat und Mängel in der Organisation nicht moniert und abstellen lässt, ist in der *Haftungsverantwortung* (§§ 116, 107 AktG).

Vgl. vertieft unten Punkt 11.

Höchste Brisanz für Unternehmen und Manager aufgrund weiterer aktueller Rechtsprechung: Der Albtraum einer Führungskraft

Im Rahmen der Grundsätze der *zivilrechtlichen Arbeitnehmerhaftung* schlug das in der Organisations-Praxis zu wenig beachtete Urteil des *LAG Köln*[45] bei Führungskräften hohe Wellen: Die außerordentliche Kündigung eines Vertriebsleiters wurde bestätigt und er wurde zu Schadensersatz in Höhe von 2 Jahresgehältern verurteilt, weil er Vorgaben im einschlägigen Handbuch nicht beachtet hatte und das Unternehmen dadurch erheblich schädigte.

Das Unternehmen muss entsprechende Organisationsvorgaben, wie Handbücher, Richtlinien, Kontrollmaßnahmen vorhalten, da andernfalls Unternehmen

---

[43] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, Kapitel 6.5, S. 138 ff.: Verantwortung, Delegation, Haftung.

[44] Interessant ist hierbei die 130-Millionen-Schadensersatz-Klage von *Continental* gegen die Anwaltskanzlei *Noerr*, in der wohl Continental ihren Beratern im Kontext mit dem Diesel-Skandal und Internal Investigations unzureichende Risikoanalysen (insbesondere zu Bußgeldrisiken, vgl. §§ 130, 30, 9 OWiG), Defizite in der Steuerung der Kooperation mit Ermittlungsbehörden u.v.m. vorwirft, vgl. *Schmidbauer,* Warum Continental gegen Noerr klagt, LTO vom 10.4.2026, im Internet verfügbar.

[45] *LAG Köln*, Urteil vom 19.12.2024, Az. 8 Sa 830 / 22 (Back to back Vertriebsleiter), vgl. hierzu *Scherer, Romeike*, Vom Geschäftsrisiko zur persönlichen Haftung, 4/ 2026: *zum* kostenlosen Download im Internet: https://www.risknet.de/themen/risknews/vom-geschaeftsrisiko-zur-persoenlichen-haftung/

und Geschäftsführer / Vorstand wegen Organisationsverschulden haften können, wenn fehlerhaftes Handeln oder Unterlassen[46] die Rechte Dritter verletzt.

Vgl. vertiefend unten Punkt 10.

Albtraum von Führungskräften auch im Kontext von KI-Einsatz

Aufgrund der völlig neuen *Rechtsprechung zur Haftung bei Benutzung von KI, die durch unrichtigen Output andere schädigt*,[47] führen die vom *LAG Köln* ausgesprochenen Grundsätze zur Arbeitnehmerhaftung zu einem *noch überwiegend unbekannten Haftungsrisiko für Führungskräfte auch im Kontext von KI-Einsatz*.

Auch hier gilt:

Das Unternehmen muss entsprechende Organisationsvorgaben[48], wie Handbücher, Richtlinien, Kontrollmaßnahmen vorhalten, da andernfalls Unternehmen und Geschäftsführer / Vorstand wegen Organisationsverschulden haften können, *wenn fehlerhafter KI-Output die Rechte Dritter verletzt*.

Und die Führungskräfte müssen sich an die Vorgaben halten, um nicht selbst zu haften.

Neue Anforderungen von Gesetzgeber und Wirtschaftsprüfern an Risikofrüherkennung

Risikofrüherkennung ist nicht nur eine der neuen Kardinalpflichten von Führungskräften, sondern unverzichtbare Voraussetzung für langfristige Existenzsicherung und ökonomische Nachhaltigkeit. Was eine angemessene Risiko- und Krisenfrüherkennung bedeutet, hat das IDW in einem neuen Standard IDW S16: 2025 zur Prüfung des Krisenfrüherkennungssystems nach § 1 StaRUG ausführlich und schon recht gut dargestellt.[49]

Vgl. vertiefend unten Punkt 4.

Abzuleitende Maßnahmen und Lösungsansätze

Organe und Führungskräfte sollten sich trotz des fordernden Tagesgeschäfts die Zeit nehmen, die Risikolage ihrer Organisation *und ihrer eigenen Person* unter den oben angeführten Aspekten zu reflektieren und eine gute

---

[46] Bei bestehender Handlungspflicht.

[47] *LG Hamburg*, Az. 324 O 461 / 25 und *OLG Hamm*, Az. 4 UKl 3 / 25 (Revision zum BGH zugelassen).

[48] Vgl. *Scherer, Pothorn*, Integriertes IT- (KI-) Governance-Compliance-Managementsystem, 2026, zum kostenlosen Download im Internet und *Scherer*, Nachhaltige Führung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, Kapitel 6.8: Daten und Entscheidungen. Es ist in nahezu allen Organisationen zu beobachten, dass bzgl. der sog. *IT- und KI-Literacy,* also dem Verständnis der Basics, ein gefährlicher Nachholbedarf herrscht.

[49] Vgl. zu den noch weiterbestehenden Mängeln beim IDW S 16: *Giesen, Gleißner, Haarmeyer, Romeike, Wieczorek*, (Arbeitskreis Krisenfrüherkennung), IDW S 16: Wichtige Klarstellungen und weiter offene methodische Klarstellung, ZInsO Heft 21, 2026.

unternehmerische und persönliche Entscheidung treffen: Zeitnahe Installation eines ***Managersicherheitspaketes*** **mit folgenden** ***Komponenten***:

Ein angemessener ***Risikomanagement-Prozess***[50] mit Analysen[51], Quantifizierung, Aggregation, Bewertung der Risikotragfähigkeit und priorisierte Risiko-Steuerung (auch bzgl. **der *persönlichen Risiken als Führungskraft***) sorgt für rechtssicheres risikobasiertes Vorgehen.

Aus den durchgeführten Analysen lassen sich an die aktuelle Situation angepasste zukunftssichernde ***Ziele, Strategie und Planung***[52] ableiten.

Die ***Governance- und Kardinalpflicht-Compliance*** sorgt mit einem die Kardinalpflichten der Organe und Führungskräfte umfassenden ***Rechtskataster***[53], das nicht nur dokumentiert, sondern auch die Pflichterfüllung steuert, für den wichtigsten Schritt in Richtung Managersicherheit.

Flankierend dazu wird der ***Versicherungsschutz*** mit Haftpflicht-, D&O-, Vermögensschadenshaftpflicht und Strafrechtsschutz-Versicherung und die Erfüllung der Obliegenheiten gecheckt und bei Bedarf optimiert.

Ein sog. „***Interaktionsmanagement***“[54] sorgt für rechtssichere Dokumentation und Umsetzung von Rollen, Aufgaben, Verantwortung, Zusammenarbeit, Aufsicht etc. der Organe und Leitungsfunktionen (Vorstand, Geschäftsführer, Aufsichtsrat, Gesellschafter, Stabsstellen, Beauftragten, Abteilungsleiter, etc.).

Die Implementierung oder Auditierung ***rechtssicherer Organisationsstrukturen***[55] mit Stellenbeschreibungen, lückenloser ***Pflichtendelegation***[56], etc. und vor allem angemessenem ***Prozessmanagement***[57] sorgt nicht nur für Sicherheit, sondern auch für Struktur.

Bestimmte *Bereiche* werden derzeit nahezu bei fast allen Organisationen / Unternehmen weiteren ***Handlungsbedarf*** zeigen:

- ***Financial Governance***[58] sorgt dafür, dass rechtliche und wirtschaftliche Pflichten, wie Wirtschafts- und Liquiditätsplanung, etc. dokumentiert erfüllt werden.

---

[50] Gemäß den Anforderungen des IDW S 16 neu und § 1 StaRUG. Vgl. auch *Scherer*, Nachhaltige Führung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, Kapitel 6.9: Risiko-Governance.

[51] Organisations- / Unternehmens- (Geschäftsmodell-), Umfeld-, Stakeholder-, Risiko- und Chancen- (SWOT) Analyse, vgl. *Scherer*, Nachhaltige Führung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, Kapitel 3.2: Analysen des Governance-Managementsystems.

[52] In Übereinstimmung mit den *Grundsätzen ordnungsgemäßer Planung* (GoP 2022). Vgl. *Scherer*, Nachhaltige Führung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, Kapitel 6.3: Strategie.

[53] Vgl. *Scherer*, Nachhaltige Führung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, Kapitel 4.4: Das Management aktueller, neuer und geänderter zwingender Governanace-Compliance-Verpflichtungen.

[54] Vgl. *Scherer*, Nachhaltige Führung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, Kapitel 4.3, S. 93 ff.: Interaktionsmanagement.

[55] Vgl. *Scherer*, Nachhaltige Führung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, Kapitel 3.2.2: Der aus Analysen abgeleitete Rahmen für die Organisation.

[56] Vgl. *Scherer*, Nachhaltige Führung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, Kapitel 4.2, S. 68 ff.: Governance und Delegation.

[57] Vgl. *Scherer,* Das gefährliche (alte) Neue an der ISO 9001:2026 (Qualitäts-Managementsystem), 2026, zum kostenlosen Download im Internet.

[58] Zur Financial Governance gehören neben Finanz-, Wirtschafts-, Liquiditäts- auch Investitions-Planung u.v.m., sowie auch konsequente Umsetzung der Planungen, vgl. *Scherer*, Nachhaltige Führung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, Kapitel 6.2.

- ***IT- und KI-Governance***[59] ist umfassend regulierte Führungsaufgabe.
- ***Business Continuity- und Krisen-Governance***[60] ist ebenfalls bei vielen Organisationen aufgrund des geänderten Umfelds ein bisher noch vernachlässigter Bereich.

Ein ***Integriertes (IT- / KI-) Governance-Compliance-Managementsystem***[61] beinhaltet und vernetzt die angesprochenen Komponenten in effektiver und zugleich effizienter Weise. Ein ***(externes) Internes Audit***[62] deckt Schwachstellen mit Handlungsbedarf auf und dokumentiert positiv die bereits existierenden angemessenen Komponenten positiv.

Einige auch für Compliance-Managementsysteme akkreditierte Zertifizierungsstellen bieten mittlerweile „im Kombipack" ***ISMS-CMS- Zertifizierungen*** nach DIN ISO 37301 und ISO 27001 und / oder ISO 42001 mit einem besonderem Scope des ***Audits* auf *(IT-/KI-) Governance-Compliance***[63] an.

Vgl. vertiefend unten Punkte 18 und 19.

Wertbeiträge

Die dargestellten Elemente des „Managersicherheitspakets" sorgen zum einen für ***Resilienz*** der Organisation, ihrer Führungskräfte und ihrer Beschäftigten.

Darüber hinaus werden ***transparente und effiziente Strukturen*** implementiert oder optimiert.

Schließlich werden auch noch *Sicherheit bei unternehmerischen Entscheidungen und Rechtssicherheit* gewährleistet: Durch ein Managersicherheitspaket mit Compliance kann – auch nach Ansicht des ehemaligen Vorsitzenden *BGH*-Richters *Raum*[64] – indiziert werden, dass etwaige, weiterhin nicht vermeidbare und sich ereignende Pflichtverletzungen nicht vorsätzlich oder wissentlich erfolgten. Das wirkt enthaftend und könnte auch bei Bedarf der Berufung des Versicherers auf einen vertraglichen Risikoausschluss entgegengehalten werden.

Nicht zuletzt werden dadurch auch ***persönliche Freiheit und Vermögen*** geschützt und das Risiko des Verlustes des Arbeitsplatzes wird geringer.

Vgl. vertiefend unten Punkt 20

---

[59] Vgl. *Scherer, Pothorn*, Integriertes IT- (KI-) Governance-Compliance-Managementsystem, 2026, zum kostenlosen Download im Internet und *Scherer*, Nachhaltige Führung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, Kapitel 6.8: Daten und Entscheidungen.

[60] Vgl. *Scherer*, Nachhaltige Führung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, Kapitel 6.11: Langfristige Existenzfähigkeit und Leistung.

[61] Vgl. *Scherer*, Nachhaltige Führung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025.

[62] Vgl. *Scherer*, Nachhaltige Führung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, Kapitel 9: Steuerung und Überwachung.

[63] In Anlehnung an DIN ISO 42001:2026, DIN ISO 37000 und ISO/IEC 38500.

[64] Vgl. *Scherer*, Compliance-Managementsystem nach DIN ISO 37301, DIN Media, 2022, Kapitel Einleitung, S. 23 ff..

1. Zuspitzung der Risikolage in Zeiten multipler Transformationen

Die weltweiten geopolitischen, ökonomischen und ökologischen Krisen in Zeiten grundlegender Transformation (technologisch, demografisch, ökologisch, sozial, regulatorisch) spitzen sich allmählich zu. Die Insolvenzzahlen steigen derzeit auf Höchstwerte.

Ein angemessenes Risikomanagement inklusive Risikofrüherkennung[65] muss auch Worst-Case-Szenarien berücksichtigen, alle Risiken angemessen quantifizieren, aggregieren, steuern und mit der Risikotragfähigkeit in Abgleich bringen.[66]

2. Fehlende Risikoorientierung in Leitung und Überwachung

Der aktuelle Handlungsdruck ist offenbar noch nicht bei den Geschäftsführern, Vorständen und Überwachern (Aufsichtsräten, Abschlussprüfern, Lines of Defense mit Interner Revision, Risiko- und Compliance-Management etc.), aber auch bei den diversen Arten von Auditoren angekommen.

Die *Untersuchung der Geschäftsberichte* von Organisationen indiziert häufig große Versäumnisse bei Governance, Risk und Compliance, also der ökonomischen Nachhaltigkeit. Bspw. existiert bei den Organen (Geschäftsführer, Vorstand, Aufsichtsgremien) und „Lines of Defense" i.d.R. noch wenig Verständnis bzgl. des Inhalts von sog. „Kardinalpflichten" und „risikobasierter Governance-Compliance", obwohl dies aktuell das Top-Risiko nahezu aller Organisationen verkörpert. Wenn das Leitungsorgan Führung und Überwachung (Governance) im Bereich der Resilienz und Transformation delegiert, die Delegationsempfänger jedoch nicht effektiv sind, stellt sich die Frage der Abgrenzung von fehlerhafter Delegation und Mitarbeiterexzess.

Worst-Case-Szenarien werden häufig bewusst oder aus Ignoranz ausgeblendet.[67] Oft fehlt auch echte Governance-, Risiko- und Compliance-Kompetenz und die GRC-Experten werden vor meist intuitiven Entscheidungen der Organe nicht beigezogen oder ernstgenommen.[68] Die Fachleute werden vielmehr mit operativen Aufgaben, wie Schulungen und bürokratischem Reporting[69] beschäftigt.

3. Unzureichende Umsetzung des risikobasierten Ansatzes

Auch der „*risikobasierte Ansatz*", nämlich sich nach angemessener Risikobewertung priorisiert um die wichtigen Dinge zu kümmern, ist zu wenig bekannt oder praktiziert: Wichtig sind primär die Vermeidung von Gefahr für Leib und Leben oder persönlicher Sanktionen Beschäftigter oder Dritter und von erheblichen finanziellen Einbußen, die die Risikotragfähigkeit beeinträchtigen.

---

[65] Vgl. hierzu ausführlich *Scherer/Seehaus*, Governance und Compliance nach § 1 StaRUG, 2024, RiskNET.de, abrufbar unter: *https://www.risknet.de/themen/risknews/kontinuierliche-risikoueberwachung-in-echtzeit/*, und *Romeike*, IDW ES 16 – Krisenfrüherkennung und Krisenmanagement nach § 1 StaRUG, 2025, RiskNET.de, abrufbar unter: *https://www.risknet.de/themen/risknews/krisenfrueherkennung-und-krisenmanagement-nach-1-starug/*.

[66] Vgl. *Scherer/Romeike/Gursky*, Mehr Risikokompetenz für eine neue Welt, RiskNET.de, 2021, abrufbar unter: *https://www.risknet.de/themen/risknews/mehr-risikokompetenz-fuer-eine-neue-welt/* und *Pätzold*, ZInsO 2025, 605 ff.

[67] Vgl. *Scherer/Romeike/Gursky*, Mehr Risikokompetenz für eine neue Welt, RiskNET.de, 2021, abrufbar unter: *https://www.risknet.de/themen/risknews/mehr-risikokompetenz-fuer-eine-neue-welt/*.

