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.

Josef Scherer, 15.6.2026[1]

Neues Unternehmenssanktionsrecht, Legalitätspflicht und Criminal Compliance, auch bei KI-Einsatz

Summary

Nachfolgender Artikel[2] behandelt u.a. die Governance-Pflichten der Führungskräfte[3] und die *aktuelle Entwicklung der Gesetzgebung zum Unternehmenssanktionsrecht* nebst höchstrichterlicher Rechtsprechung[4] zum Thema „*Legalitäts- und Kardinalpflichten von Führungskräften, wissentliche Pflichtverletzung und Auswirkung auf D&O-)Versicherungen*“, auch beim Einsatz von *KI.*

Die Bundesregierung brachte am 26.5.2026 einen *Gesetzentwurf zur Änderung des Strafrechts - Umsetzung der EU-Richtlinie 2024 / 1203 zum strafrechtlichen Schutz der Umwelt etc. …* - (BT-Drucksache 21 / 6133 vom 26.5.2026) in den Bundestag ein. In diesem Gesetzesentwurf befanden sich auch Vorschläge für die Änderung des Ordnungswidrigkeitenrechts.

Insbesondere sollten Bußgeldhöchstbeträge für Unternehmen bis 40 Mio. EUR (bei Vorsatz) bzw. 20 Mio. EUR (bei Fahrlässigkeit) vorgesehen werden.

Der Bundesrat beschloss in seiner Stellungnahme vom 12.6.2026 Interessantes in Richtung Unternehmenssanktionsrecht: Die bußgeldmindernde Wirkung von Compliance-Maßnahmen findet sich in § 30 Abs. 2a OWiG der Stellungnahme.

---

[1] Das Bild mit Hund wurde mithilfe von KI generiert. Manchmal ist ein Hundebild attraktiver als Compliance .. Der Artikel ist meinem Sohn Valentin gewidmet. Er wünscht sich primär einen Hund.

[2] Dieser Artikel fußt auf *Scherer,* Legalitätspflicht als Kardinalpflicht, 6 / 2026 und *Scherer, Romeike*, Vom Geschäftsrisiko zur persönlichen Haftung, 4/ 2026: alle Artikel *zum* kostenlosen Download im Internet.

[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*“).

In § 130 OWiG sollen nicht abschließend („insbesondere“) *fünf Aufsichtsmaßnahmen* kumulativ gefordert (nicht lediglich als bußgeldmindernd wirkend statuiert) werden:

Rechtssichere Pflichtendelegation[5],

Compliance-Risikoanalyse[6],

Compliance-Richtlinien mit Schulungen[7],

Hinweisgebersysteme (Whistleblowing)[8],

angemessene interne Untersuchung und Sanktionen bei Pflichtverletzungen (Internal Investigations)[9].

Abgelehnt wurde der Vorschlag einer zwingenden Sanktionsmilderung bei Kooperation mit Ermittlungsbehörden.

Bereits Monate zuvor wurde seitens der Rechtsprechung festgestellt, dass die *Beachtung der Legalitätspflicht, also von Compliance, zu den „wesentlichen Berufspflichten“ von Organen und sonstigen Führungskräften* gehört.[10] Dies zeitigt enorme Auswirkungen auf die persönliche Haftungs-Verantwortung. Dies müssten neben Geschäftsführern, Vorständen, Aufsichtsräten, weiteren Führungskräften, Lines of Defense-Funktionen, Abschlussprüfer, Aufsichtsbehörden etc. auch die Verantwortlichen für Qualitäts-, Risiko-, Compliance-, KI- und Informationssicherheits-Managementsysteme beachten.

Ein *Managersicherheitspaket* inkl. Absicherung des Privatvermögens[11] und ein *Integriertes (IT- / KI-) Governance-Compliance-Managementsystem* lösen effektiv und effizient die angesprochenen Probleme und bringen Sicherheit, Struktur, Resilienz, Zukunftsfähigkeit und Erfolg.

---

[5] Vgl. *Scherer,* Compliance-Managementsystem nach DIN ISO 37301, DIN Media, 2022, Kapitel 4.5 und 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.

[6] Vgl. *Scherer,* Compliance-Managementsystem nach DIN ISO 37301, DIN Media, 2022, Kapitel 4.6.

[7] Vgl. *Scherer,* Compliance-Managementsystem nach DIN ISO 37301, DIN Media, 2022, Kapitel 4.5.

[8] Vgl. *Scherer,* Compliance-Managementsystem nach DIN ISO 37301, DIN Media, 2022, Kapitel 8.2.

