Prof. Dr. Josef Scherer

Rechtsanwalt,
Vorstand des Internationalen Instituts für Governance, Management,
Risk- und Compliancemanagement und Leiter der Stabsstelle ESGRC
der Technischen Hochschule Deggendorf. Mitglied diverser ISO/
DIN-Normenausschüsse (Governance, Compliance, Personalmanagement).

**Scherer** **09.08.23**

# KI[1]-Verantwortung und enthaftende Wirkung eines *KI-Compliance-Managementsystems*[2] für Leitung (Vorstand, Geschäftsführer, Officers), Aufsichtsgremium und sonstige Führungskräfte

#künstlicheintelligenz #managementsysteme #compliance #ChatGPT #Bard #Intellectual Property #Governance #Haftungsverantwortung #Vorstand #Geschäftsführer #Aufsichtsrat #Stand der Technik #Standards #Richtlinien #policies #technischen Gefahren #KI-CMS #enthaftend #KI-Compliance-Management #Angemessenheit #Wirksamkeit #Achtsamkeit #Bildung #Kommunikation #KI-Compliance-Anforderungen #Compliance-Risiko-Analyse #Technikklauseln #Teschnisch-organisatorische Voraussetzungen #KI-Systemtransparenz #Technische Risiko-Folgeabschätzung #Ethics by Design #Assessments #KI-System-Testing #Audits #Zertifikate #KI-Prüfsiegel #unbestimmte Rechtsbegriffe #EU-Produkthaftungsrichtlinie mit Bezug zu KI #KI als Produkt #naheliegende Fehlanwendungen #Beweiserleichterungen für Geschädigte #Disclosure of Documents #risikobasierter Ansatz #Rechtsgebiete-Matrix/Rechtskataster #RACI-Methode #Freiheitsstrafen, Geldstrafen und Schadensersatzforderungen #Reputationsverlust #KI-Compliance-Risiken #Quantifizierung, Aggregation, Betrachtung der Risikotragfähigkeit #Risiko-Steuerung #„Lines-of-Defense"-Modell #Monitoring-Prozesse #Code of Conduct #Einbindung der Beschäftigtenvertretung #KI-Richtlinienmanagement #ausgelagerte Prozesse #ausgegliederte/outgesourcte Leistungen #Delegationsempfänger #Business Continuity-Managementsystem #Früherkennung #Organisations-, Rollen-, Aufgaben- und Berechtigungs-Konzept #Risk-Assessment #Top-Risks #Worst-Case-Szenarien #Prophylaxemaßnahmen #Reaktionssystem #Business Partner Screening #Einkaufs-Compliance #Know your supplier #Lieferantenaudit #Einforderung diverser Zertifikate #Lieferketten-Sorgfaltspflichten-Gesetz #Auslagerungen #Governance #ISO 37000 #gute unternehmerische Entscheidungen

## Breaking news

Eine der ersten Sanktionen inkl. Reputationsschaden? Zumindest extrem peinlich:
„Von ChatGBT erfundene Fälle: Anwälte müssen Geldstrafe zahlen"[3]

[1] Akronym für „Künstliche Intelligenz", englisch: Artificial Intelligence (AI)
[2] *„KI-CMS"*
[3] *Oswald*, Von ChatGBT erfundene Fälle: Anwälte müssen Geldstrafe zahlen, 23.6.23, BR24, Netzwelt

KI-Themen sind täglich in den Medien:

„Gestaltung von KI-Leitlinien für Unternehmen[4]“,
„KI-Gesetz: Erste Regulierung der künstlichen Intelligenz[5]“,
„KI-Verordnung: Einigung bis Jahresende erwartet[6]“,
„ChatGBT-Macher auf Milliarden verklagt[7]“,
„Milliardenklage gegen Google[8]“,
„KI-Firmen geben Versprechen an US-Präsidenten ab[9]“,
„Keine einheitliche Richtlinie für ChatGBT in der Bundesregierung[10]“,
etc., etc.:

Etwas chaotisch noch.
Dabei geht es bei KI auch nur um eine neue Technologie, wie schon bei Webstühlen, Dampfmaschinen, Computer, Internet und Co.

Egal, welche Technologie zu erfinden, bewerten, regulieren und zu steuern ist:
Die Basis dafür ist „Technik-Governance[11],“ auf Basis von Compliance-, Risiko- und neuerdings auch Nachhaltigkeits-Management.