[68] Beispiel: Angemessene Business Judgment Rule-Gutachten *vor* relevanten Entscheidungen fehlen häufig. Bayer hat noch immer unter dem Kauf von Monsanto während laufender US-Product-Compliance-Prozessen zu leiden.

[69] Z.B. dem LKSG-Bericht, den die BAFA nicht ernsthaft einforderte bzw. dessen Ausbleiben nicht sanktionierte.

4. Virulente Rolle und Verantwortung der Wirtschafts- und Abschlussprüfer

Die Welt der Überwacher[70] schafft es offenbar trotz des hohen Ressourceneinsatzes nicht, die wirklich wichtigen Dinge effektiv zu steuern und zu überwachen. Die Rolle der Wirtschafts- und Abschlussprüfer als unabhängige Instanz zur Sicherstellung der Verlässlichkeit von Unternehmensabschlüssen gerät zunehmend unter Druck. Kritiker bemängeln eine strukturelle Nähe zu den geprüften Unternehmen sowie wirtschaftliche Abhängigkeiten, die die objektive Prüfungsqualität beeinträchtigen könnten.

Zitat:[71]

„(…) Wirtschaftsprüfer sind gemäß § 317 HGB und den Grundsätzen ordnungsmäßiger Abschlussprüfung (IDW PS 200 ff.) verpflichtet, risikoorientiert zu prüfen. Das bedeutet, dass insbesondere bei Unternehmen mit angespannten Bilanzkennzahlen und erhöhter Bestandsgefährdung das Risikomanagementsystem als zentrales Element einer Going Concern-Würdigung in den Fokus der Prüfung rücken muss. (…)

Gerade bei einem Konzern wie BayWa, der hochgradig abhängig ist von externen Einflussfaktoren wie Rohstoffpreisen, Zinssätzen oder regulatorischen Änderungen, ist ein solch vereinfachender Risikoblick grob fahrlässig und führt zu einer kompletten Risikoblindheit.

Es ist daher umso irritierender, dass Wirtschaftsprüfer ein solche Aussage im Risikobericht akzeptieren. Doch leider ist BayWa (PWC) hier keine Ausnahme.

Auch bei Wirecard (Ernst & Young), Lehman Brothers (Ernst & Young), Gerry Weber International (Ebner Stolz), Thomas Cook (Ernst & Young), Prokon Regenerative Energien (BDO), Luckin Coffee (Ernst & Young), Schlecker Drogeriemärkte (Grant Thornton, vormals Baker Tilly Roelfs), NMC Health (Ernst & Young), Greensill Capital (Grant Thornton), Carillion (KPMG), Steinhoff (Deloitte), Hypo Alpe Adria/ HETA (KPMG) und vielen weiteren Unternehmenskrisen und -pleiten waren die Wirtschaftsprüfer in einem kompletten Blindflug unterwegs. (…)“

5. Neue Anforderungen an Risikofrüherkennung und Krisenmanagement nach IDW S 16:2025

Im September 2025 veröffentlichte das Institut Deutscher Wirtschaftsprüfer den IDW S 16 mit Anforderungen an Risiko- und Krisenfrüherkennung und Krisenmanagement nach § 1 StaRUG. Dieser Standard[72] berücksichtigt im Gegensatz zum früheren Entwurf ES 16[73] nun erfreulicherweise besser[74] die Anforderungen des Gesetzgebers zu § 1 StaRUG und des DIIR Nr. 2 und verweist auf IDW PS 340:

Risiken müssen quantifiziert und aggregiert werden.[75] Methoden wie Szenarioanalysen mit z.B. Monte Carlo-Simulation und Bandbreitenplanung gehören inzwischen – nicht nur in der

---

[70] Vgl. *Scherer*, Die Welten der Überwacher, FIRM Jahrbuch 2017, S. 79 f., zum kostenlosen Download im Internet.

[71] Vgl. *Romeike*, Der Erwartungswert-Irrtum – Selbsttäuschung im Risikobericht der BayWa, 2025, RiskNET.de, abrufbar unter: *https://www.risknet.de/themen/risknews/der-erwartungswert-irrtum/*.

[72] Zitat: „(…) In diesem IDW-Standard legt das IDW vor dem Hintergrund des derzeitigen Stands von Theorie, Praxis und Rechtsprechung die Anforderungen des § 1 StaRUG an die Krisenfrüherkennung und an das Krisenmanagement nach § 1 StaRUG dar. Dieser Standard richtet sich primär an die Geschäftsleiter von haftungsbeschränkten Unternehmensträgern. Darüber hinaus ist IDW S 16 von Relevanz auch für Berufsträger mit (Annex-)Kompetenz zur Rechtsberatung (insb. Rechtsanwälte, Wirtschaftsprüfer, Steuerberater) (…)“

[73] Vgl. *Romeike*, IDW ES 16 – Krisenfrüherkennung und Krisenmanagement nach § 1 StaRUG, 2025, RiskNET.de.

[74] Vgl. zu den noch weiterbestehenden Mängeln beim IDW S 16: *Giesen, Gleißner, Haarmeyer, Romeike, Wieczorek*, (Arbeitskreis Krisenfrüherkennung), IDW S 16: Wichtige Klarstellungen und weiter offene methodische Klarstellung, ZInsO Heft 21, 2026.

[75] Zitat: *„(…) Risiken sind systematisch zu aggregieren und Interdependenzen bzw. Kombinationseffekte müssen analysiert und berücksichtigt werden. Dabei liegen der Detaillierungsgrad der Bewertung und die Darstellung der Risiken in der Verantwortung der Geschäftsleitung. Die Einzelrisiken sind (…) quantitativ einzuschätzen. Qualitative Ausführungen reichen nicht aus. Hierbei sind verschiedene Methoden denkbar, etwa eine Szenarioanalyse oder Planung in Bandbreiten. (…)“.*

Krise - zu den Anerkannten Regeln der Technik und gesetzlichen Anforderungen.[76]

Zu einer den rechtlichen Anforderungen genügenden und damit enthaftenden angemessenen Risiko- und Krisenfrüherkennung sind entsprechende Prozessabläufe und eine Verzahnung mit der Unternehmensplanung erforderlich.[77]

6. Wichtiges wird oft nicht gesehen: Governance und Top Risks 2026

Nach dem *Allianz Risk Barometer 2026* finden sich *Cyberrisiken, Business Continuity, Regulierung und KI* und auf den ersten vier Positionen der Unternehmens-Top Risks.[78]

Die sich ausdehnende und vielfältige Risikolandschaft[79] erfordert höchste Aktualität und Qualität bei Risikofrüherkennung und -management sowie der *Governance, also der „nachhaltigen compliance- und risikobasierten, gewissenhaften Führung und Überwachung von Organisationen*".[80]

Erschwerend wirkt sich bei der Erfüllung der Anforderungen aus Governance-Compliance aus, dass bereits mangels Legaldefinition Unklarheit bzgl. der Definition, des Inhalts und der konkreten Anforderungen von Governance in Wissenschaft und Praxis herrscht. Dadurch interpretieren die o.g. Verantwortlichen inklusive der Auditoren völlig willkürlich und unterschiedlich, was – wie nachfolgend aufgezeigt wird – zu fatalen Ergebnissen führt.

Auch die (Arbeitssicherheits-, Umwelt-, Informationssicherheits-, Qualitäts-, Nachhaltigkeits-, Energieeffizienz- etc.-) Managementsystem-Verantwortlichen nebst deren Auditoren und Zertifizierern müssten längst realisiert haben, dass angemessenes Compliance- und Risikomanagement auch für das von ihnen betreute System die primäre und unverzichtbare Anforderung darstellt.

I.d.R. sind nicht bestandsgefährdende Einzelrisiken, sondern die kumulierende Wirkung vieler Einzelrisiken fatal; daher ist eine methodisch fundierte Aggregation der Risiken wichtig.[81]

---

[76] Zitat: *„(…) 46 Einer gestiegenen Unsicherheit in Bezug auf den Eintritt einzelner prognostizierter Entwicklungen oder Auswirkungen eines volatilen Marktumfelds ist zumindest im Krisenfall durch Sensitivitätsanalysen oder Szenariorechnungen zu begegnen. Bei großen Unternehmen kann die Anwendung spezieller Verfahren (z.B. Monte-Carlo-Simulation) sinnvoll sein. (…)"*

[77] Zitat: *„(…) 54 Der Nachweis, dass eine KFE wirksam eingerichtet wurde, wird den Geschäftsleitern immer dann gelingen, wenn im Unternehmen die oben beschriebenen Prozesse zur systematischen Erfassung und Bewertung von Risiken und zur Unternehmensplanung implementiert sind und eine Verzahnung der Systeme mit der Unternehmensplanung vorliegt. (…)". Vgl. die „Grundsätze ordnungsgemäßer Planung".*

[78] Vgl. *Scherer, Pothorn*, Integriertes IT- (KI-) Governance-Compliance-Managementsystem, 2026, zum kostenlosen Download im Internet und *Scherer*, Nachhaltige Führung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, Kapitel 6.8: Daten und Entscheidungen.

[79] Vgl. oben, Einleitung.

[80] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000 - erfolgreich umsetzen, auditieren und reporten, DIN Media, 2025, Kapitel Einleitung.

[81] Vgl. *Romeike*, Qualitative Methoden zur Risikoaggregation sind eine Fiktion, 2019, abrufbar unter: *https://www.risknet.de/themen/risknews/qualitative-methoden-zur-risikoaggregation-sind-eine-fiktion/* sowie *Romeike*, Risikoaggregation wird zur Pflicht, 2025, abrufbar unter: *https://www.risknet.de/themen/risknews/risikoaggregation-wird-zur-pflicht/* und *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000 – erfolgreich umsetzen, auditieren und reporten, DIN Media, 2025, Kap. 6.9.

7. Governance-Compliance

Das *Governance-Compliance*-Managementsystem ist eine Aufbau- und Ablauforganisation, bestehend aus Komponenten (z.B. Rollen, Zielen, Ressourcen, Prozessabläufen, Delegationen und Interaktionen etc.), mit dem Zweck, eine Organisation bei Entscheidungen, Zielsetzung und Planung, Umsetzung sowie Steuerung und Überwachung zur *Erreichung zwingender und fakultativ gesetzter Ziele im Bereich Governance* zu unterstützen.

Governance umfasst dabei alle relevanten Bereiche/Funktionen/Prozesse einer Organisation.

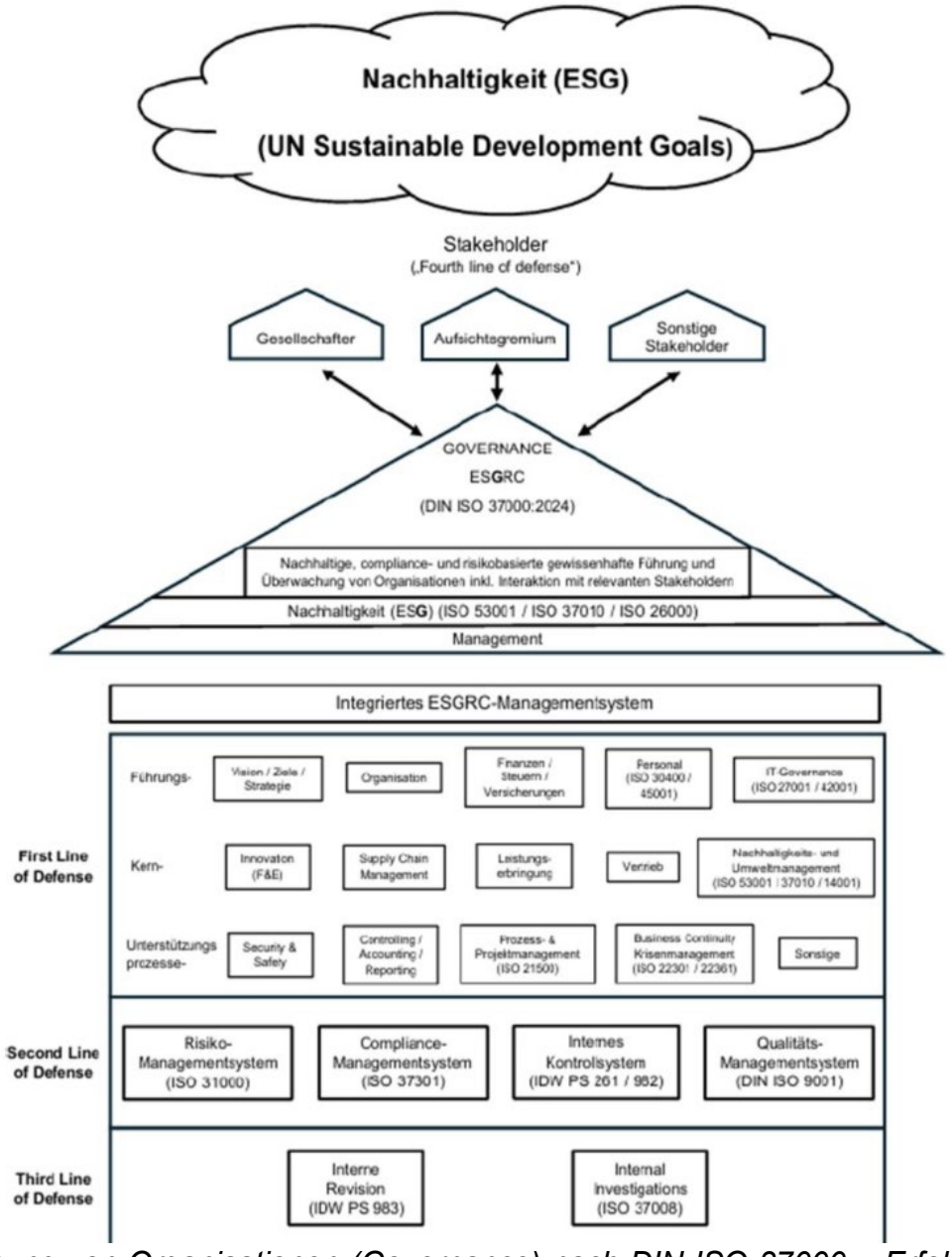

Abb. 1: Das „ESGRC-Haus“, *vgl. Scherer, Führung Nachhaltige und Überwachung von Organisationen (Governance) nach DIN ISO 37000 – Erfolgreich umsetzen, auditieren und reporten, DIN Media, 2025, Kapitel Einleitung.*

Die §§ 91 Abs. 2 und Abs. 3, 107 AktG, § 1 StaRUG mit der haftungsbewehrten Pflicht zur Risikofrüherkennung mit Quantifizierung, Aggregation, Steuerung, Abgleich mit Risikotragfähigkeit und Business Continuity- und Krisenmanagement (vgl. IDW S 16,[82] IDW PS 340 und DIIR Revisionsstandard Nr. 2) beziehen sich ebenso auf Governance-Risiken wie die Rechtsprechung. Diese fordert, ein Geschäftsführer oder Vorstand habe stets die *Pflicht zur Kenntnis der finanziellen und wirtschaftlichen Verhältnisse (kontinuierliche Risikofrüherkennung in Echtzeit) und Einleitung angemessener Maßnahmen bei krisenhaften Anzeichen*.[83]

§ 1 StaRUG verpflichtet zur Einrichtung eines angemessenen kontinuierlichen, in Echtzeit wirksamen Frühwarnsystems. Die zeitliche Dimension der Risikofrüherkennung wird in der Praxis oft unterschätzt. Die Bestimmung des Prognosezeitraums für die Insolvenzwahrscheinlichkeit (p_1) i.S.d. § 1 StaRUG orientiert sich an der insolvenzrechtlichen *Fortbestehensprognose*, nicht an der handelsrechtlichen *Fortführungsprognose*. InsO und StaRUG adressieren beide das *Fortbestehen des Rechtsträgers*, während es beim „going concern" (Fortführungsprognose) des HGB um die *Fortführung des Geschäftsmodells* geht.

Ausgehend von §§ 18, 19 InsO ist die Planung auf mindestens 12, i.d.R. auf 24 Monate oder sogar noch länger zu erstrecken.[84] Der Planungshorizont sollte sich innerhalb dieses Zeitrahmens befinden und sich nach der Größe und Komplexität des Unternehmens richten, da sich hieraus im Einzelnen die relevanten Stellgrößen und Einflüsse ergeben, die in der Planung zu berücksichtigen sind.