[9] Vgl. *Scherer,* Compliance-Managementsystem nach DIN ISO 37301, DIN Media, 2022, Kapitel 8.2.

[10] Vgl. *Scherer,* Legalitätspflicht als Kardinalpflicht, 6 / 2026 *zum* kostenlosen Download im Internet.

[11] 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.

Durch die aktuelle Rechtsprechung[12] zur Haftungs-Verantwortung *auch* bei Nutzung von KI wird das Thema noch relevanter und aktueller.

1. Entwurf der Bundesregierung und Stellungnahme des Bundesrates

Text der Stellungnahme des Bundesrates vom 12.6.26 - Drucksache 266/26 (Beschluss) S. 20 ff. - zum Abschnitt § 130 Abs. 1, S. 3 OWiG neu:

*„**15. Zu Artikel 3 Nummer 3 – neu – (§ 130 Absatz 1 Satz 2, 3 – neu – OWiG)**[13]*

Nach Artikel 3 Nummer 2 ist die folgende Nummer 3 einzufügen:

3. § 130 Absatz 1 Satz 2 wird durch die folgenden Sätze ersetzt:

„Erforderlich sind solche Aufsichtsmaßnahmen, die unter Berücksichtigung von Größe, Art und Organisation des Betriebes oder Unternehmens und der von ihm ausgehenden Gefahren geeignet und zumutbar sind. Geeignete Maßnahmen sind insbesondere

1. die sorgfältige Auswahl, Unterweisung und Überwachung von Mitarbeitern und Aufsichtspersonen,

2. die regelmäßige Ermittlung und Bewertung vom Betrieb oder Unternehmen ausgehender Gefahren der Begehung von Straftaten und Ordnungswidrigkeiten,

3. der Erlass und die Fortentwicklung von Richtlinien und Weisungen sowie die Schulung der Mitarbeiter zum Zweck der Verhinderung von unternehmensbezogenen Straftaten und Ordnungswidrigkeiten,

4. ein Verfahren, das es den Mitarbeitern unter Wahrung von Vertraulichkeit ermöglicht, Hinweise auf mögliche unternehmensbezogene Straftaten oder Ordnungswidrigkeiten an eine geeignete Stelle zu geben, und

5. die Aufklärung von Verdachtsmomenten, die auf unternehmensbezogene Straftaten oder Ordnungswidrigkeiten hindeuten, sowie die Ahndung entsprechenden Fehlverhaltens.“'

Begründung:

*Die vorgeschlagene Änderung dient dazu, für **Unternehmen (Verbände)** und andere Rechtsanwender einen **gesetzlichen Referenzmaßstab für die Anforderungen an eine ordnungsgemäße Aufsicht und Organisation zu schaffen und zugleich einen Anreiz für die Einrichtung und Fortentwicklung von Compliance-Systemen** zu bilden.*

Im Einzelnen:

*(1) „Compliance“ steht für die Gesamtheit der Bemühungen in einem Verband, Fehlverhalten zu verhindern und aufzudecken sowie sicherzustellen, dass die Verbandsaktivitäten in Übereinstimmung mit den geltenden Gesetzen, Vorschriften und Regeln durchgeführt werden**. Die Wurzel von Compliance liegt in der Legalitätspflicht des Verbands in ihrer besonderen Ausprägung der Legalitätskontrollpflicht.***

Rechtsgrundlage von Compliance ist damit das Gesetz als Summe aller Normen des kodifizierten Rechts. Durch die hohe und weiter anwachsende Regelungsdichte und die oftmals nur relativ unbestimmt gehaltenen gesetzlichen Vorgaben stehen Verbände zum Teil vor der Schwierigkeit, die für ihren Betrieb erforderlichen Maßnahmen zu bestimmen.

Für Verbände ist daher zum Teil auch nicht hinreichend vorhersehbar, ob ein Gericht ex post die ergriffenen Maßnahmen als ausreichend ansehen wird. Zugleich müssen Compliance-Maßnahmen auf den spezifischen Verband ausgerichtet sein. Die primäre Compliance-Verpflichtung eines Verbands muss also vor allem darauf abzielen, für seine konkrete Struktur und sein konkretes Geschäftsfeld die spezifischen Risiken zu identifizieren und speziell zugeschnittene Gegenmaßnahmen zu installieren.

---

[12] Vgl. z.B. *LG München I*, Urteil vom 28.5.2026, Az. 26 O 869 / 26 („Snippet“) und unten Punkt 7.