Das *OLG Nürnberg* entschied im Fall eines kleinen Unternehmens und ergänzte noch, der Geschäftsführer habe die *Pflicht, für ein angemessenes und wirksames Compliance-, Risiko-Management- und Internes Kontroll-System zu sorgen*.[85]

In diesem Fall ging es um den Angestellten bei einer kleinen Tankstelle mit wenigen Mitarbeitern, der offenbar die den Geschäftskunden gesetzten Kreditlimits z.T. ignorierte bzw. umging, wodurch es zu Zahlungsausfällen kam.

Als dies bekannt wurde, war ein Schaden von ca. einer 3/4 Mio. € entstanden. Der Geschäftsführer (Pächter der Tankstelle) wurde persönlich wegen Pflichtverletzung zu Schadensersatz an die Gesellschaft in dieser Höhe verurteilt.

Das *OLG Nürnberg* führte aus, er habe es pflichtwidrig unterlassen, für ein angemessenes und wirksames Compliance- und Internes Kontroll-Managementsystem zu sorgen.

Ein Geschäftsführer habe stets die „Pflicht zur Kenntnis der finanziellen und wirtschaftlichen Verhältnisse (kontinuierliche Risikofrüherkennung in Echtzeit) und Einleitung angemessener Maßnahmen bei krisenhaften Anzeichen".

Die Entschuldigung des Geschäftsführers, er habe ja gerade eine Stelle für einen Controller ausgeschrieben, der sich genau darum hätte kümmern sollen, aber in Zeiten von Fachkräftemangel habe er niemanden gefunden, erkannte das Gericht nicht an: Dann müsse er sich als Geschäftsführer halt persönlich darum kümmern.

Wichtig: *In diesem Fall ging es nicht um Insolvenz- oder Krisenvermeidung, sondern um die Pflicht zur generellen Schadensvermeidung*.[86]

---

[82] Vgl. *Romeike*, IDW ES 16 – Krisenfrüherkennung und Krisenmanagement nach § 1 StaRUG, 2025, RiskNET.de, abrufbar unter: *https://www.risknet.de/themen/risknews/krisenfrueherkennung-und-krisenmanagement-nach-1-starug/*.

[83] Vgl. z.B.: BGH, Versäumnisurt. v. 19.6.2012 – II ZR 243/11, ZInsO 2012, 1536 und BGH, Urt. v. 23.7.2024 – II ZR 206/22, ZInsO 2024, 1980.

[84] Vgl. IDW S 16. Noch weitergehend: *Bea/Dressler*, NZI 2021, 67, 70 – diese generell für eine Planung über 24 Monate.

[85] Vgl. OLG Nürnberg, Urt. v. 30.3.2022 – 12 U 1520/19, NZG 2022, 1058.

[86] Vgl. hierzu ausführlich: *Scherer/Seehaus*, Governance und Compliance nach § 1 StaRUG, 2024, RiskNET.de, abrufbar unter: *https://www.risknet.de/themen/risknews/kontinuierliche-risikoueberwachung-in-echtzeit/*.

8. Zunehmende persönliche Haftung von Geschäftsleitern und Funktionsträgern

Proportional zu den regulatorischen Anforderungen steigen die Haftungsrisiken für Organe (Aufsichtsräte, Vorstände, Geschäftsführer), exponierte Funktionen, wie Abteilungsleiter, Risiko- oder Compliance-Officer und Unternehmen enorm:

„Chefposten werden riskanter – mehr Klagen werden erwartet" „Spitzenpositionen sind auch mit einem wachsenden Risiko verbunden, Ziel eine Klage zu werden." […]

„Wir beobachten, dass Aufsichtsbehörden auf der ganzen Welt das Unternehmensverhalten schärfer überprüfen, wodurch Unternehmenslenker anfälliger für Untersuchungen, Strafen und Klagen werden."[87]

Der Gesamtverband der Deutschen Versicherungswirtschaft berichtet aktuell von einem Anstieg der D&O-Haftungsfälle im dritten Jahr mit aktuell 2.500 Fällen in 2024 und nennt als Ursachen die schlechte Konjunktur mit Anstieg der Insolvenzen und wachsende gesetzliche und compliancebezogene Anforderungen.[88]

9. Exkurs: Möglichkeiten für Führungskräfte, persönlich zu haften

Haftungsbereiche: Straf-, Ordnungswidrigkeiten- und Zivilrecht[89]

Zunächst ist zwischen Straf- und Ordnungswidrigkeitenrecht auf der einen Seite und Zivilrecht auf der anderen Seite zu unterscheiden.

Beispiel

Der Fall „O. J. Simpson"[90] illustriert diese Unterscheidung sehr schön: Strafrechtlich, wo es um Spezial- und Generalprävention geht und der Grundsatz „im Zweifel für den Angeklagten" (in dubio pro reo) besteht, wurde Simpson freigesprochen. Zivilrechtlich, wo es meist um Entschädigung geht und die Beweislast häufig gesetzlich oder via Rechtsprechung zu Lasten der Organisation oder des Schädigers ausgestaltet ist, kam es dagegen zu einer Verurteilung.

Haftung nach dem Straf- und Ordnungswidrigkeiten-Recht

Im Straf- und Bußgeldrecht gibt es vielfältige gesetzliche Regeln, die zu einer Haftung einer Führungskraft führen können:

Zunächst sind im Strafgesetzbuch viele Delikte genannt und in §§ 130, 30, 9 OWiG die Möglichkeit geregelt, dass bei Unternehmensbußgeldern auch eine Führungskraft persönlich sanktioniert werden kann. Dazu kommen weitere Straf- und Bußgeldregeln in Spezialgesetzen.

Manager (Organe und Führungskräfte) sowie alle sonstigen Beschäftigten können strafrechtlich persönlich bereits bei Fahrlässigkeit haften (z.B. fahrlässige Körperverletzung oder Tötung[91]) haften.

---

[87] Zitat aus: beck-aktuell, Allianz: Chefposten werden riskanter – mehr Klagen erwartet, 2024,
[88] Vgl. *GdV*, Haftungsrisiken für Manager und Berater steigen, 13.11.2025, zum kostenlosen Download im Internet.
[89] Vgl. *Scherer*, Nachhaltige Führung von Organisationen (Governance) nach DIN ISO 37000, DIN Media Verlag, 2025, Kapitel 6.5, S. 138 ff.: Verantwortung, Delegation, Haftung.
[90] Vgl. *Welt,* Der rätselhafte Fall des O. J. Simpson, https://www.welt.de/vermischtes/gallery111426499/Der-raetselhafte-Fall-des-O-J-Simpson.html (abgerufen am 14.08.2024).
[91] Vgl. *Beck-aktuell*, Zugunglück bei Garmisch-Partenkirchen: Freispruch, 19.1.2026, zum kostenlosen Download im Internet: Selbst, wenn zum Schluss ein Freispruch rauskommt, ist das Strafverfahren mit meist begleitenden Medienberichten psychisch enorm fordernd.

Sollte die Führungskraft bestraft oder persönlich mit einem Bußgeld sanktioniert werden, nutzt hier weder eine Rechtsprechung des Bundesarbeitsgerichts zur betrieblich veranlassten Tätigkeit[92] noch irgendeine Manager-Haftpflichtversicherung.

Lediglich über eine Strafrechtsschutzversicherung könnte sich der Betroffene einen besonders teuren aber hoffentlich auch besonders qualifizierten Strafverteidiger leisten.

Nach einer aktuellen Entscheidung des *OLG Frankfurt* vom 21.10.2025[93], die die bisherige Linie der Rechtsprechung[94] verlässt, verschärft sich nun die oben beschriebene Bußgeldhaftung für die Manager zu einer persönlichen Haftung enorm: Wenn Organisationen nach § 30 OWiG i.V.m. Spezialgesetzen sanktioniert werden, können bzw. müssen[95] sie nach der neuen Rechtsprechung nach §§ 43 GmbHG oder 93 AktG bei Geschäftsführer oder Vorstand regressieren.

Ohne entsprechende Absicherung ist das gesamte Privatvermögen der Führungskraft im Feuer.

Die Organe müssen sich daher bereits im Bußgeldverfahren gegen die Organisation angemessen „verteidigen“. In der Folge wird außerdem versucht werden, dass der Anspruch gegen die Organe wiederum über die D&O-Haftpflicht ersetzt wird.

Mittelbar kann damit die D&O die Verbandsgeldbuße gegen die Organisation erstatten, wenn eine solche Versicherung besteht und ihr der Einwand einer wissentlichen Pflichtverletzung i.S. der Versicherungsbedingungen durch ein angemessenes Compliance-Managementsystem abgeschnitten wird.

Zivilrechtliche Haftung

Bezüglich der zivilrechtlichen Haftung auf Schadenersatz ist zwischen „Außenhaftung“ gegenüber geschädigten Dritten und der „Innenhaftung“ gegenüber der Organisation (bei Schädigung des Arbeitgebers) zu unterscheiden.

Bei der Außenhaftung kommt eine vertragliche Haftung der Führungskraft mangels Vertrags mit den Geschädigten nicht in Betracht. Auch nicht über die Figur des Vertrags mit Schutzwirkung für Dritte oder Vertrag zugunsten Dritter.

Dagegen ist eine deliktische Haftung über § 823 Abs. 1 BGB bei Verletzung entsprechender Rechtsgüter oder auch gemäß § 823 Abs. 2 BGB in Verbindung mit Straf- oder sonstigen Schutzgesetzen durchaus denkbar.

Bzgl. der Haftung gegenüber der Organisation, die unter Umständen Dritten regresspflichtig ist oder eigene Schäden durch die Pflichtverletzung der Führungskraft hat, besteht die Möglichkeit der vertraglichen Haftung aus dem Dienstverhältnis beziehungsweise dem Arbeitsvertrag in Verbindung mit § 280 BGB.

Das Arbeitsrecht kann hier Haftungsschranken setzen**.** An dieser Stelle ist zum einen an ein mögliches Mitverschulden des Arbeitgebers zu denken und an die Beweislastregelung des § 619 a BGB: Das Verschulden der Führungskraft hat der Arbeitgeber zu beweisen.

---

[92] Vgl. *Huep*, Arbeitnehmerhaftung / 3.2.1 Betrieblich veranlasste Tätigkeit, in: Haufe.de, https://www.haufe.de/personal/haufe-personal-office-platin/arbeitnehmerhaftung-321-betrieblich-veranlasste-taetigkeit_idesk_PI42323_HI15222722@HI520113.html (abgerufen am 02.09.2024).

[93] *OLG Frankfurt*, Urteil vom 21.10.2025, Az. 31 U 3 / 25 (BaFin-Bußgeld gegen AG (§ 30 OWiG i.V.m. 264 HGB) wegen unterlassenem Bilanzeid kann beim Vorstand (nach § 93 AktG) regressiert werden.

[94] Z.B. in Kartellsachen.

[95] So die *ARAG-Garmenbeck*-Entscheidung des *BGH*.

Außerdem ist an die *Grundsätze zur Arbeitnehmerhaftung bei betrieblich veranlasster Tätigkeit mit innerbetrieblichem Schadensausgleich* zu denken:

Arbeitnehmerhaftung bei betrieblich veranlasster Tätigkeit

Bei leichter und mittlerer Fahrlässigkeit haftet der Arbeitnehmer nicht oder nur anteilig oder er hat einen Freistellungsanspruch gegen den Arbeitgeber. Nur bei grober Fahrlässigkeit oder Vorsatz haftet der Arbeitnehmer grundsätzlich voll, wobei sich sogar bei grober Fahrlässigkeit noch Haftungsreduktionsmöglichkeiten ergeben, vgl. sogleich unten.

Vorsatz i. S. von Dolus Eventualis liegt vor, wenn eine negative Folge für möglich gehalten und sich damit abgefunden wird.

Das Ergebnis einer entsprechenden Risikobewertung im Vorfeld könnte in diesen Fällen eine „negative Dokumentation" darstellen, die den Vorwurf des Vorsatzes untermauert, wenn keine sich umgehend ausschließenden Abhilfemaßnahmen durchgeführt wurden.

10. Das *LAG Köln* und der Albtraum einer Führungskraft

Weil ich es mir wert sein muss: Gehören Sie zur Risikogruppe?

Führungskraft? Ehrgeizig? Motiviert? Am Erfolg des Unternehmens und am eigenen Erfolg interessiert? Mittleren Alters? Verantwortung für andere (Familie) tragend? Sensibel bzgl. der eigenen Zukunft (Job-Sicherheit, finanzielle Absicherung der Familie und des eigenen Alters …)?

Dann vorab eine Warnung: Das nachfolgend dargestellte Urteil des *LAG Köln*[96], das eine einfache Führungskraft zu erheblichem Schadensersatz verurteilte und die Rechtmäßigkeit deren außerordentlicher Kündigung bestätigte, könnte Ihnen schlaflose Nächte bereiten.

Dieser Fall behandelt dabei nur eine von vielen Varianten, wie eine Führungskraft haften kann: [97]

Hintergrund und Zitate aus dem Urteil *LAG Köln*[98]:

Einer Führungskraft (Vertriebsleitet) wurde fristlos gekündigt und auf Schadensersatz in Höhe von 3 Millionen Euro verklagt, weil sie interne Vorgaben nicht beachtet hatte, um für das Unternehmen[99] ein günstiges Geschäft zu tätigen.[100]

Die Führungskraft, geboren 1964, war zu diesem Zeitpunkt verheiratet, unterhaltspflichtig und zuletzt als Vertriebsleiter Geschäftskunden zu einem durchschnittlichen Bruttomonatsgehalt von 8.433,33 EUR beschäftigt. Sein Vorgesetzter war der Leiter Vertrieb / Shared Service. Für den Vertriebsleiter und seinen Vorgesetzten bestand eine Eigenschadenversicherung, die Schäden des Arbeitgebers bis zu 500.000,00 EUR abdecken sollte.

Der Vertriebsleiter verfügt neben dem selbst bewohnten und mit einer Grundschuld belasteten Einfamilienhaus lediglich über Vermögen in Form von Altersvorsorgeverträgen. Sein damaliges Nettoeinkommen von 4.725,64 EUR wird in Höhe von 3.534,66 EUR für

---

[96] *LAG Köln,* Urteil vom 19.12.2024[96] – 8 Sa 830/22 („Backtoback Vertriebsleiter"), Nichtzulassungsbeschwerde anhängig beim BAG unter 8 AZN 163/25.

[97] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance), DIN Media, 2025, Kapitel 6.5, S. 138 ff.: Verantwortung, Delegation, Haftung.

[98] *LAG Köln,* Urteil vom 19.12.2024[98] – 8 Sa 830/22, Nichtzulassungsbeschwerde anhängig beim BAG unter 8 AZN 163/25.

[99] Ein *kommunales Energieversorgungsunternehmen.*

[100] Vgl. hierzu *Scherer, Romeike*, Vom Geschäftsrisiko zur persönlichen Haftung, 4/ 2026: zum kostenlosen Download im Internet: https://www.risknet.de/themen/risknews/vom-geschaeftsrisiko-zur-persoenlichen-haftung/

durchlaufende Verbindlichkeiten verbraucht. Sein pfändbares Einkommen liegt derzeit bei 1.611,17 EUR.

Das „Beschaffungshandbuch Strom" seines Arbeitgebers lautet auszugsweise wie folgt:

„Die Absatzmengen für Kunden mit > 200 MWh/a werden zum Zeitpunkt des jeweiligen Vertragsabschlusses mit dem Endkunden unverzüglich Backto-Back beschafft. Somit wird erreicht, dass das Preisrisiko zwischen den kalkulatorischen Energiekosten und dem tatsächlich realisierten Beschaffungspreis möglichst gering ist."

Eines Tages wurde festgestellt, dass entgegen der Vorgaben des Beschaffungshandbuches für das Jahr 2022 erst 23 % der Strommengen eingekauft waren. Darauf erhielt der Vertriebsleiter den Arbeitsauftrag, alle offenen Beschaffungen zu erledigen. Am 02.12.2021 gab der Vertriebsleiter gegenüber zwei potenziellen Geschäftskunden Angebote über die Lieferung von Strom ab dem Kalenderjahr 2022 ab.

Der Vertriebsleiter unterließ es allerdings, die entsprechenden Strommengen für beide Firmen Back to Back beim Vorlieferanten einzukaufen. Die Nettostrompreise der beiden Verträge liegen bei 6,5 Mio. EUR.

Der Vertriebsleiter versuchte in der Folgezeit diese Verträge abzudecken, was ihm nicht gelang. Die fehlende Absicherung teilte er niemandem mit.