[13] Hervorhebungen in fett durch den Verfasser.

Diese Notwendigkeit zur individualisierenden Einzelfallbeurteilung steht einer gesetzlichen Konkretisierung bei der Formulierung von allgemeinen Anforderungen an Compliance-Systeme aber nicht grundsätzlich entgegen. Vielmehr liegt es in der gesetzgeberischen Gestaltungsmacht und auch Verantwortung, jedenfalls allgemeine Vorgaben zu den Anforderungen an geeignete Compliance-Systeme zu normieren. Eine solche gesetzgeberische Konkretisierung findet sich bereits in anderen Rechtsordnungen. Sie gibt Verbänden zumindest eine Leitlinie an die Hand, bei Einhaltung welcher Maßnahmen das Risiko von Verbandsgeldbußen nach §§ 30, 130 OWiG reduziert werden kann. Dadurch können die ***Rechtssicherheit*** *gerade auch in kleinen und mittleren Unternehmen (KMU)* ***verbessert****, die Einschätzung des Umfangs notwendiger Compliance-Maßnahmen erleichtert und Maßnahmen zu rechtstreuem Verhalten gefördert werden.*

Als Anknüpfungspunkt für derartige Vorgaben bietet sich die Bußgeldvorschrift zur Verletzung der Aufsichtspflicht in Betrieben und Unternehmen (§ 130 OWiG) an. Die Regelung statuiert eine Verantwortlichkeit der Unternehmensleitung, die durch unzureichende Aufsicht die Begehung betriebsbezogener Straftaten und Ordnungswidrigkeiten erleichtert hat, und stellt die praktisch wohl bedeutsamste Bezugstat für eine Verbandsgeldbuße nach § 30 OWiG dar. Zwischen der in § 130 OWiG in Bezug genommenen Aufsichtspflicht und den vom Verband zu ergreifenden Compliance-Maßnahmen besteht ein weitreichender Gleichlauf:

Für beide ***geht es um die aus der Legalitätspflicht des Verbands folgende Aufgabe, Mitarbeiter und Gefahrenquellen zu beaufsichtigen und den Verband derart zu organisieren, dass kein Schaden für die Rechtsgemeinschaft entsteht. § 130 OWiG ist daher der zentrale positivrechtliche Anknüpfungspunkt für Compliance.***

Problematisch ist dabei, dass die Voraussetzungen für die „erforderlichen Aufsichtsmaßnahmen" (und damit auch Compliance-Maßnahmen) aus dieser Vorschrift bislang nicht hinreichend ersichtlich sind. Welche Aufsichtsmaßnahmen als erforderlich erachtet werden, bleibt mit Ausnahme der in § 130 Absatz 1 Satz 2 OWiG beispielhaft aufgezählten „Bestellung, sorgfältige[n] Auswahl und Überwachung von Aufsichtspersonen" nach geltender Rechtslage eher unklar.

Um Rechtssicherheit und Transparenz zu erhöhen, ist es daher geboten, diese Regelung zu konkretisieren. ***Auch die von der EU bereits beschlossene Richtlinie des Europäischen Parlaments und des Rates zur Bekämpfung der Korruption****, zur Ersetzung des Rahmenbeschlusses 2003/568/JI des Rates und des Übereinkommens über die Bekämpfung der Bestechung, an der Beamte der Europäischen Gemeinschaften oder der Mitgliedstaaten der Europäischen Union beteiligt sind, sowie zur Änderung der Richtlinie (EU) 2017/1371 des Europäischen Parlaments und des Rates hält die Mitgliedstaaten in Erwägungsgrund 5 dazu an, die Entwicklung und Umsetzung robuster und wirksamer Compliance-Mechanismen in privaten Unternehmen zu fördern.*

(2) Die ***Grundelemente eines geeigneten Compliance-Systems werden*** *– in Anknüpfung und Anlehnung an frühere Vorschläge –* ***kodifiziert,*** *indem § 130 Absatz 1 Satz 2 OWiG durch die im Antrag genannte Regelung ersetzt wird.*

Die Regelung formuliert allgemeine Grundsätze für geeignete Aufsichtsmaßnahmen im Sinne des § 130 OWiG und für ein tragfähiges Compliance-Konzept.

Die hierzu genannten fünf Grundelemente orientieren sich an anerkannten internationalen und nationalen Standards und lassen sich als holzschnittartige Umschreibung der „Best Practices" eines effektiven Compliance-Managements charakterisieren, sind aber nicht als zwingend abschließender Maßnahmen-Katalog zu verstehen („insbesondere").