Erstmals am 08.03.2022 brachte der Vertriebsleiter dem Vorstand zur Kenntnis, dass eine Beschaffung für die Verträge mit den beiden Großkunden nicht erfolgt war. Auszugsweise lautet dieser Bericht:

„Am 02.12.2022 habe ich ein Stromangebot an die folgenden Unternehmen gerichtet. ***Da ich wusste, dass der traditionelle Anbieter noch im Wettbewerb zu uns stand, habe ich am 02.12.2021 ein eng kalkuliertes Angebot abgegeben. Ich habe dann auch den Zuschlag für beide Unternehmen erhalten.***

Leider haben sich an diesem Tag die Strompreise an den Handelsplätzen sehr volatil verhalten und ich konnte, trotz einer recht kurzer Bindefrist, die Zielbeschaffungspreise nicht mehr realisieren. Hätte ich dennoch die Mengen über das RETWeb Tool bestellt, wäre der Abschluss mit einem negativen Ergebnis verlaufen ***und es wäre ein Schaden entstanden. Diese Tatsache hat mich persönlich sehr getroffen und mich zu einer nicht regelkonformen Vorgehensweise verleitet.***

Da ich den Abschluss nicht mit einem Schaden für die BHAG enden lassen wollte ***und auch Befürchtung hatte sanktioniert zu werden, habe ich versucht, das Geschäft durch eine spätere Eindeckung noch zu retten****. Leider haben die Marktgeschehnisse nicht dazu beigetragen, dass mir das gelingen konnte.*

... Ich möchte an dieser Stelle erwähnen, dass der Fehler ganz alleine bei mir zu suchen ist, ***da ich übermotiviert einen Erfolg gesucht und dabei nicht alle Regeln eingehalten habe."***

Daraufhin kündigte der Arbeitgeber das Arbeitsverhältnis „*fristlos und aus wichtigem Grund*" und beantragte zudem, den Kläger zu verurteilen, an sie einen Betrag in Höhe 3.000.000 Euro gesamtschuldnerisch mit weiteren Beschäftigten, unter anderem dem Vorgesetzten des Vertriebsleiters, zu zahlen.

Das *Arbeitsgericht Siegburg* bestätigte mit Urteil vom 21.10.2022 die außerordentliche Kündigung und verurteilte vollumfänglich zum Schadensersatz. Gegen dieses Urteil legte der Vertriebsleiter beim *LAG Köln* Berufung ein.

Das *LAG Köln* bestätigte die Rechtmäßigkeit der Kündigung, reduzierte aber den Schadensersatz auf zwei Jahresgehälter, weil es anstelle von Vorsatz lediglich von grober Fahrlässigkeit des Vertriebsleiters ausging*:*

„(…) Allerdings hat der Kläger seine arbeitsvertraglichen Pflichten in erheblichem Maße verletzt, indem er für die beiden genannten Kunden entgegen dem ihm bekannten Beschaffungshandbuch Strom die verkauften Strommengen seinerseits nicht backtoback beim Stromlieferanten (R AG) beschafft hat. Diese Pflichtverletzung wiegt besonders schwer, weil die Beschaffung im Hinblick auf das Volumen der Verträge ein besonderes Risiko barg und dies den Kläger zu besonders aufmerksamem Handeln hätte veranlassen müssen. (…)"

Der Arbeitgeber habe gegen den Vertriebsleiter einen Schadensersatzanspruch in Höhe von 202.399,92 EUR aus § 280 Abs. 1 BGB. Nach den **Grundsätzen der Arbeitnehmerhaftung** setze dieser Schadensersatzanspruch u.a. voraus, dass der Arbeitnehmer arbeitsvertragliche Pflichten verletzt hat, dem Arbeitgeber hierdurch ein Schaden entstanden ist, ein Kausalzusammenhang zwischen Vertragsverletzung und Schaden vorliegt und der Arbeitnehmer die Vertragsverletzung zu vertreten hat.

Das LAG Köln ging bei der Frage des Vertretenmüssens, anders als das Arbeitsgericht, nicht von einer vorsätzlichen Schadensverursachung aus.

Der Vertriebsleiter habe gerade nicht die Entstehung eines Schadens billigend in Kauf genommen, sondern weiterhin gehofft, diesen noch durch Beschaffungen zu einem günstigeren Preis abwenden zu können. Ein vorsätzliches Handeln liege daher nicht vor. Stattdessen nimmt das LAG Köln ein grob fahrlässiges Handeln an.

Der Schaden sei auch nicht aufgrund eines Mitverschuldens des Arbeitgebers gemindert. Ein **Mitverschulden würde in der Regel dann vorliegen, wenn der Arbeitgeber die ihm als Inhaber der Organisationsmacht *im Betrieb obliegende Pflicht zur Schadensminderung durch Erteilung von Weisungen, Kontrollmaßnahmen, Überprüfungen etc. nicht hinreichend beachte.***

Solche konkreten Obliegenheiten haben aber vorliegend nicht bestanden, da die Anweisungen für die Abdeckung der verkauften Strommengen (backtoback) eindeutig waren. Im Übrigen habe ein 4-Augen-Prinzip bestanden.

Für den entstandenen Schaden müsse der Vertriebsleiter aber nicht in vollem Umfang einstehen, sondern nur im Umfang von zwei Jahresgehältern:

***„Nach den vom Großen Senat des Bundesarbeitsgerichts entwickelten Grundsätzen** (…) hat ein Arbeitnehmer vorsätzlich verursachte Schäden in vollem Umfang zu tragen, bei leichtester Fahrlässigkeit haftet er dagegen nicht. Bei normaler Fahrlässigkeit ist der Schaden in aller Regel zwischen Arbeitnehmer und Arbeitgeber zu verteilen, bei grober Fahrlässigkeit hat der Arbeitnehmer in aller Regel den gesamten Schaden zu tragen, jedoch können Haftungserleichterungen, die von einer Abwägung im Einzelfall abhängig sind, in Betracht kommen (…). Solche hat das Gericht hier angenommen."*

11. Persönliche Haftung des Delegierenden und des Delegationsempfängers bei fehlerhafter Übertragung oder Wahrnehmung von Unternehmerpflichten (Pflichtendelegation)[101]

[101] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, Kapitel 6.5, S. 138 ff.: Verantwortung, Delegation, Haftung.

In der arbeitsteiligen Wirtschaftswelt wird üblicherweise von den primär- und letztverantwortlichen Organen (Vorstand / Geschäftsführer / etc.) auf Führungskräfte (Stabsstellen, Abteilungsleiter etc.) delegiert. Und diese delegieren oft weiter.

Auch auf Externe (Berater[102], Lieferanten, Auftragsdatenverarbeiter, Assembler, Veredler, verlängerte Werkbanken, etc.) wird häufig delegiert, wobei die nachfolgend dargestellten Grundsätze weitgehend auch hier gelten.

Bei Delegation wandelt sich die primäre Ausführungspflicht in eine Auswahl-, Instruktions- und *Überwachungs*pflicht bzgl. des Delegationsempfängers.

Deshalb umfasst der Begriff Governance neben Führung auch *Überwachung*.

Werden bei der sogenannten Pflichtendelegation Fehler gemacht, kann das zu einer Haftung sowohl des Delegationsempfängers als auch der Organisation und des Leitungsorgans führen (vgl. §§ 130, 9, 30 OWiG). Auch der Aufsichtsrat, der den Vorstand zu überwachen hat und Mängel in der Organisation nicht moniert und abstellen lässt, ist in der Haftungsverantwortung (§§ 116, 107 AktG).

Aktuell akquirieren und ernennen immer mehr Organisationen (konkret: deren Leitungsorgane als Delegierende) sogenannte Beauftragte für spezielle Bereiche, wie KI-, Informationssicherheits-, Compliance-, Risiko-, Datenschutz- (Art. 37 ff. DSGVO, § 7 BDSG), Umwelt-, Abfall- (§§ 59, 60 KrWG), Exportkontroll-[103] bzw. Ausfuhr- (§§ 4, 8, 11, 17, 18 AWG, 5, 9, 74 AWV, 1, 2, 6, 8 KWKG), Brandschutz-, Arbeitssicherheits- (§ 10 ArbSchG etc.), Strahlenschutzbeauftragte (§ 70 StrlSchG) etc., deren Aufgaben und Verantwortung nicht stets gesetzlich geregelt sind und denen mehr oder weniger förmlich Unternehmerpflichten übertragen wurden (vgl. § 9 Abs. 2 Nr. 2 OWiG etc.).

Unsicherheit über Haftungsverantwortung

Da meist weder die diversen Berufsbezeichnungen noch deren Aufgaben und (Haftungs-)Verantwortung legaldefiniert sind, besteht in der Praxis aufgrund der diesbezüglich vorherrschenden Unsicherheit Aufklärungsbedarf.

Weiteres Fallbeispiel zur Haftung einer Führungskraft (Leiter Recht und Interne Revision)

Für Aufsehen sorgte 2009 ein höchstrichterliches Urteil: Der Bundesgerichtshof (BGH) verurteilte am 17.07.2009[104] einen Leiter einer Rechtsabteilung und Revision eines Berliner Entsorgungsbetriebs wegen Beihilfe zum Betrug durch Unterlassen zu einer Geldstrafe von 120 Tagessätzen. Hintergrund war der Vorwurf gegenüber dem Leiter der Innenrevision der Berliner Stadtreinigung, er habe von überhöhten Gebührenfestsetzungen gewusst, ohne sie beim Vorstand zu beanstanden. Dadurch habe er Beihilfe zum Betrug geleistet. Hierbei referenziert der BGH auf die sogenannte Garantenplicht, wonach für eine Strafbarkeit durch Unterlassen eine Pflicht zum Handeln bestehen muss.

In dem Urteil wird explizit die Rolle und Verantwortlichkeit des Compliance-Beauftragten in Unternehmen angesprochen: *„[…] Deren Aufgabengebiet ist die Verhinderung von*

[102] Interessant ist hierbei die 130-Millionen-Schadensersatz-Klage von *Continental* gegen die Anwaltskanzlei *Noerr*, in der wohl Continental ihren Beratern im Kontext mit dem Diesel-Skandal und Internal Investigations unzureichende Risikoanalysen (insbesondere zu Bußgeldrisiken, vgl. §§ 130, 30, 9 OWiG), Defizite in der Steuerung der Kooperation mit Ermittlungsbehörden u.v.m. vorwirft, vgl. *Schmidbauer,* Warum Continental gegen Noerr klagt, LTO vom 10.4.2026, im Internet verfügbar.

[103] Der/die Exportkontroll- oder Ausfuhrbeauftragte unterstützt operativ den/die Ausfuhrverantwortliche/n und ist deshalb mittels Stellenbeschreibung konkret von dessen/deren Rolle abzugrenzen. Der/die Ausfuhrverantwortliche als Mitglied der Geschäftsleitung wird in den Anträgen auf Genehmigung der Ausfuhr von Rüstungsgütern, Waffen und Dual Use-Gütern als Verantwortliche/r genannt.

[104] BGH, Urteil vom 17.07.2009, (Az 5 StR 394/08 - „Berliner Entsorgungsbetrieb“).

Rechtsverstößen, insbesondere auch von Straftaten, die aus dem Unternehmen heraus begangen werden und diesem erhebliche Nachteile durch Haftungsrisiken oder Ansehensverlust bringen können. […] Derartige Beauftragte wird regelmäßig strafrechtlich eine Garantenpflicht im Sinne des § 13 StGB treffen, solche im Zusammenhang mit der Tätigkeit des Unternehmens stehende Straftaten von Unternehmensangehörigen zu verhindern. Dies ist die notwendige Kehrseite ihrer gegenüber der Unternehmensleitung übernommenen Pflicht, Rechtsverstöße und insbesondere Straftaten zu verhindern […].“

Beweislastumkehr bei Delegationen

Nach *BGH*[105] trägt ein Geschädigter grundsätzlich die Beweislast für die Pflichtverletzung, Schadensentstehung und den Ursachenzusammenhang zwischen Pflichtverletzung und Schaden. Die Pflichtverletzung durch Delegationsempfänger kann den Delegierenden bzw. der Organisation aufgrund diverser Rechtskonstrukte zugerechnet werden.[106]

Im Arzthaftungsrecht, aber laut *BGH* nun auch bei der Verletzung sonstiger Berufs- und Organisationspflichten, die dem Schutz von Leben und Gesundheit anderer dienen, kann eine *grobe Organisationspflichtverletzung u. U. sogar zur Umkehr der objektiven Beweislast für den ursächlichen Zusammenhang zwischen der Pflichtverletzung und dem Schaden führen*. D. h. der potenzielle Schädiger oder dessen Organisation müssten sich sogar bzgl. der Ursächlichkeit entlasten.

Grobe Pflichtverletzung durch mangelhafte Dokumentation und unangemessene Personalressourcen

In den meisten Fällen ist dies aufgrund fehlender oder lückenhafter Dokumentation nicht möglich: Eine grobe Pflichtverletzung kommt nämlich beispielsweise in Betracht, wenn mangelhafte Dokumentation und nicht angemessene quantitative und/oder qualitative Personalressourcen aufeinandertreffen.[107]

In Zeiten von Personaleinsparungen aus Kostengründen in Kombination mit Fachkräftemangel besteht hier in vielen Unternehmen ein enormes Haftungsrisiko. Dagegen hilft nur, die haftungsträchigen Pflichtstellen sorgsam zu planen, zu monitoren und angemessen zu besetzen.

Wenn z.B. Stellen, wie Brandschutz-, Arbeitssicherheits-, Exportkontroll-, Compliance-, Risiko-, Informationssicherheits- oder sonstige relevante Beauftragte nicht angemessen (Kompetenz, Ressourcen, Zuverlässigkeit etc.) besetzt sind und was Einschlägiges passiert, werden Organisation, Leitungs- und Überwachungsorgan im Focus von Ermittlern und „feindlichen“ Anwälten stehen und wegen Organisationspflichtverletzung haften.

Enthaftung bei Pflichtverletzungen durch Delegationsempfänger unterhalb der Leitungsebene

Die Organisation haftet i. d. R. gemäß § 30 OWiG, wenn ihr gem. §§ 130, 9 OWiG die schuldhafte Pflichtverletzung einer Leitungsperson zugerechnet werden kann.

Der EuGH hat für Art. 83 DSGVO jüngst mehrfach entschieden, dass für die Sanktionierung der Organisation – analog zur Haftung im Kartellrecht – keine Zurechnung der schuldhaften Pflichtverletzung einer Leitungsperson nötig ist. Gleichwohl muss eine schuldhafte

---

[105] Vgl. BGH, Urteil vom 11.5.2017, (Az. III ZR 92 / 16 - „Hausnotruf“).
[106] Vgl. *Scherer*, Business Partner Screening – Überwachungspflichten bei Delegation von Aufgaben auf Externe: Organisationspflichten versus "Scheinselbstständigkeit", abrufbar unter https://www.gmrc.de/images/Docs/07.06.2017-sonderdruck-ueberwachungspflichten-bei-delegation/Sonderdruck_Ueberwachungspflichten_bei_Delegation.pdf.
[107] Vgl. *OLG Nürnberg*, Beschluss vom 25.11.2020, (Az.11 W 4194/19 - „Geburtsklinik“).

Pflichtverletzung irgendeiner Person identifiziert sein. Es gibt also keine „strict liability“ bzw. Gefährdungshaftung.

Rechtskonforme Delegation

Der Delegationsempfänger muss nicht nur rechtskonform bzgl. fachlicher und persönlicher Eignung ausgesucht, über Arbeitsvertrag, Beschluss, Direktionsrecht etc. „beauftragt“ und angemessen bzgl. Aufgaben und Verantwortung mithilfe von Stellenbeschreibungen oder Geschäftsverteilungsplan etc. instruiert werden. Auch eine angemessene Überwachung ist Pflicht. Ebenso auch die Ausstattung des Delegationsempfängers mit angemessenen (finanziellen, sachlichen, personellen und zeitlichen) Ressourcen.

Fallbeispiel

Interessant erscheint in diesem Zusammenhang das Urteil des ArbG Heilbonn[108], das eine fristlose Kündigung eines Datenschutzbeauftragten (DSB) für unwirksam erklärte. Obwohl ein Gutachten schwerwiegende Datenschutzmängel feststellte, wäre keine Kündigung des Arbeitsverhältnisses, sondern nur eine Abberufung als DSB möglich gewesen. Außerdem sei nicht der DSB, sondern der Vorstand Verantwortlicher i. S. d. DSGVO. Der DSB hätte darüber hinaus auch die nötigen zeitlichen Ressourcen zur Verfügung gestellt bekommen müssen.