Auf diese Weise schafft die Regelung für Verbände und andere Rechtsanwender einen Referenzmaßstab für die Anforderungen an eine ordnungsgemäße Aufsicht und Organisation und bildet zugleich einen Anreiz für die Einrichtung und Fortentwicklung von Compliance-Systemen. Sie stärkt die Akzeptanz der Wirtschaft und fördert die Kalkulierbarkeit des Nutzens kostenintensiver Überwachungsmaßnahmen. Die Regelung stellt einen Mittelweg dar zwischen der Regelungsarmut der geltenden Regelung in § 130 Absatz 1 OWiG und zu detaillierten Vorgaben, die zu Lasten der notwendigen Flexibilität bei der Ausgestaltung von Compliance-Maßnahmen gehen und vor allem die KMU übermäßig belasten könnten.

Durch die Regelung in Satz 2 wird zunächst der Rahmen der erforderlichen Aufsichtsmaßnahmen ***im Einklang mit der Rechtsprechung (grundlegend LG München I, Urt. v. 10.12.2013 – 5 HKO 1387/10****, 1. Leitsatz mit Rn. 89, zitiert nach juris) und Literatur (vgl. nur BeckOK OWiG/Beck, 50. Ed. 1.4.2026, OWiG § 130 Rn. 45-58; KK-OWiG/Rogall, 6. Aufl. 2025, OWiG § 130 Rn. 40 ff.) bestimmt.*

Auf die dort entwickelten Grundsätze kann zurückgegriffen werden. Die Anknüpfung an Art, Größe, Organisation und von dem Unternehmen oder Betrieb ausgehender Gefahren bringt zum Ausdruck, dass die geforderten Aufsichtsmaßnahmen nur vor dem Hintergrund der konkreten Struktur, des konkreten Geschäftsfelds und der jeweiligen Risiken beurteilt werden können.

Hierdurch und durch die Anbindung der Maßnahmen an das Kriterium der Zumutbarkeit werden insbesondere die Belange der KMU sowie Start-Ups bewusst in den Blick genommen. Gerade dort können auch einfache Maßnahmen ausreichend sein, ohne dass es eines eigens entwickelten Compliance-Programms oder gar einer Zertifizierung bedarf.

In Satz 3 werden zentrale Grundelemente geeigneter Aufsichtsmaßnahmen – nicht abschließend – aufgelistet. ***Hervorzuheben ist dabei, dass die Implementierung derartiger Maßnahmen für sich allein nicht ausreicht, um kriminalpräventive Effekte zu erzielen. Die Maßnahmen müssen auch in ein entsprechendes Wertemanagement und in eine ethische Unternehmenskultur eingebettet sein*** *(vergleiche etwa Bussmann/Niemeczek/Vockrodt, MSchrKrim 99 [2016], 23, 24 ff.).* ***Eine gelebte Compliance-Kultur („tone from the top" oder das Bekenntnis der Unternehmensleitung zur Rechtstreue und zur aktiven Unterstützung der Compliance-Maßnahmen) stellt ein wichtiges Grundelement guter Compliance dar, das die Unternehmensleitung zur regelmäßigen Kommunikation klarer Botschaften und zur Festlegung von bzw. Aktualisierung von Standards im Unternehmen verpflichtet.***

Zu den Regelungen im Einzelnen:

– In ***Nummer 1*** *wird die* ***sorgfältige Auswahl, Unterweisung und Überwachung von Mitarbeitern und Aufsichtspersonen*** *genannt. Dies erfasst die bereits derzeit im Gesetz beispielhaft genannten Aufsichtsmaßnahmen und erstreckt diese generell auf Mitarbeiter sowie auf die Unterweisung (Instruktion) der genannten Personenkreise. Die Schulung zum Zweck der Verhinderung von unternehmensbezogenen Straftaten und Ordnungswidrigkeiten wird gesondert in Nummer 3 geregelt.*

– ***Nummer 2*** *bringt die Bedeutung einer* ***kriminalpräventiven Risikoanalyse*** *im Unternehmen zum Ausdruck. Sie trägt dem Umstand Rechnung, dass effektive Aufsichts- und Organisationsmaßnahmen zur Verhinderung von Fehlverhalten im Unternehmen nur auf Grundlage einer vorhergehenden Risikoanalyse denkbar sind.*