Der Vorsitzende Richter des 1. Strafsenats des Bundesgerichtshofes wies 2017 darauf hin, dass keine Strafbarkeitslücke entstehen dürfe, wenn die Geschäftsleitung Aufgabe und Verantwortung bzgl. Compliance auf einen Compliance-Officer delegiere, also entweder Geschäftsleitung oder Compliance-Officer (oder im Worst Case beide) geradestehen müssten.[109]

Sanktionsmildernde Wirkung eines Compliance-Managementsystems

Gleichwohl belohnt der Staat auch die Einrichtung einer entsprechenden Organisation: Die Rechtsfigur, Rechtspflichtverletzungen bei Vorhalten eines Compliance-Managementsystems weniger hart oder gar nicht zu bestrafen, findet sich bereits in den 1980er Jahren in „US Sentencing Guidelines“. Jetzt zeigt sich diese Rechtsfigur als Trend sowohl in der Gesetzgebung als auch in der Rechtsprechung.

In jüngerer Zeit gab es dazu eine Serie von Urteilen des BGH, angefangen mit dem „KMW-Urteil“ vom 9.5.2017[110], in dem der BGH das erste Mal auf eine mögliche sanktionsmildernde Wirkung eines Compliance-Managementsystems bei Pflichtverletzungen durch Delegationsempfänger unterhalb der Leitungsebene hinweist. Weitere BGH-[111] und auch EuGH-Urteile[112] folgten, sodass nunmehr von „ständiger höchstrichterlicher Rechtsprechung“ ausgegangen wird.[113]

Der BGH stellte in seinem Urteil vom Mai 2017[114] fest, dass bei Vorhalten eines Compliance-Managementsystems möglicherweise eine Verantwortung des Unternehmens und der Geschäftsleitung im Bußgeldbereich entfallen könne, selbst dann, wenn es zu Verstößen

---

[108] Vgl. *ArbG Heilbronn*, Urteil vom 29.9.2022 (Az. 8 Ca 135 / 22 – „Datenschutz-Beauftragter“).

[109] Vgl. *Raum*, Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten, 2017, S. 33 ff. in: *Hastenrath* (Hrsg.), Compliance-Kommunikation 2017, zitiert von *BGH,* Urteil vom 9.5.2017, (Az. 1 StR 265 / 16 – „*KMW*“), Rn. 110. Entscheidung und Bezugsartikel werden ausführlich kommentiert in *Scherer*, Compliance-Managementsystem nach DIN ISO 37301:2021 – erfolgreich implementieren, integrieren, auditieren, zertifizieren, 2022, S. 22 ff.

[110] *BGH*, Urteil vom 09.05.2017, (Az. 1 StR 265/16 – „KMW“).

[111] *BGH*, Urteil vom 27.4.2022, (Az. 5 StR 278 / 21 – „Selbstreinigung“) und *BGH*, Urteil vom 9.11.2023, (Az. III ZR 105 / 22 – „Geschäftsverteilung“).

[112] *EuGH*, Urteil vom 5.12.2023 („*Deutsche Wohnen*“); *EuGH*, Urteil vom 14.12.2023 („*Hackerangriff*“); *EuGH*, Urteil vom 30.1.2024 („*USt-Betrug*“); *EuGH*, Urteil vom 11.4.2024 („*Juris-Datenschutz*“).

[113] Vgl. *Grötsch/Scherer*, Die Bedeutung von Compliance-Managementsystemen im Straf- und Ordnungswidrigkeitenrecht sowie im Zivil- und Steuerrecht, wistra 2024, S. 139 ff.

[114] *BGH*, Urteil vom 09.05.2017 (Az. 1 StR 265/16 – „KMW“) mit Verweis auf einen instruktiven Artikel von Raum im Urteil unter Rn. 110 ff.

gekommen sei und das System entsprechend nachgebessert werde. Vereinfacht ausgedrückt stellt diese Rechtsprechung bei Pflichtverstößen unterhalb der Leitungsebene auf eine möglicherweise fehlende Organisationspflichtverletzung respektive fehlendes Verschulden der Leitung beim Vorwurf mangelhafter Überwachung der Delegationsempfänger ab, wenn ein entsprechendes Aufsichts- und Kontrollsystem gerade auch zu diesem Zweck eingeführt wurde.

Grundsätzliche Rechtsfiguren zu Haftung und Enthaftung bei „Sonderbeauftragten“

Die Rechtsprechung des BGH zur Haftung des Compliance-Officers im Fall des Berliner Entsorgungsbetriebs lässt sich nicht direkt auf die Haftung anderer Sonderbeauftragter, beispielsweise Nachhaltigkeits-, Umwelt-, Risiko-, Datenschutz-, Qualitäts-, Arbeitssicherheits-Beauftragte etc. übertragen. Jedes Urteil ist individuell zu sehen und auszuwerten. Wird ein Jurist gefragt, wie ein Sachverhalt rechtlich zu beurteilen sei, wird er immer antworten: „Es kommt darauf an.“ Das ist hier sogar zutreffend.

Gleichwohl lassen sich Parallelen und Grundsätze herausarbeiten: Fakt ist zum einen, dass Sonderbeauftragte, z. B. auch Governance-Beauftragte, bzgl. ihrer Aufgaben und Verantwortung bzw. Haftung eine besondere Rolle einnehmen und damit grundsätzlich schon einmal bei entsprechenden Pflichtverstößen in ihrem Verantwortungsbereich im Fokus von Ermittlern, gegnerischen Rechtsanwälten oder den Medien stehen.

Garantenstellung

„Gefährlich“ wird es für die Sonderbeauftragten, wenn die Ausgestaltung der Delegation zur Annahme einer Garantenstellung führen kann. Sofern ein Governance- oder sonstiger Sonderbeauftragter eine Garantenstellung innehat, kommt auch eine verschärfte straf-, bußgeld- und auch zivilrechtliche Haftung sogar bei Untätigkeit oder Unterlassen in Betracht.

Garant ist allgemein, wer eine Herrschaftsposition innehat, sei es eine Schutzherrschaft (d. h. Obhut über ein zu schützendes Rechtsgut) oder eine Überwachungsherrschaft (d. h. Sicherung einer Gefahrenquelle zur Vermeidung von Schäden Dritter). Für die Herleitung einer Garantenstellung als Voraussetzung für eine Haftung bei Unterlassen sowohl im Straf- wie im Zivilrecht gibt es unterschiedliche wissenschaftliche Ansätze:

Die Funktionenlehre leitet eine Rechtspflicht zum Schutz von Rechtsgütern u. a. aus Gesetz her oder eine Rechtspflicht zum Schutz vor einer Gefahrenquelle als Überwachergarant beispielsweise aus Ingerenz (d. h. pflichtwidriges, gefährliches Vorverhalten), dem Inverkehrbringen gefährlicher Gegenstände. Die Rechtsquellenlehre sieht die Garantenstellung in bestimmten Rechtsquellen, wie Gesetz, sonstigen Normen oder Vertrag, begründet. Diese unterschiedlichen Ansätze dürften nur einen rein wissenschaftlichen Streit darstellen.[115]

Für die Praxis lässt sich festhalten, dass theoretisch nahezu jeder Sonderbeauftragte auch eine Garantenstellung innehaben kann.

Fehlende gesetzliche Regelungen zu Aufgaben und Haftung

Gesetzliche Grundlagen bzgl. der Aufgaben und Verantwortung eines Governance-, Compliance-, Risiko- oder Nachhaltigkeitsbeauftragten fehlen bisher. Anders ist das z. B. beim Datenschutzbeauftragten, dessen Aufgaben u. a. in der DSGVO, oder beim Strahlenschutzbeauftragten, dessen Aufgaben im StrlSchG beschrieben sind. Auch erhellende Rechtsprechung bzgl. der meisten Sonderbeauftragten fehlt: Es gibt hier also keine Legaldefinition oder dezidierte Regelung.

---

[115] Vgl. zu den verschiedenen Lehren, RiskNET: „Haftung eines Risikomanagers“, Interview vom 16.07.2018, abrufbar unter https://www.risknet.de/themen/risknews/haftung-eines-risikomanagers.

Es gilt jedoch ein allgemeiner Grundsatz: Je weiter der Aufgabenbereich und die Befugnisse eines Sonderbeauftragten gefasst sind, desto eher wird dieser eine Garantenstellung innehaben: Falls also der Governance- oder sonstige Sonderbeauftragte nicht explizit bloß beratend oder unterstützend tätig wird, sondern eher Verantwortung für das Erkennen, Bewerten und Behandeln von Risiken trägt und neben umfassenden Informationsrechten auch eigene Entscheidungs-, Eingriffs- und Weisungsrechte hat, desto eher ist er als Garant verantwortlich.

Klarstellen lässt sich dies über die jeweilige Fassung von Stellen- und Arbeitsplatzbeschreibungen, Ernennungsbeschluss sowie vertragliche Regelungen mit den jeweiligen Beauftragten.

Empfehlung

Regeln Sie in Stellen-, Arbeitsplatzbeschreibung, Ernennungsbeschluss und unter Umständen im Anstellungsvertrag explizit den Aufgaben- und Verantwortungsbereich des Governance-, bzw. sonstigen Sonderbeauftragten bis hin zur expliziten Klärung der Frage, ob damit eine Garantenstellung begründet werden soll.

Beispiel

Ein dezentraler Risikoverantwortlicher, etwa im Bereich der Produktion, weist den Governance-Beauftragten auf zwei wesentliche Governance-Risiken hin: Aufgrund zahlreicher Medienberichte hat er mitbekommen, dass der aktuelle starke Anstieg von Insolvenzen[116] auch in der Branche seiner Organisation existenzbedrohend sein könnte. Darüber hinaus bringt die Neuregelung der Produkthaftung auf europäischer Ebene[117] neue erhebliche Compliance-Risiken.

Ein in vielen Fachzeitschriften kommuniziertes Risiko-Früherkennungssystem nach § 1 StaRUG existiert bei seinem Arbeitgeber aktuell ebenso wenig wie ein Product-Compliance-Managementsystem. Der Governance-Beauftragte hätte gemäß seiner Stellenbeschreibung die Aufgabe, hier entsprechende Maßnahmen zur Risikominimierung oder -vermeidung zu initiieren. Er unterlässt dies und informiert auch die Geschäftsleitung nicht über diese Risiken. Nun kommt es in der Folge zu einem Risikoeintritt mit Auswirkungen auf Leib und Leben oder durch eine Krise auch auf das Vermögen der Organisation. Nachweislich hätten diese Risiken präventiv vermieden werden können.

Für die Haftung des Governance-Beauftragten ist nun zu unterscheiden, ob es sich hier um eine mögliche Pflichtverletzung durch aktives Tun oder durch Unterlassen handelt.

Aktives Tun wäre beispielsweise gegeben, wenn für den Governance-Beauftragten in Prozessen eine aktive Freigabefunktion eingebaut wäre – wie bei modernen Risiko-Managementsystemen mit Automatisierung und Workflows bei entsprechenden Fehlermeldungen üblich. Hier würde sich bei einer (pflichtwidrigen) Freigabe durch den aktiven Verursachungsbeitrag des Governance-Beauftragten die Frage nach einer besonderen Garantenstellung nicht stellen. Sein Handeln wäre eine „conditio sine qua non“: Da er zumindest eine Mitursache gesetzt hat, reicht das auch, ihm als Mitverantwortlichen Haftungsverantwortung vorzuwerfen.

---

[116] Vgl. *Handelsblatt, dpa*, Zahl der Insolvenzen steigt wieder zweistellig, 09.08.2024, abrufbar unter https://www.handelsblatt.com/unternehmen/handel-konsumgueter/wirtschaft-zahl-der-insolvenzen-steigt-wieder-zweistellig/100058439.html.

[117] Vgl. *Scherer*, Innovationen und enthaftende Wirkung eines Product- oder Nachhaltigkeits-Compliance-Managementsystems, ZfPC 01/2024, S. 15-20, abrufbar unter https://www.risknet.de/elibrary/paper/innovationen-und-enthaftende-wirkung-eines-product-oder-nachhaltigkeits-compliance-managementsystems-im-lichte-aktueller-hoechstrichterlicher-rechtsprechung/

Ähnlich war es im Transrapid-Fall.[118] Hier gab es Verurteilungen gegen Fahrdienstleister wegen fahrlässiger Tötung (mehr als 20 Tote), weil sie die Fahrt „freigegeben" hatte. Dagegen wurden deren Vorgesetzte verurteilt, weil sie es unterlassen hatten, für eine rechtssichere Organisation (entsprechende Prozessbeschreibungen) zu sorgen.

Unterlassen liegt dagegen vor, wenn der Governance-Beauftragte lediglich entsprechende Sicherungsmaßnahmen unterlässt. Dann stellt sich tatsächlich die Frage nach der Garantenpflicht, die bereits oben beantwortet wurde.

Empfehlung

Achten Sie bei dokumentierten Risikobewertungen immer darauf, dass weder unter- noch übertrieben wird: Risikobewertungen sind von kompetenten Beschäftigten durchzuführen, die Risiken angemessen, nicht intuitiv identifizieren und bewerten.

Wenn die Risikobewertung ein Risiko bzgl. der Auswirkungen als hoch einstuft, ist auch bei niedriger Eintrittswahrscheinlichkeit sofort mit der Risikosteuerung zu beginnen und dies zu dokumentieren.

12. Entwicklungen bei der D&O-Versicherung

„D&O-Versicherung: Manager werden öfter zur Kasse gebeten

(…) Die Versicherer rechnen damit, dass Schadenersatzforderungen gegen Manager künftig zunehmen werden. Dies ist auf die konjunkturelle Lage und höhere gesetzliche Anforderungen zurückzuführen. Nach der aktuellen D&O-Statistik des GDV stieg die Zahl der Schäden bereits das zweite Jahr in Folge. Dabei steigen die Schäden schneller als die Beitragseinnahmen.

Die in Deutschland tätigen Managerhaftpflicht-Versicherer haben 2023 erneut mehr Schäden regulieren müssen. Die Zahl der Fälle ist auf 2.200 gestiegen, fast sieben Prozent mehr als im Vorjahr. Eine D&O- bzw. Managerhaftpflichtversicherung zahlt Schadenersatzforderungen gegen Manager-/innen, wenn diese gegen ihre Pflichten verstoßen haben. Jeder Schaden kostete die Versicherer im Schnitt fast 100.000 Euro.

Die Entwicklung führen die Versicherer auf die konjunkturelle Lage und höhere gesetzliche Anforderungen zurück. Die Zahl der Insolvenzen ist zuletzt deutlich gestiegen. Das zieht oft hohe Schadenersatzforderungen von Insolvenzverwaltern gegen die Verantwortlichen nach sich.

Dazu kommen stetig wachsende Compliance-Anforderungen. Manager haften persönlich, wenn sie kein funktionierendes Compliance-System eingerichtet haben. (…)"[119]

13. Haftungsverschärfung durch jüngste „Kardinalpflicht"-Rechtsprechung: „Blind in Haftung und Versicherungsverlust segeln"

Neben des nachgewiesen drastisch steigenden Risikos der persönlichen Haftung droht aufgrund des von aktueller Rechtsprechung des *OLG Frankfurt/M.*[120] und des *BGH*[121] angenommenen Vorwurfs der „*Verletzung von Kardinalpflichten*" und der daraus abgeleiteten

[118] Vgl. *ZEIT online, dpa*, Tote bei Transrapid-Unfall, abzurufen unter https://www.zeit.de/online/2006/39/transrapid-unfall.
[119] Zitat aus: GDV-Gesamtverband der Deutschen Versicherer, D&O-Versicherung: Manager werden öfter zur Kasse gebeten, 11 / 2025.
[120] Vgl. OLG Frankfurt/M., Beschl. v. 16.1.2025 – 7 W 20/24, NJW-RR 2025, 731: „blind in die Krise segeln".; vgl. auch OLG Frankfurt/M., Urt. v. 5.3.2025 – 7 U 134/23, DStR 2025, 917, mit einem ähnlichen Fall, der in der Revision vom BGH (Az. IV ZR 66/25) zur weiteren Aufklärung zurückverwiesen wurde.
[121] *BGH*, Urteil vom 19.11.2025, Az. IV ZR 66 / 25 („*ULLA-Versicherungsschutz-Ausschluss*").