– Nach ***Nummer 3*** *stellen auch der* ***Erlass und die Fortentwicklung von Richtlinien und Weisungen sowie die Schulung der Mitarbeiter*** *zum Zweck der Verhinderung von unternehmensbezogenen Straftaten und Ordnungswidrigkeiten ein wichtiges Beispiel geeigneter Aufsichtsmaßnahmen dar. In derartigen Maßnahmen tritt auch die Haltung der Unternehmensführung zu einer integritätsförderlichen Unternehmenskultur zum Ausdruck („tone from the top", siehe oben). Regelmäßige Schulungen helfen, die Verhaltensleitlinien dauerhaft und somit nachhaltig der Belegschaft zu verdeutlichen und so deren Akzeptanz im Sinne einer präventiven Beratung zu fördern (Beulke/Moosmayer, CCZ 2014, 146, 152).*

– Mit der Regelung in ***Nummer 4*** *kommt zum Ausdruck, dass in der Einrichtung eines* ***Hinweisgebersystems*** *eine gebotene Aufsichtsmaßnahme liegen kann. Für die unter das Hinweisgeberschutzgesetz (HinSchG) fallenden Unternehmen sind die dortigen Maßgaben rechtlich bindend und bieten eine klare Struktur, die es zu beachten gilt. Die „geeignete Stelle" im Sinne von Nummer 4 ist dann auch die „interne Meldestelle" im Sinne des § 7 Absatz 1 Satz 1 HinSchG. Für nicht vom HinSchG erfasste Unternehmen gibt die Regelung die Möglichkeit, den Vorgaben ohne unverhältnismäßigen Aufwand gerecht zu werden, etwa durch die Benennung eines vertrauenswürdigen internen Ansprechpartners (vergleiche Beulke/Moosmayer, CCZ 2014, 146, 152).*

Dort, wo präventive Maßnahmen nicht umfassend zum Erfolg führen und Verdachtsmomente auf unternehmensbezogene Straftaten oder Ordnungswidrigkeiten zutage treten, ***muss sichergestellt sein, dass einem derartigen Verdacht nachgegangen wird und, bei Bestätigung des Verdachts, angemessene Sanktionsmaßnahmen ergriffen werden. Nummer 5*** *bringt dies zum Ausdruck.*

Zugleich gehört es zur Aufgabe des Unternehmens, im Rahmen einer anlassbezogenen Risikoanalyse (Nummer 2) aus dem Fehlverhalten Rückschlüsse zu ziehen und das Compliance-Programm dort, wo geboten, entsprechend anzupassen. Die in Satz 3 aufgeführten Grundelemente sind teilweise ineinander verwoben und ergänzen sich im Einzelfall. Sie sind idealerweise in ein umfassendes Gesamtkonzept eingebettet. (…)

16. Zu Artikel 3 Nummer 1 Buchstabe b (§ 30 Absatz 2a Satz 3 Nummer 5, Satz 4 – neu –, 5 – neu – OWiG)

Artikel 3 Nummer 1 Buchstabe b § 30 Absatz 2a ist wie folgt zu ändern:

a) Satz 3 Nummer 5 ist zu streichen.

b) Nach Satz 3 sind die folgenden Sätze einzufügen:

„Zu Gunsten der juristischen Person oder Personenvereinigung zu berücksichtigen sind insbesondere ***vor oder nach der Straftat oder Ordnungswidrigkeit von ihr getroffene geeignete Vorkehrungen zur Vermeidung oder Aufdeckung von Straftaten und Ordnungswidrigkeiten****, für die sie nach Absatz 1 verantwortlich wäre. Geeignete Vorkehrungen in diesem Sinne können insbesondere Maßnahmen nach § 130 Absatz 1 Satz 3 Nummer 1 bis 5 sein."*

***Begründung**:*

*Die vorgeschlagenen Änderungen dienen dazu, den **sanktionsmildernden Charakter der Vornahme geeigneter Compliance-Maßnahmen** noch klarer herauszustellen und deren Bedeutung für Unternehmen (Verbände) und Verfolgungspraxis zu unterstreichen.*

Im Einzelnen:

(1) Mit der Regelung in § 30 Absatz 2a Satz 3 Nummer 5 OWiG-E will der Gesetzentwurf die Auswirkungen von Compliance-Maßnahmen für die Bemessung der Verbandsgeldbuße regeln (vgl. BR-Drs. 266/26, S. 101).

Die vorgesehene Verortung von Compliance-Maßnahmen als bloßes Zumessungskriterium, das heißt als „insbesondere in Betracht" zu ziehender Umstand, wird der Bedeutung dieser Maßnahmen für die Vermeidung von unternehmensbezogenem Fehlverhalten allerdings nicht ausreichend gerecht.