Indikation einer „*wissentlicher Pflichtverletzung*“ der Verlust des Versicherungsschutzes für Manager und Führungskräfte.

Nach der neuesten Entscheidung des *BGH*[122] bleiben die Ausführungen der bisherigen Judikatur zu Haftung von Führungskräften bei Pflichtverletzungen unberührt:

Zum einen kann ein Organ (Vorstand / Geschäftsführer) aus unterschiedlichen Gründen persönlich auf Schadensersatz haften, wenn er keine angemessene Risiko- oder Krisenfrüherkennung betreibt und dadurch die Gesellschaft schädigt (§§ 43 GmbHG, 93 AktG, etc.). Hier reicht bereits Fahrlässigkeit.

Falls der Geschäftsführer / Vorstand nicht über eine D&O- (Managerhaftpflicht-Versicherung) verfügt, muss er persönlich den Schaden ersetzen.

Sofern er versichert ist, stellte sich nun die Frage, ob die Versicherung die Zahlung unter Verweis auf einen Risikoausschluss in den *ULLA*-Versicherungsbedingungen „*wegen wissentlicher Pflichtverletzung*“ verweigern kann.

In den *ULLA-Versicherungsbedingungen für die Vermögensschadenshaftpflichtversicherung von Unternehmensleitern und Leitenden Angestellten* ist ein Risikoausschluss für den Fall des Vorsatzes und der wissentlichen Abweichung von Gesetz etc. geregelt:

„*1. Gegenstand der Versicherung / 1.1 Versicherte Tätigkeit / (…) Versicherungsschutz für den Fall, dass eine versicherte Person wegen einer (…) begangenen Pflichtverletzung (…) auf Schadenersatz in Anspruch genommen wird. ... / 6. Ausschlüsse / Ausgeschlossen (…) sind Haftpflichtansprüche wegen vorsätzlicher Schadenverursachung oder durch* wissentliches Abweichen von Gesetz, Vorschrift, Beschluss, Vollmacht oder Weisung oder durch sonstige wissentliche Pflichtverletzung *durch eine versicherte Person.“*

Nach dem aktuellen Urteil des *BGH* heißt „*vorsätzlich*“ und „*wissentlich*“ sinngemäß, dass der Versicherer für eine Verweigerung seines Schutzes nachweisen muss, dass die versicherte Führungskraft die Vorschrift kannte und bewusst davon abwich.

Der *BGH* widersprach insoweit damit lediglich der Ansicht des *OLG Frankfurt*, dass bei wissentlichen Pflichtverletzungen generell sogleich ein Risikoausschluss gemäß der Allgemeinen D&O-AGB *ULLA*[123] vorliege. Es müsse schon ein wissentlicher Pflichtverstoß im Sinne eines direkten Vorsatzes oder gar Absicht[124] vorliegen. Fahrlässigkeit oder ein bloßes „für-möglich-halten-und-sich-damit-abfinden“[125] reiche nicht.

Zitat des BGH:

„aa) Wissentlich handelt nur derjenige Versicherte, der die verletzten Pflichten positiv kennt. Bedingter Vorsatz, bei dem er die in Rede stehende Verpflichtung nur für möglich hält, reicht dafür ebenso wenig aus wie eine fahrlässige Unkenntnis. Es muss vielmehr feststehen, dass der Versicherte die Pflichten zutreffend gesehen hat (…) Der Versicherte muss die von ihm verletzte Pflicht positiv gekannt und subjektiv das Bewusstsein gehabt haben, gesetz-, vorschrifts- oder sonst pflichtwidrig zu handeln. (…) (

bb) Das Berufungsgericht hat (…) zur Kenntnis des Geschäftsführers jedoch nur festgestellt, dass dieser sich der Gewissheit der Zahlungsunfähigkeit zumindest bewusst verschlossen habe. Die positive Kenntnis des Geschäftsführers folgt daraus nicht. Ein bewusstes Verschließen vor der Kenntnis von Tatumständen ist dann anzunehmen, wenn die Unkenntnis auf einem gewissenlosen oder grob fahrlässigen (leichtfertigen) Handeln beruht (…). Wenn sich der Betreffende einer Kenntnis bewusst verschließt, erlaubt dies nur die Annahme eines bedingten Vorsatzes (…). Die von der Ausschlussklausel geforderte wissentliche Pflichtverletzung kann nicht in dieser Weise auf ein Verhalten ohne direkten Vorsatz erstreckt werden. (…)“

---

[122] *BGH*, Urteil vom 19.11.2025, Az. IV ZR 66 / 25 („*ULLA-Versicherungsschutz-Ausschluss*“).
[123] ULLA: Versicherungsbedingungen für die Vermögensschadenshaftpflichtversicherung von Unternehmensleitern und Leitenden Angestellten
[124] Dolus directus 2. Grades (Wissentlichkeit) oder 1. Grades (Absicht).
[125] Dolus eventualis.

Streitigkeiten mit dem Versicherer und das Risiko, dass der Versicherer sich erfolgreich auf einen Risikoausschluss beruft, sollten vermieden werden.

Dafür eignet sich die Implementierung eines angemessenen und wirksamen (zertifizierten) Compliance-Managementsystems. Dadurch kann – auch nach Ansicht des ehemaligen Vorsitzenden BGH-Richters Raum - indiziert werden, dass etwaige Pflichtverletzungen nicht vorsätzlich i.S. eines Dolus Directus 1. oder 2. Grades erfolgten und somit der Berufung des Versicherers auf einen vertraglichen Risikoausschluss entgegengetreten werden.

Im Übrigen mag es sein, dass die Versicherer nun ihre Ausschluss-Klauseln in die Versicherungsbedingungen überarbeiten und präziser formulieren, was die Wichtigkeit von Compliance-Systemen weiter erhöht.

Zu den sogenannten Kardinalpflichten *führte der* BGH *nichts aus. „Kardinalpflichten“* sind nach den aktuellen Urteilen des *OLG Frankfurt/M. „elementare berufliche Pflichten, deren Kenntnis nach der Lebenserfahrung bei jedem Berufsangehörigen vorausgesetzt werden kann.“*

Somit bleibt es bei der Rechtsprechung, dass eine Kardinalpflichtverletzung eine wissentliche Pflichtverletzung indiziert.

Dabei zeigt das aktuelle Urteil des 5. Senats des *OLG Frankfurt*[126] vom 20.11.2025 die besondere Relevanz von Kardinalpflichten (dazu eingehend unten):

Insoweit ist nachfolgend zu differenzieren:

Kardinalpflichtverletzungen können nach der aktuellen Rechtsprechung eine außerordentliche Kündigung rechtfertigen oder Schadensersatzansprüche der Gesellschaft oder Dritter begründen.

Solche zu sanktionierenden Pflichtverletzungen können bereits bei Eventualvorsatz oder sogar bei Fahrlässigkeit in Betracht kommen. Hierzu ist die Rechtsprechung noch nicht eindeutig.

Im Rahmen des Ausschlusses der Einstandspflicht der D&O-Versicherung nach den ULLA-Versicherungsbedingungen mag zwar ein Verstoß gegen Kardinalpflichten einen wissentlichen Pflichtverstoß i.S. der ULLA-Bedingungen indizieren.

Gleichwohl hat der BGH aufgrund der nicht eindeutigen Formulierungen in den ULLA-Bedingungen festgestellt, dass nur bewusst oder absichtlich vorsätzliche Verstöße gegen Gesetze als wissentlich im Sinne dieser Bedingungen die Versicherung legitimieren, den Eintritt zu verweigern.

Außerdem stellte der BGH klar, dass bzgl. jeder einzelnen haftungsbegründenden und schadensauslösenden Pflichtverletzung, für die die D&O-Versicherung nicht zahlen will, von der Versicherung dargelegt bzw. nachgewiesen werden muss, „*dass gerade die Pflichtverletzung wissentlich erfolgte, wegen der der Versicherte im konkreten Fall für einen Vermögensschaden auf Schadensersatz in Anspruch genommen wird.*“[127]

---

[126] *OLG Frankfurt*, Urteil vom 20.11.2025, Az. 5 U 15 / 25 („*Außerordentliche Kündigung eines Geschäftsführers bei Verstoß gegen Legalitätsprinzip als Kardinalpflicht*“).

[127] Vgl. *Seehaus*, Kurzanalyse des Urteils des BGH vom 19.11.2025 – IV ZR 66 / 25, ZInsO 2026, S. 899 ff.. Beispiel: Da nach Insolvenzreife nur bestimmte Zahlungen des Schuldners verboten und damit Pflichtverletzung sind, muss der Versicherer darlegen und beweisen, dass der zahlende Unternehmer (Schuldner) *bei der einzelnen bestimmten nicht erlaubten Zahlung, für die die D&O-Versicherung Ersatz leisten soll, wusste, dass er dies nicht durfte*.

Dass in der Praxis Versicherer jedoch versuchen, dem Versicherungsnehmer unter Hinweis auf eine (falsche) Rechtslage den Versicherungsschutz zu verweigern, zeigen viele Fälle des Unterzeichners:

Hier ein Original-Zitat aus dem Schreiben eines Bayerischen Versicherers an seinen Kunden vom 22.4.2026 im Bereich einer Unfallversicherung:

„(…) Die herrschende Rechtsprechung geht bei einer Falschbeantwortung von Fragen in der Unfallanzeige regelmäßig mindestens von einer vorsätzlichen Obliegenheitsverletzung aus, so dass wir gemäß Ziffer 8 der Allgemeinen Unfallversicherungsbedingungen von der Verpflichtung zur Leistung frei werden. Wir bitten um Verständnis, dass wir aus diesem Grund hier nicht weiter für Sie tätig werden können. (…)".

Insofern ist anzuraten, neben der Beachtung der Kardinalpflichten auch die Obliegenheiten im Rahmen der „Versicherungs-Compliance" zu checken, dokumentieren und dem Versicherer keinen Raum zu geben, dann über das Bestehen des Versicherungsschutzes zu streiten, wenn diese Frage existenziell wird.

14. Kardinalpflichten im Bereich Governance

Von der aktuellen Rechtsprechung wurden *Kardinalpflichten im Rahmen der Governance (gewissenhafte Führung und Überwachung von Organisationen*) statuiert.

Dabei haben sich in der Rechtsprechung bereits diverse Fallgruppen herausgebildet.

Fallgruppen:[128]

„(…) Für eine geschäftsführende Person (Vorstand einer Aktiengesellschaft, Geschäftsführer einer GmbH oder sonstigen Gesellschaft, leitender Angestellter) sollen zu diesen Kardinalpflichten gehören:

- *weder sich noch Dritten aus dem Unternehmensvermögen Vorteile zu gewähren, auf die kein Anspruch besteht,[129]*
- *das Unternehmensvermögen nicht für unternehmensfremde Zwecke zu verwenden,*
- *bei Insolvenzreife rechtzeitig Insolvenzantrag zu stellen,*
- *sich jederzeit über die wirtschaftliche Lage der Gesellschaft zu vergewissern[130] und eingehend zu prüfen, ob Insolvenzreife vorliegt: wer erkennt, dass die Gesellschaft zu einem bestimmten Stichtag nicht in der Lage ist, ihre fälligen und eingeforderten Verbindlichkeiten vollständig zu bedienen, hat die Zahlungsfähigkeit anhand einer Liquiditätsbilanz zu überprüfen (OLG Frankfurt, Urteil vom 5.3.2025 – 7 U 134/ 23 (…)".*

15. Erweiterung der Fallgruppen der Kardinalpflichtverletzung auf Governance-Compliance

Die aktuelle Rechtsprechung erweitert diese Fallgruppen nun

---

[128] Zitat aus: Wikipedia, Kardinalpflicht/Kardinalpfichten bei der Geschäftsführung, abrufbar unter: *https://de.wikipedia.org/wiki/Kardinalpflicht*.

[129] Vgl. hierzu BGH, Urt. v. 10.1.2023 – 6 StR 133/22, BGHSt 67, 225, („*Vergütung VW-Betriebsräte*") und BGH, Urt. v. 10.2.2022 – 3 StR 329/21, ZInsO 2022, 765 („*Haftung von Vorständen wegen Untreue bei Entscheidungen bei mangelhafter Informationsgrundlage*"). Vgl. hierzu ausführlich *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000 – erfolgreich umsetzen, auditieren und reporten, DIN Media, 2025, Kap. 6.8.

[130] Vgl. BGH, Versäumnisurt. v. 19.6.2012 – II ZR 243/11, ZInsO 2012, 1536, und BGH, Urt. v. 23.7.2024 – II ZR 206/22, ZInsO 2024, 1980, und OLG Nürnberg, Urt. v. 30.3.2022 – 12 U 1520/19, NZG 2022, 1058.

- auf die Pflicht zur Risiko- bzw. Krisenfrüherkennung und zum
- Krisenmanagement und
- auf die „*vielfältigen Pflichten in Bezug auf die Unternehmensleitung, die mit Eintragung als Geschäftsführer einer Kapitalgesellschaft verbunden sind*".

Zitat des *OLG Frankfurt/M.*:[131]

„Grundsätzlich setzt die Annahme einer Kardinalpflichtverletzung voraus, dass die (…) verletzte Rechtsnorm zu den zentralen, fundamentalen Grundregeln einer bestimmten Regelungsmaterie gehört."

„Die allgemein anerkannte (…) Pflicht zur Krisenfrüherkennung und zum Krisenmanagement bei haftungsbeschränkten Unternehmensträgern bestand schon vor Inkrafttreten des § 1 Abs. 1 StaRUG aus § 43 Abs. 1 GmbHG."

16. Exkurs: Risikofrüherkennung als notwendiger Bestandteil der Krisenfrüherkennung

Soweit § 1 StaRUG und die aktuelle Rechtsprechung von „*Krisenfrüherkennung*" und nicht „*Risikofrüherkennung*" sprechen, ist anzumerken, dass Risikofrüherkennung die unverzichtbare Vorstufe der Krisenfrüherkennung ist.

Die Risikofrüherkennung als zwingendes Element eines Überwachungssystems, um „bestandsgefährdende Entwicklungen frühzeitig zu erkennen", wurde bereits 1998 mit dem KonTraG in § 91 AktG als gesetzliche Pflicht für AG und (analog) für große GmbHs statuiert (vgl. die Gesetzgebungsmaterialien zum KonTraG und zum FiSG).

Da zumeist nicht ein einziges Risiko sich als bestandsgefährdend auswirkt, sondern viele sich aggregierende Einzelrisiken, ist auch im Rahmen der Krisenfrüherkennung zunächst auf Risikofrüherkennung mit Quantifizierung und Aggregation und Abgleich mit der Risikotragfähigkeit zu achten (was dazu führt, dass aufgrund der allgemeinen Pflicht zur gewissenhaften Geschäftsführung – § 43 GmbHG, § 93 AktG – auch bei Risiken unterhalb der Schwelle der Bestandsgefährdung angemessen gesteuert werden muss).[132]

- *Unzureichendes Risikomanagement und Aggregation zahlreicher Einzelrisiken als Hauptursache für Insolvenz*

In dem von einer anerkannten Wirtschaftsprüfungsgesellschaft testierten Lagebericht für eine vom Verfasser verwaltete Insolvenz heißt es:

„Darstellung der Lage: […] Ein Hauptgrund ist im fehlenden Risikomanagement zu sehen, was in einer unkontrollierten Häufung zahlreicher und für die Unternehmensgröße in Summe zu vieler Unternehmensrisiken führte."[133]

Durch ein funktionierendes Risiko-Managementsystem wäre hier großer Schaden vermieden worden: Ca. 73 Mio. € angemeldete Forderungen seitens der Gläubiger der Gruppe, ca. 50 Mio. davon wurden durch den Insolvenzverwalter festgestellt. Über Unternehmensfortführung, übertragende Sanierung, Absonderungen, Verwertung etc. konnten bisher an die Gläubiger ca. 17 Mio. € zurückfließen. Der Rest bleibt wohl unwiederbringlich verloren. Vielmehr müssen sie sich, um nicht sanktioniert zu werden, an zahlreiche rechtliche Vorgaben halten.