Es ist vielmehr geboten, die Relevanz dieser Maßnahmen in einer von dem Beispielskatalog losgelösten, eigenständigen Regelung in der im vorstehenden Antrag vorgeschlagenen Ausgestaltung zu regeln.

*Dies geschieht zu dem Zweck, die Vornahme (geeigneter) Maßnahmen zur **Criminal Compliance** besonders in den Blick von Sanktions- und Unternehmenspraxis zu rücken und zugleich den obligatorischen und sanktionsmildernden Einfluss auf die Sanktionsentscheidung zu betonen.*

Dies trägt auch den Vorgaben der Richtlinie des Europäischen Parlaments und des Rates zur Bekämpfung der Korruption, zur Ersetzung des Rahmenbeschlusses 2003/568/JI des Rates und des Übereinkommens über die Bekämpfung der Bestechung, an der Beamte der Europäischen Gemeinschaften oder der Mitgliedstaaten der Europäischen Union beteiligt sind, sowie zur Änderung der Richtlinie (EU) 2017/1371 des Europäischen Parlaments und des Rates (fortan: Richtlinie [EU] zur Korruptionsbekämpfung von 2026) besser Rechnung. Nach der Regelung in Artikel 16 Satz 1 Buchstabe c („Mildernde Umstände") haben die Mitgliedstaaten sicherzustellen, dass für die Sanktionierung von Verbänden wegen Korruptionsstraftaten vor oder nach der Begehung der Straftat durchgeführte wirksame Programme für interne Kontrollen, Ethiksensibilisierungsprogramme und Compliance-Programme als mildernde Umstände gelten können.

(2) Hiervon ausgehend wird vorgeschlagen, die Regelung in Satz 3 Nummer 5 von § 30 Absatz 2a OWiG-E zu streichen und stattdessen die im Antrag aufgeführten Sätze 4 und 5 anzufügen.

Die Neuregelung bringt den sanktionsmildernden Charakter von Compliance-Maßnahmen, also Vorkehrungen zur Vermeidung und Aufdeckung unternehmensbezogener Straftaten und Ordnungswidrigkeiten, klarer zum Ausdruck. Voraussetzung hierfür ist nach Satz 1, dass die Vorkehrungen sich als „geeignet" darstellen müssen.

***Es muss vermieden werden, dass Maßnahmen, die nur zum Schein ergriffen werden und das Vorhandensein wirksamer Bemühungen nur vorgaukeln sollen (sogenanntes window dressing), sanktionsmildernd auswirken können** (vergleiche hierzu auch Erwägungsgrund 29 der Richtlinie [EU] zur Korruptionsbekämpfung von 2026); **für diesen Fall kommt** auf der Grundlage der Zumessungskriterien in Satz 3 Nummer 1 und 2 von § 30 Absatz 2a OWiG-E (Art der Ausführung, Beweggründe und Ziele des Täters) sogar eine **bußgelderhöhende Berücksichtigung in Betracht** (vergleiche auch BR-Drs. 266/26, S. 101).*

*An einer entsprechenden Eignung wird es auch fehlen, wenn eine von der **Leitungsebene** getragene Compliance-Organisation nicht besteht (vergleiche auch BR-Drs. 266/26, S. 101).*

Für die Frage, was geeignete Vorkehrungen sein können, wird in Satz 5 beispielhaft auf die mit gesondertem Antrag gesetzlich neu vorgeschlagenen Grundelemente geeigneter Compliance-Systeme in § 130 OWiG-E verwiesen.

Nicht geboten erscheint es im Übrigen, nur solche Vorkehrungen zu honorieren, die darauf gerichtet sind beziehungsweise waren, Zuwiderhandlungen gerade der eingetretenen Art zu verhüten.

Bei entsprechenden, vor der Tat ergriffenen Vorkehrungen wird es im Übrigen häufig bereits an einer sanktionsbegründenden Aufsichtspflichtverletzung nach § 130 Absatz 1 Satz 1 OWiG fehlen.