---

[131] Vgl. OLG Frankfurt/M., Urt. v. 5.3.2025 – 7 U 134/23, DStR 2025, 917, mit einem ähnlichen Fall (Rev. eingelegt, BGH – IV ZR 66/25).
[132] Vgl. *Scherer/Seehaus*, Governance und Compliance nach § 1 StaRUG, 2024, RiskNET.de, abrufbar unter: *https://www.risknet.de/themen/risknews/kontinuierliche-risikoueberwachung-in-echtzeit/*.
[133] Vgl. den veröffentlichten Lagebericht der N.N. Raumexklusiv GmbH für das Geschäftsjahr v. 1.1. bis zum 31.12.2012.

Zitat des OLG Frankfurt/M.:[134]

„Grundsätzlich setzt die Annahme einer Kardinalpflichtverletzung voraus, dass die (…) verletzte Rechtsnorm zu den zentralen, fundamentalen Grundregeln einer bestimmten Regelungsmaterie gehört."

„Die allgemein anerkannte (…) Pflicht zur Krisenfrüherkennung und zum Krisenmanagement bei haftungsbeschränkten Unternehmensträgern bestand schon vor Inkrafttreten des § 1 Abs. 1 StaRUG aus § 43 Abs. 1 GmbHG."

Die aktuelle Gerichtsentscheidung sieht hier – wohl zu Recht – § 43 GmbHG (Pflicht des GmbH-Geschäftsführers zur gewissenhaften Geschäftsführung) als Rechtsnorm an, die „*zu den zentralen, fundamentalen Grundregeln einer bestimmten Regelungsmaterie gehört*".

Damit ist konsequenterweise für Vorstände § 93 AktG (Pflicht des Vorstands einer AG zur gewissenhaften Geschäftsführung) inklusive § 93 Abs. 1 Satz 2 mit der Obliegenheit zur Einhaltung der sog. Business Judgment Rule) eine entsprechende Rechtsnorm, die zu den Kardinalpflichten zählt.

Und für Aufsichtsräte ist § 116 AktG, der auf § 93 AktG verweist, einschlägig.

Somit ist die Governance-Compliance[135] zu Recht als eine elementare berufliche Pflicht eines Geschäftsführers, Vorstandes oder Aufsichtsrats anzusehen.

Sicher wird bei jeder einzelnen Pflichtverletzung i.S.d. § 43 GmbHG bzw. §§ 93, 116 AktG zu prüfen sein, ob die jeweils fundamentalen Grundregeln der Regelungsmaterie verletzt wurden. Dies wird wieder eng mit der jeweiligen Risikolage bzgl. dieser Regelungsmaterie in Bezug auf die konkrete Organisation zusammenhängen.

So ist Risiko- und Krisenfrüherkennung und -management sicher für alle Organisationen fundamental, weil damit die Existenz der Organisation geschützt werden soll. Aktuell ähnlich wichtig für alle Organisationen dürften die Themen IT-Governance inklusive Informationssicherheit sein. Auch Nachhaltigkeitsrisiken dürften immer mehr zu diesen Risikobereichen gehören.

Generell würde eine angemessene (Compliance-) Risikoanalyse[136] in der individuellen Organisation Aufschluss darüber geben, welche (Rechts-)Bereiche mit den zugehörigen Pflichten zu den Kardinalpflichten zu zählen sind. Der risikobasierte Ansatz sieht Anforderungen mit dem Ziel der Vermeidung von Gefahr von Leib und Leben, erheblichen zivil- oder strafrechtlichen Sanktionen oder erheblicher finanzieller Einbußen, die die Risikotragfähigkeit beeinträchtigen, als besonders wichtig an.

17. Nun auch Legalitätspflicht nach *aktueller Rechtsprechung*[137] als Kardinalpflicht

Das Legalitätsprinzip,[138] bzw. die Pflicht zur Compliance, also die Pflicht aller, sich an verbindliche Regeln, wie Gesetze oder Rechtsprechung zu halten, hat sich in den letzten Jahren auch in der Rechtsprechung manifestiert:

---

[134] Vgl. OLG Frankfurt/M., Urt. v. 5.3.2025 – 7 U 134/23, DStR 2025, 917, mit einem ähnlichen Fall (Rev. eingelegt, BGH – IV ZR 66/25).

[135] Vgl. zu den Inhalten von Governance-Compliance: *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000 – erfolgreich umsetzen, auditieren und reporten, DIN Media, 2025.

[136] Vgl. DIN ISO 37301 Normabschnitt 4.6 Compliance-Riskoanalyse und ISO IEC 31010 Risk Assessment.

[137] Vgl. *OLG Frankfurt*, Urteil vom 20.11.2025, Az. 5 U 15 / 25 („*Außerordentliche Kündigung eines Geschäftsführers bei Verstoß gegen Legalitätsprinzip als Kardinalpflicht*").

[138] Vgl. BGH, Urt. v. 27.8.2010 – 2 StR 111/09, ZCG 2010, 285 (RWE-Tochter: Müllentsorgung und schwarze Kassen"), kommentiert in *Scherer*, Das interessiert Kapitalgeber: Antifragilität und der „Achilleskörper" des Ordentlichen Kaufmanns, 2019, abrufbar unter: https://www.scherer-grc.net/publikationen/das-interessiert-kapitalgeber-antifragilitaet-und-der-achilleskoerper-des-ordentlichen-kaufmanns

Beginnend mit dem „berühmten“ „Neubürger“-Urteil des LG München v. 10.12.2013[139] im Siemens-Compliance-Skandal, führten das LAG Düsseldorf,[140] das ArbG Frankfurt,[141] der BGH[142] und aktuell das OLG Nürnberg[143] aus, das es Obliegenheit des Geschäftsführers oder Vorstands sei, ein angemessenes und wirksames Compliance-Managementsystem einzurichten.[144]

Flankierend dazu entschied der BGH im „Buchhändler-Urteil“,[145] ein beruflich Tätiger habe das erforderliche Wissen bzgl. der für seine Tätigkeit relevanten Compliance-Anforderungen zu haben oder es sich über Experten zu besorgen. Darüber hinaus müsse er diese Anforderungen auch erfüllen. Die Befolgung der Empfehlung des Experten kann gemäß BGH in den „ISION-Entscheidungen“ enthaftend wirken.[146]

Aus der jahrelang kontinuierlichen Wiederholung der Rechtsprechung lässt sich schlussfolgern, dass Compliance- und Legalitätspflicht eine selbstverständliche Kardinalpflicht der Organe ist, was nun auch das OLG Frankfurt bestätigt hat:

Das Urteil des 5. Senats des *OLG Frankfurt*[147] vom 20.11.2025 statuiert Verstöße gegen das Legalitätsprinzip als Verletzung von Kardinalpflichten, die eine außerordentliche Kündigung rechtfertigen:

Einem GmbH-Geschäftsführer wurde nach Ansicht des *OLG Frankfurt* wirksam außerordentlich gekündigt, weil er gegen die *Kardinalpflicht der Beachtung des Legalitätsprinzips* verstoßen hatte:

„(…) Zuvorderst hat der (…) [Geschäftsführer, Anm. des Verf.] betreffend die Eingruppierung des Herrn E (…) gegen die ihm als ressortverantwortlicher Geschäftsführer obliegende Legalitätspflicht verstoßen.

***Der Geschäftsführer hat die gesetzlichen und statutarischen Vorgaben zu beachten. Diese Legalitätspflicht gilt ausnahmslos und ist eine Kardinalpflicht des Geschäftsführers**. Auch Satzungs- oder Gesetzesverstöße, die nach Meinung der Geschäftsführer im wohlverstandenen Interesse der Gesellschaft liegen (sog. nützliche Pflichtverletzungen), sind pflichtwidrig. (…).“*

Der Geschäftsführer oder Vorstand eines mehrköpfigen Gremiums kann sich auch nicht dadurch entlasten, weil er gemäß Geschäftsverteilung nicht primär zuständig gewesen sei:

Exkurs: Pflichten und Haftung im mehrköpfigen Gremium gemäß *OLG Frankfurt*

„(…) Den Kläger entlastet es entgegen seiner Auffassung nicht, dass innerhalb der Geschäftsführung überwiegend Herr A für das Ressort Personal zuständig war.

Sind - wie im Streitfall - die verschiedenen Aufgaben der Geschäftsführung zwischen mehreren Geschäftsführern (horizontal) verteilt, wandelt sich die sog. Leitungspflicht zur Pflicht zur Überwachung der jeweils

---

[139] Das sog. „Siemens/Neubürger-Urt.“ des LG München I, Urt. v. 10.12.2013 – 5 HK O 1387/10, NZG 2014, 345, gilt als richtungsweisendes Urteil zur organisationsbezogenen Haftung von Vorständen in AG. Im Zentrum stand die Frage, ob der ehemalige Siemens-Vorstand *Dr. Uriel J. Neubürger* gegen seine Sorgfaltspflichten gem. § 93 Abs. 1 AktG verstoßen habe, indem er defizitäre Compliance-Strukturen im Konzern nicht angemessen verbessert habe. Das Gericht bejahte die persönliche Haftung und stellte klar, dass Vorstandsmitglieder auch dann haften, wenn sie Organisationspflichten verletzen, insbesondere bei unzureichender Kontrolle von Korruptionsrisiken und internen Kontrollsystemen. Dabei wurde betont, dass die Pflicht zur Etablierung eines funktionierenden Compliance- oder Risikomanagementsystems nicht delegierbar sei und zu den zentralen Leitungsaufgaben eines Vorstands gehört. Ein bloßes Vertrauen auf nachgeordnete Stellen entlaste nicht von der Verantwortung.

[140] Vgl. LAG Düsseldorf, Urt. v. 27.11.2015 – 14 Sa 800/15, Rn. 242 (Schienenkartell-Urteil).

[141] Vgl. ArbG Frankfurt, Urt. v. 11.9.2013 – 9 Ca 1541/13 (Libor-Manipulation).

[142] Vgl. BGH, Urt. v. 15.1.2013 – II ZR 90/11, NJW 2013, 1958 Rn. 22 (unternehmenszweckwidrige Derivatgeschäfte) und BGH, Urt. v. 9.5.2017 – 1 StR 265/16, NJW 2017, 3798 (Panzerhaubitzenfall).

[143] Vgl. OLG Nürnberg, Urt. v. 30.3.2022 – 12 U 1520/19, NZG 2022, 1058.

[144] Vgl. *Scherer*, Compliance-Managementsystem nach DIN/ISO 37301 erfolgreich, implementieren, integrieren, auditieren, zertifizieren, DIN Media Verlag, 2022, 39.

[145] Vgl. BGH, Urt. v. 18.11.2020 – 2 StR 246 /20, wistra 2021, 355.

[146] Vgl. *Scherer*, Compliance-Managementsystem nach DIN/ISO 37301 erfolgreich, implementieren, integrieren, auditieren, zertifizieren, DIN Media, 2022, 233: „Wer soll das alles wissen?“.

[147] *OLG Frankfurt*, Urteil vom 20.11.2025, Az. 5 U 15 / 25 (*„Außerordentliche Kündigung eines Geschäftsführers bei Verstoß gegen Legalitätsprinzip als Kardinalpflicht*“).

zuständigen Ressortgeschäftsführer. Für Fehler, die in einem Nachbarressort passieren, sind die Geschäftsführer nur verantwortlich, wenn ihnen eine mangelnde Überwachung des zuständigen Geschäftsleiters vorzuwerfen ist. Die gegenseitige Kontrolle der Entscheidungsträger in wichtigen Angelegenheiten ist Ausdruck der Gesamtverantwortung des Leitungsorgans und entspricht insoweit auch dem Sinn und Zweck eines mehrköpfigen Führungsorgans. Eine zulässige horizontale Delegation bewirkt somit eine Veränderung bei der Verantwortlichkeit der Geschäftsleiter:

Aus der Verantwortung für die sorgfältige Wahrnehmung der Aufgabe wird eine Verantwortung für die angemessene Überwachung der Leitungskollegen. Diese Überwachungspflicht besteht latent immer, verpflichtet aber grundsätzlich nur anlassbezogen zu konkreten Maßnahmen, wie beispielsweise Rückfragen, Bitten um Unterlagen, Thematisierung in Leitungssitzungen oder Einschaltung von Kontrollstellen im Unternehmen (vgl. BGH, Urt. v. 6.11.2018 - II ZR 11/17) (…).

Dem Kläger oblag daher eine Kontroll- und Überwachungspflicht gegenüber dem Mitgeschäftsführer Herrn A, die hinsichtlich der Wahrnehmung von nicht übertragbaren Aufgaben wie etwa die Einstandspflicht des Geschäftsführers für die Gesetzmäßigkeit der Unternehmensleitung auch weitgehend war (vgl. zum Umfang der Kontrollpflicht BGH, Urt. v. 23.7.2024 - II ZR 206/22) (…).

Nach Auffassung des Senats hatte der Kläger begründeten Anlass, die Tätigkeit von A im Zusammenhang mit verschiedenen Höhergruppierungen und Zulagengewährungen der Betriebsratsmitglieder E, F und G sowie des Schwerbehindertenvertreters H zu kontrollieren und geeignete Maßnahmen zu ergreifen, um zu gewährleisten, dass die entsprechenden, auch von ihm (…) unterzeichneten Entscheidungen der Geschäftsführung dem Legalitätsprinzip entsprechen. (…)

Da der Kläger gemäß § 43 Abs. 1 GmbHG verpflichtet war, die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden, hatte er die ihm hier obliegende Kontrolle auf angemessen informierter Basis wie jemand in leitender Stellung eines Verwalters fremden Vermögens auszuüben. Nach diesem Sorgfaltsmaßstab (…) bestand jedenfalls Gesprächsbedarf. (…)“

Auch der Entlastung durch Berufung auf eingeholten Rechtsrat sind enge Grenzen gesetzt:

Enthaftung durch Einholung externen Rechtsrats

„ (…) Soweit der Kläger unter Bezugnahme auf die Rechtsprechung des Bundesgerichtshofs im Urt. v. 28.4.2015 - II ZR 63/14 (…) der Auffassung ist, er habe auf den eingeholten Rechtsrat vertrauen dürfen, lässt er unberücksichtigt, dass der Bundesgerichtshof in vorgenannter Entscheidung aufgezeigt hat, dass der Organwalter bei Einholung von Rechtsauskunft als Rechtsunkundiger zwar keine rechtliche Prüfung der erhaltenen Rechtsauskunft vornehmen, jedoch prüfen müsse, ob dem Berater nach dem Inhalt der Auskunft alle erforderlichen Informationen zur Verfügung standen, er die Informationen verarbeitet und alle sich in der Sache für einen Rechtsunkundigen aufdrängenden Fragen widerspruchsfrei beantwortet hat oder sich aufgrund der Auskunft weitere Fragen aufdrängen. Vorliegend waren - wie aufgezeigt - jedenfalls nicht alle sich auch dem Rechtsunkundigen aufdrängenden Fragen widerspruchsfrei beantwortet. (…)“

Anforderungen an ein Kontrollsystem

„(…) Trotz dieser - nicht abschließenden - greifbaren Anhaltspunkte für Unregelmäßigkeiten (…) hat der Kläger keine hinreichenden Kontrollmaßnahmen ergriffen, um seine Überwachungspflicht zu erfüllen. Vortrag dazu hält der Kläger weder erst- noch zweitinstanzlich. Im Gegenteil behauptet er, Herrn A vertraut und ohne Detailkenntnis mitunterzeichnet zu haben. Soweit er der Auffassung ist, er sei der Überwachungspflicht dadurch nachgekommen, dass es ein funktionierendes Kontrollsystem derart gegeben habe, dass Personalentscheidungen von der Personalabteilung und einem Personalausschuss begleitet worden seien und anwaltlicher Rat eingeholt worden sei, entlastet dies den Kläger nicht. Wie aufgezeigt, kann von einem Kontrollsystem nicht im Ansatz gesprochen werden, (…) Für sich genommen reichte der bloße Wunsch um einen Gesprächstermin nicht aus, um in der konkreten Situation als Sachwalter des Vermögens der Beklagten wirtschaftlichen Schaden von dieser abzuhalten.

Dass der Kläger wie ausgeführt seine Überwachungspflicht bei den vorstehend aufgezeigten unzulässigen Begünstigungen der Mandatsträger verletzt hat, stellt einen wichtigen Grund zur außerordentlichen Kündigung des Geschäftsführeranstellungsvertrages dar. (…)“

Zwischenfazit:

Wer wissentlich (dolus eventualis, also das „Für-möglich-halten und sich-damit-abfinden" reicht[148]) gesetzliche Vorgaben missachtet, verstößt also vorsätzlich gegen grundlegende Berufspflichten, die sog. Kardinalpflichten.

Dass vorsätzliche Gesetzesverstöße in nahezu allen Rechtsgebieten (Strafrecht, Versicherungsrecht, Vertragsrecht etc.) streng sanktioniert werden, dürfte nicht überraschen.

Gegenmeinungen, die mittelbar argumentieren, Vorstand oder Geschäftsführer sei kein Beruf, der eine bestimmte Qualifikation voraussetzen würde, wird durch den Hinweis des *BGH*,[149] ein Geschäftsführer, der sich haftungsbefreiend von der Gesellschaft trennen möchte, müsse sein Amt niederlegen, der Boden entzogen.

Ebenso sieht es der *BFH*, der ausführte:

„[…] wer den Anforderungen an einen gewissenhaften Geschäftsführer nicht entsprechen kann, muss von der Übernahme des Geschäftsführeramtes absehen, bzw. dieses Amt niederlegen. […]"[150]

Es ist sicher nicht einfach, stets alle Compliance-Anforderungen zu erfüllen. Es wird aber bzgl. der Kardinalpflichten primär gefordert, dass nicht *vorsätzlich* Compliance-Pflichten verletzt werden.

Ob auch fahrlässige Verletzungen des Legalitätsprinzips zur Annahme einer Kardinalpflichtverletzung führen, kann dem Urteil des 37. Senats des *OLG Frankfurt* nicht entnommen werden.

Flankierend zur verschärften Kardinalpflicht-Haftungs-Rechtsprechung entwickelte die Rechtsprechung[151] das *Korrektiv der enthaftenden Wirkung eines Compliance-Managementsystems*: Bei Pflichtverstößen unterhalb der Leitungsebene kann bei Existenz eines Compliance-Managementsystems der Vorwurf des Organisationsverschuldens im Sinne einer Aufsichtspflichtverletzung entfallen. Das System muss sich dann natürlich auch gerade um diese Kardinalpflichten und sonstigen relevanten Themen gekümmert haben, in denen sich trotz aller Maßnahmen noch ein Verstoß ereignete.

Diese Entwicklung der Rechtsprechung und zumindest das *Risiko* der Annahme einer Kardinalpflichtverletzung bei vorsätzlichen Complianceverstößen (bereits bei dolus eventualis) kann enorme Auswirkungen auf Organe und Führungskräfte haben und sollte im Risiko- und Compliancemanagement angemessen reflektiert werden.

18. Korrektiv der enthaftenden Wirkung eines angemessenen Governance-Compliance-Managementsystems und bei Mitarbeiter-Exzess

Die Aufgaben der Risiko- und Krisenfrüherkennung, Compliance, Informationssicherheit und Business Continuity, aber auch relevante Transformationsbereiche, wie Digitalisierung und Organisationsentwicklung werden häufig auf die entsprechenden Stabsstellen bzw. Lines of Defense-Funktionen delegiert. Diese arbeitsteilige Struktur ist betriebswirtschaftlich sinnvoll – sie

[148] Lediglich im Rahmen der D&O-Versicherung ist für die Versagung des Versicherungsschutzes eine wissentliche oder gar absichtliche Verletzung von Compliance-Pflichten erfordrerlich.
[149] Beschl. v. 21.5.2019 – II ZR 337/17.
[150] Vgl. BFH, Beschl. v. 15.11.2022 – VIII R 23/19, LS Rn. 35, BFHE 278, 392.
[151] BGH 2017: (KMW), Urt. v. 9.5.2017; BGH 2022: (Selbstreinigung), Urt. v. 27.4.2022; BGH 2023 (Geschäftsverteilung), Urt. v. 9.11.2023; EuGH 2023: (Deutsche Wohnen), Urt. v. 5.12.2023; EuGH 2023: (Hackerangriff), Urt. v. 14.12.2023; EuGH 2024: (USt-Betrug), Urt. v. 30.1.2024; EuGH 2024: Urt. v. 11.4.2024 – C-741/21, NJW 2024, 1561; OLG Stuttgart 2025: (Mitarbeiterexzess), Beschl. v. 25.2.2025 – 2 ORbs 16 Ss 336/24, NJW 2025, 1279.

ändert jedoch nichts an der originären Verantwortung der Geschäftsleitung (Geschäftsherrenverantwortung).

Sofern die Delegationsempfänger, also die jeweils qua delegatione verantwortlichen Führungskräfte ihre Aufgaben nicht oder nicht ordnungsgemäß erfüllen und dadurch die Organisation oder Dritte zu Schaden kommen, stellt sich die Frage nach der (Haftungs-)Verantwortung der Organe und Delegationsempfänger.

Bei pflichtwidrigem Handeln oder Unterlassen der Delegationsempfänger im Rahmen ihrer betrieblichen Tätigkeit kann ein Aufsichtsverschulden der Organe vorliegen, jedoch ein angemessenes Compliance-Managementsystem enthaftend wirken.[152]

Sofern die Delegationsempfänger aufgrund der Verfolgung eigener, unternehmensfremder Ziele nicht pflichtgemäß agieren, stellt sich die Frage, ob die Organe auch für einen sog. „Mitarbeiterexzess“ verantwortlich sind.

Beispiel im Kontext der Erfüllung der Überwachungspflichten

Liegt Mitarbeiter-Exzess vor, wenn trotz Kenntnis der relevanten und riskanten Schwachstellen in der Organisation die Lines of Defense-Funktion ohne Kenntnis oder gar Weisung durch die Organe bewusst andere Themen prüft und reported?

Dogmatisch liegt in Fällen des Mitarbeiterexzesses ein Verhalten außerhalb des Weisungsrechts und der arbeitsvertraglichen Bindung vor. [153] Das Unternehmen und dessen Geschäftsleiter haftet dann grds. nicht als „Verantwortlicher“ i.S.v. Art. 4 Nr. 7 DSGVO, § 831 oder § 278 BGB.

Maßgeblich für die Zurechnung ist, ob die Handlung noch innerhalb des vom Arbeitgeber übertragenen Aufgabenbereichs liegt – was sich regelmäßig aus Stellenbeschreibungen, Arbeitsverträgen, Dienstanweisungen oder konkreten Einzelaufträgen ergibt. Handelt ein Mitarbeiter innerhalb dieses Rahmens – selbst weisungswidrig –, bleibt das Verhalten grds. dem Unternehmen zurechenbar. Erst wenn der Handlungsrahmen objektiv überschritten und der Bezug zum Unternehmenszweck vollständig verloren ist, liegt ein echter Exzess vor. Der Exzess führt grds. zur Eigenverantwortlichkeit des Mitarbeiters.[154]

Der Mitarbeiterexzess wirft grundlegende haftungsrechtliche Fragen auf. Weder die Rechtsprechung noch die Literatur haben bislang ein konsistentes Kriteriensystem entwickelt, das die dogmatischen Voraussetzungen, Reichweiten und Grenzen der Zurechnung bei Überschreitungen des Pflichtenkreises einzelner Mitarbeitender hinreichend konturiert. Ob die Schwelle zur Enthaftung erreicht ist, bedarf daher stets einer sorgfältigen und differenzierten Einzelfallanalyse.

19. Governance-Compliance-Zertifizierungen

Einige für Compliance-Managementsysteme akkreditierte Zertifizierungsstellen bieten mittlerweile Kombi ISMS-KI-CMS-Zertifizierungen nach DIN ISO 37301 und ISO 27001 oder ISO 42001 mit einem besonderem Scope des Audits auf (IT- / KI-) Governance-Compliance in Anlehnung an DIN ISO 37000 und ISO/IEC 38500 an.

---

[152] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000 – erfolgreich umsetzen, auditieren und reporten, DIN Media, 2025, Kap. 4.2 „Governance und Delegation“.

[153] BGH, Urt. v. 20.10.2011 – 4 StR 71/11, BGHSt 57, 42.

[154] Vgl. die zitierte Rechtsprechung bei *Scherer, Seehaus,* Pflicht zu Governance mit Risikofrüherkennung, Resilienz, und Transformation als Kardinalpflicht von Organen und Führungskräften, ZInsO 2025, S.1515 ff., zum kostenlosen Download im Internet.

Viele unserer im Bereich Compliance und IT-/ KI-Governance betreuten Mandanten gehören zu den deutschlandweit ersten Unternehmen, die von der einzigen[155] für ISO 37301- (CMS) DAkkS-akkreditierten Zertifizierungsstelle zertifiziert wurden:

„Die Zertifizierung zeigte aufgrund der wichtigen Governance-Compliance-Themen den Wertbeitrag der in Bezug auf QM, Umwelt etc. integrativen Funktion eines Compliance-Managementsystems – eine wertvolle Investition."

Zitat des Vorstandes der Karl-Gruppe, Hengersberg

20. Wertbeiträge und Ausblick

Investitionen in Digitalisierung mit KI, Governance, Risk und Compliance kosten zunächst Geld. Aber sie verstärken Resilienz und bedeuten nachhaltige Unternehmenswertsteigerung und Zukunftsfähigkeit. Ein weiterer derzeit unverzichtbarer Wertbeitrag eines Governance-Compliance-Managementsystems ist die – gemäß ständiger höchstrichterlicher Rechtsprechung[156] – *enthaftende Wirkung für Geschäftsführung, Aufsichtsrat, Management, Abteilungsleiter, Compliance- und Risikomanager und sonstige Beschäftigte*.[157]

Die unzähligen schwerwiegenden täglichen Ereignisse mit Gefahren für Leib und Leben, p**er**sönlichen Haftungsgefahren für Organe und sämtliche Beschäftigten einer Organisation oder erheblichen finanziellen Schäden bis hin zur Insolvenzverursachung zeigen, dass das Thema Governance nicht sensibel genug behandelt werden kann.

Die aus der Governance abzuleitenden zwingenden Anforderungen und Maßnahmen erscheinen erschlagend, sind es aber nicht. Sofern die Governance als Klammer über dem Integrierten Managementsystems (IMS) geführt wird, ergeben sich zum einen zahlreiche Überschneidungen mit bereits im IMS vorhandenen Elementen, zum anderen werden die korrekt zu erledigenden Aufgaben auf viele Schultern verteilt.

Governance ist primär „Chefsache", also von der Unternehmensleitung (z.B. Geschäftsführer, Vorstand) in Primär- und Letztverantwortung zu übernehmen. Nur durch rechtssichere Pflichtendelegation können Aufgaben und Verantwortung auf kompetente andere Funktionen delegiert werden.

Governance heißt aber auch, dass das Thema in der Überwachungsverantwortung des Aufsichtsgremiums bzgl. der Geschäftsführung und der Weisungsbefugnis des Gesellschafters liegt. All das, was im Themenfeld Governance getan werden muss, muss (!) getan werden. Das ist reine Compliance ohne Ermessensspielraum bzgl. des „Ob" und damit gebundene Entscheidung. Da gibt es auch keinen Risiko-Appetit und kein Pareto-Prinzip. Da gibt es nur den „risikobasierten Ansatz": Statt alles gleichzeitig – was ja unmöglich ist: Das Wichtigste zuerst! Um nicht aufgrund des Vorwurfs einer nicht rechtssicheren Organisation in die persönliche Haftungsfalle zu stolpern, ist ein *enthaftendes*[158] *Governance-Compliance-Managementsystem* unverzichtbar.

---

[155] Stand 05/2025.

[156] Vgl. u.a. BGH 2017: (KMW), Urt. v. 9.5.2017; BGH 2022: (Selbstreinigung), Urt. v. 27.4.2022; BGH 2023 (Geschäftsverteilung), Urt. v. 9.11.2023; EuGH 2023: (Deutsche Wohnen), Urt. v. 5.12.2023; EuGH 2023: (Hackerangriff), Urt. v. 14.12.2023; EuGH 2024: (USt-Betrug), Urt. v. 30.1.2024; EuGH 2024: (juris), Urt. v. 11.4.2024; OLG Stuttgart, Beschl. v. 25.2.2025 – 2 ORbs 16 Ss 336/24, NJW 2025, 1279 (Mitarbeiter-Exzess).

[157] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000 – erfolgreich umsetzen, auditieren und reporten, DIN Media, 2025, Kap. 4.2 „Governance und Delegation".

[158] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000 – erfolgreich umsetzen, auditieren und reporten, DIN Media, 2025, Kap. 4.2 „Governance und Delegation".

Autorenprofil Prof. Dr. jur. Josef Scherer

Prof. Dr. jur. Josef Scherer ist Rechtsanwalt und Consulter, Gründer (2012) und Leiter des Internationalen Instituts für Governance, Management, Risk- und Compliance-Management und Leiter der Stabsstelle ESGRC der Technischen Hochschule Deggendorf (THD). Seit 1996 ist er Professor für Unternehmensrecht (Compliance), Risiko- und Krisenmanagement, Sanierungs- und Insolvenzrecht an der THD. Zuvor arbeitete er als Staatsanwalt an diversen Landgerichten und als Richter am Landgericht in einer Zivilkammer.

Neben seiner Tätigkeit als Seniorpartner der auf Wirtschaftsrecht und Governance, Risiko- und Compliance-Management (GRC) spezialisierten Kanzlei Prof. Dr. Scherer & Partner mbB erstellt er wissenschaftliche Rechtsgutachten und agiert als Richter in Schiedsgerichtsverfahren. Von 2001 bis 2024 arbeitete er auch als Insolvenzverwalter in verschiedenen Amtsgerichtsbezirken.

Prof. Dr. Scherer ist in diversen Unternehmen und Körperschaften als Compliance-Ombudsperson oder externer Compliance-Beauftragter tätig. Er ist gesuchter Referent bei Managementschulungen in namhaften Unternehmen sowie im Weiterbildungsprogramm des Senders BR-alpha und der Virtuellen Hochschule Bayern (VHB).

In Kooperation mit dem TÜV konzipierte er als Studiengangsleiter den seit über 15 Jahren renommierten und akkreditierten berufsbegleitenden Masterstudiengang Risikomanagement und Compliance-Management an der THD und leitet den Zertifikatskurs „Nachhaltigkeit und GRC“ sowie den berufsbegleitenden Bachelor „Nachhaltigkeit, Governance und Digitalisierung“.

Seit 2015 ist Prof. Dr. Scherer Mitglied des Beirats des Instituts für Risikomanagement und Regulierung (FIRM), Frankfurt (www.firm.fm). Seit 2016 ist er Mitglied des DIN-Normenausschusses Dienstleistungen (Arbeitsausschuss Personalmanagement NA 159-01-19 AA) zur Erarbeitung von ISO/DIN-Standards im Personalmanagement und seit 2017 Mitglied der Delegation ISO TC 309 Governance of Organizations (Arbeitsausschuss Governance und Compliance NA 175-00-01-AA) zur Erarbeitung von ISO/DIN-Standards im Bereich Unternehmensführung und -überwachung (Corporate Governance), Compliance und Whistleblowing.

Seit 2016 ist Prof. Dr. Scherer Fachlicher Leiter der „User Group Nachhaltige Unternehmensführung (ESG/CSR/GRC) und Compliance“ der Energieforen Leipzig, seit 2018 Mitglied der Arbeitsgruppe 252.07 von Austrian Standards International zur Erarbeitung einer ÖNORM D 4900 ff. (Risiko-Managementsystem-Standards), seit 2021 Mitglied im DICO (Deutsches Institut für Compliance e. V.) und seit 2025 Mitglied des Arbeitskreises Krisenfrüherkennung.

Seine Forschungs- und Tätigkeitsschwerpunkte liegen auf den Gebieten Nachhaltigkeit (ESG), Integrierte ESGRC-Managementsysteme, Governance-, Risiko- und Compliance-Management, Managerenthaftung, Integrierte Human-Workflow-Managementsysteme und Digitalisierung sowie Vertrags-, Produkthaftungs-, Sanierungs- und Insolvenzrecht, Arbeitsrecht und Personalmanagement.

Prof. Dr. Scherer ist auf dem Gebiet angewandte Forschung und Lösungen / Tools im Bereich ESG/GRC, Digitalisierung und integrierte Workflow-Managementsysteme Gesellschafter-Geschäftsführer der Governance-Solutions GmbH und Aufsichtsrat in diversen Unternehmen und Stiftungen.

www.scherer-grc.net

Prof. Dr. Josef Scherer

Der Verfasser publiziert über LinkedIn regelmäßig aktuelle Urteile, Gesetze, Artikel etc. zu ESGRC-Themen.