***Dass die getroffenen Compliance-Maßnahmen bereits aufgrund gesetzlicher Verpflichtung vorgenommen werden müssen oder dass mit den getroffenen Compliance-Maßnahmen eine Verantwortlichkeit nach §§ 30, 130 OWiG vermieden werden soll, steht einer bußgeldmindernden Berücksichtigung ebenfalls nicht entgegen** (vergleiche auch BR-Drs. 266/26, S. 101).*

(3) Die konkrete Festlegung der begünstigenden Auswirkungen auf die Bemessung der Verbandsgeldbuße muss der Praxis überlassen bleiben. Eine nähere gesetzliche Umschreibung ist aufgrund der Vielgestaltigkeit der vorkommenden Fälle und des sehr unterschiedlichen Gewichts der von Verbänden veranlassten (geeigneten) Präventionsbemühungen nicht möglich (dahingehend auch Erwägungsgrund 29 der Richtlinie [EU] zur Korruptionsbekämpfung von 2026). Allgemein gilt, dass eine bußgeldmindernde Berücksichtigung umso stärker

sein wird, je ernsthafter, umfassender und wirksamer die Bemühungen des Verbands sind, sich rechtskonform zu verhalten.

Für die Nachtat-Compliance wird die Bußgeldminderung insbesondere davon abhängen, wie effektiv und spezifisch mit diesen Compliance-Maßnahmen auf die vorangegangene Tat reagiert wird, um deren Wiederholung zu vermeiden oder gleichartige Taten aufzudecken und zu beenden*. Auch wird von Bedeutung sein, ob die nach der Tat getroffenen Compliance-Maßnahmen bereits vor dem Herantreten der Verfolgungsbehörden an den Verband getroffen bzw. angepasst wurden oder ob dies erst unter dem Eindruck der bereits offen gegen den Verband geführten Ermittlungen erfolgte. (…)"*

2. Steigende Zahlen von Managerhaftungsfällen, Kardinalpflichten und Gefährdung des Versicherungsschutzes nach aktueller Rechtsprechung[14]

Die Zahl der Managerhaftungsfälle steigt nach Auskunft des *Gesamtverbandes der Deutschen Versicherungswirtschaft* enorm.[15]

Neben des nachgewiesen drastisch steigenden Risikos der persönlichen Haftung droht aufgrund des von aktueller Rechtsprechung[16] angenommenen Vorwurfs der „*Verletzung von Kardinalpflichten*" und der daraus abgeleiteten Indikation[17] einer „*wissentlicher Pflichtverletzung*" der Verlust des Versicherungsschutzes für Manager und Führungskräfte.

Nach der neuesten Entscheidung des *BGH*[18] 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*[19] führte unlängst aus, *jede Verletzung des Legalitätsprinzips* stelle eine *Kardinalpflichtverletzung* dar.[20]

Damit wurde die Compliance und das nach ständiger Rechtsprechung[21] 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

---

[14] Vgl. *Scherer,* Legalitätspflicht als Kardinalpflicht, 6 / 2026 *zum* kostenlosen Download im Internet.

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

[16] 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.

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

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

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

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

[21] 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.

Allgemeinen D&O-AGB *ULLA*[22] vorliege. Es müsse schon ein *wissentlicher* Pflichtverstoß *bzgl. einer konkret bezeichneten* Pflicht im Sinne eines direkten Vorsatzes oder gar Absicht[23] vorliegen. Fahrlässigkeit oder ein bloßes „für-möglich-halten-und-sich-damit-abfinden“[24] reiche nicht.

Zu den Kardinalpflichten führte der *BGH* nichts aus. Somit bleibt es bei der Rechtsprechung, dass eine Kardinalpflichtverletzung eine wissentliche Pflichtverletzung indiziert.[25]

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.

3. Verantwortliche Führungskräfte im Fokus von Ermittlungen: Fallbeispiele[26]

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.[27]

Beim „*Love-Parade*“-Fall wurde gemeldet, dass auch gegen die *Vorgesetzten der verantwortlichen Mitarbeiter* der Stadt wegen unterlassener Überwachung ermittelt werde.[28]

Auch der „*Transrapid*“-Fall[29] 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.

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.[30] 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.

---

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

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

[24] Dolus eventualis.

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

[26] Vgl. *Scherer,* Legalitätspflicht als Kardinalpflicht, 6 / 2026 *zum* kostenlosen Download im Internet.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

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.

4. Vereinfachte Grundzüge straf-, bußgeld- und zivilrechtlicher Haftung von Organisationen und Führungskräften[31]

Manager (Organe und Führungskräfte) sowie alle sonstigen Beschäftigten können *strafrechtlich* persönlich bereits bei Fahrlässigkeit (z.B. fahrlässige Körperverletzung oder Tötung[32]) 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[33], die die bisherige Linie der Rechtsprechung[34] 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[35] 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.

Zivilrechtlich können Führungskräfte persönlich Dritten gegenüber direkt haften (Außenhaftung) oder der Organisation, in der sie tätig sind, gegenüber, wenn sie diese schädigen (Innenhaftung).[36]

5. Persönliche Haftung des Delegierenden und des Delegationsempfängers bei fehlerhafter Übertragung oder Wahrnehmung von Unternehmerpflichten (Pflichtendelegation)[37]

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.

---

[31] Vgl. *Scherer,* Legalitätspflicht als Kardinalpflicht, 6 / 2026 *zum* kostenlosen Download im Internet.

[32] 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.

[33] *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.

[34] Z.B. in Kartellsachen.

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

[36] Vgl. *Scherer,* Legalitätspflicht als Kardinalpflicht, 6 / 2026 *zum* kostenlosen Download im Internet. 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.

[37] 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.

Auch auf Externe (Berater[38], 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).

6. Höchste Brisanz für Unternehmen und Manager aufgrund weiterer aktueller Rechtsprechung: Der Albtraum einer Führungskraft[39]

Im Rahmen der Grundsätze der *zivilrechtlichen Arbeitnehmerhaftung* schlug das in der Organisations-Praxis zu wenig beachtete Urteil des *LAG Köln*[40] 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 und Geschäftsführer / Vorstand wegen Organisationsverschulden haften können, wenn fehlerhaftes Handeln oder Unterlassen[41] die Rechte Dritter verletzt.

7. Albtraum von Führungskräften auch im Kontext von KI-Einsatz[42]

Aufgrund der völlig neuen *Rechtsprechung zur Haftung bei Benutzung von KI, die durch unrichtigen Output andere schädigt*,[43] 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[44], wie Handbücher, Richtlinien, Kontrollmaßnahmen vorhalten, da andernfalls Unternehmen und Geschäftsführer / Vorstand wegen Organisationsverschulden haften können, *wenn fehlerhafter KI-Output die Rechte Dritter verletzt*.

---

[38] 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.

[39] Vgl. *Scherer,* Legalitätspflicht als Kardinalpflicht, 6 / 2026 *zum* kostenlosen Download im Internet.

[40] *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.

[41] Bei bestehender Handlungspflicht.

[42] Vgl. *Scherer,* Legalitätspflicht als Kardinalpflicht, 6 / 2026 *zum* kostenlosen Download im Internet.

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

[44] 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.

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

8. Neue Anforderungen von Gesetzgeber und Wirtschaftsprüfern an Compliance-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 S 16: 2025 zur Prüfung des Krisenfrüherkennungssystems nach § 1 StaRUG ausführlich und schon recht gut dargestellt.[45]

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

Ein angemessener ***Risikomanagement-Prozess***[46] mit Analysen[47], 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***[48] ableiten.

Die ***Governance- und Kardinalpflicht-Compliance*** sorgt mit einem die Kardinalpflichten der Organe und Führungskräfte umfassenden ***Rechtskataster***[49], 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***“[50] 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.).

---

[45] 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.

[46] 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.

[47] 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.

[48] 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.

[49] 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.

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

Die Implementierung oder Auditierung ***rechtssicherer Organisationsstrukturen***[51] mit Stellenbeschreibungen, lückenloser ***Pflichtendelegation***[52], etc. und vor allem angemessenem ***Prozessmanagement***[53] sorgt nicht nur für Sicherheit, sondern auch für Struktur.

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

- ***Financial Governance***[54] sorgt dafür, dass rechtliche und wirtschaftliche Pflichten, wie Wirtschafts- und Liquiditätsplanung, etc. dokumentiert erfüllt werden.
- ***IT- und KI-Governance***[55] ist umfassend regulierte Führungsaufgabe.
- ***Business Continuity- und Krisen-Governance***[56] ist ebenfalls bei vielen Organisationen aufgrund des geänderten Umfelds ein bisher noch vernachlässigter Bereich.

Ein ***Integriertes (IT- / KI-) Governance-Compliance-Managementsystem***[57] beinhaltet und vernetzt die angesprochenen Komponenten in effektiver und zugleich effizienter Weise. Ein ***(externes) Internes Audit***[58] 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***[59] an.

10. Wertbeiträge[60]

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*[61] - 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.

---

[51] 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.

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

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

[54] 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.

[55] 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.

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

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

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

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

[60] Vgl. *Scherer,* Legalitätspflicht als Kardinalpflicht, 6 / 2026 *zum* kostenlosen Download im Internet.

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

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

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, Managerenthaftung, Governance-, Risiko- und Compliance-Management, 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

Linkedin: Prof. Dr. Josef Scherer

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