**Summary:**

Künstliche Intelligenz wird - insbesondere seit dem jüngsten Hype um *ChatGPT* (und künftig noch mehr befeuert durch *Bard* von *Google* und weitere, vielfältige Anwendungen) - in vielen Organisationen / Unternehmen ohne Kenntnis der negativen (technischen, rechtlichen und wirtschaftlichen) Auswirkungen und häufig unstrukturiert eingesetzt:

Hochriskante Verstöße gegen Intellectual Property (IP)-, IT- und Informationssicherheits-, Datenschutz-, Geschäftsgeheimnis-, Governance-Regularien u.v.m. sind an der Tagesordnung: Die Haftungsverantwortung hierfür tragen hier primär und letztlich Leitungs- (Vorstand, Geschäftsführer) und Aufsichtsgremium (Aufsichtsrat / Beirat).[12]

Gesetze, Rechtsprechung, verbindliche Regelungen der Exekutive, Stand der Technik, Standards, interne verbindliche Vorgaben (Richtlinien / policies, Betriebsvereinbarungen, etc.), u.v.m. bilden den z.T. *haftungsbewehrten Compliance-Rahmen*, den häufig noch niemand so richtig erkannt hat – ebenso wie die technischen Gefahren von KI, die den

[4] *Bomhard,* Gestaltung von KI-Leitlinien für Unternehmen, 8.6.23, aitava.com
[5] *Europäisches Parlament,* KI-Gesetz: Erste Regulierung der künstlichen Intelligenz, 14.6.23, Europaparlament.eu
[6] *beck aktuell*, KI-Verordnung: Einigung bis Jahresende erwartet, 22.6.23
[7] *Mahler,* ChatGBT-Macher auf Milliarden verklagt, 30.6.23, Computerwoche.de
[8] *Lorz,* Milliardenklage gegen Google, 12.7.23
[9] *Ntv*, KI-Firmen geben Versprechen an US-Präsidenten ab, 22.7.23, ntv.de
[10] *Redaktion beck aktuell*, Keine einheitliche Richtlinie für ChatGBT in der Bundesregierung, 24.7.23, Beck aktuell.de
[11] Vgl. *Scherer, Fruth*, Technik-Governance, Sonderdruck des Bundesverbandes der Compliance-Manager, 1/2015
[12] Vgl. §§ 130, 30, 9 OWiG, 43 GmbHG, 93, 116 AktG und viele weitere spezielle Regelungen des „hard law.“

Chancen risikobasiert und nach den Vorgaben der Business Judgement Rule gegenübergestellt werden müssen (§ 93 Abs 1 Satz 2 AktG).

Hier besteht noch akuter großer Aufklärungsbedarf.

Ein KI-CMS wirkt enthaftend und ermöglicht uU. eine produktive Geschäftstätigkeit unter Nutzung der Chancen der neuen Technologien. Dabei hilft folgende These, mit relativ einfachen Maßnahmen den rechtlichen (und technischen) Anforderungen gerecht zu werden, sowie Chancen zu nutzen und Gefahren zu vermeiden:

KI-Compliance-Management ist *integraler Bestandteil des allgemeinen Compliance-Managementsystems* und Teil der *Governance*[13], also des verbindenden „G" bei *ESG*[14] und *GRC*[15].

## 1. First steps für „Angemessenheit" und „Wirksamkeit" eines KI-Compliance-Managementsystem

### 1.1 Achtsamkeit, Bildung und Kommunikation

Zunächst sind ein allgemeines Verständnis bzgl. der technischen, rechtlichen, wirtschaftlichen und verhaltensökonomischen Implikationen der KI, sowie entsprechende Kultur (Tone from the Top), Kompetenzen und Bewusstsein durch Schulungen und sonstige Kommunikations- und Achtsamkeits-Kampagnen zu schaffen.

### 1.2 KI-Compliance-Anforderungen und KI-Compliance-Risiko-Analyse

Geschäftsleitung und sonstige Verantwortliche *müssen* parallel dazu primär die jeweiligen von ihnen betreuten (Prozess-) Themenfelder / Bereiche *an aktuellen Anforderungen aus Gesetzgebung und Rechtsprechung sowie dem „Anerkannten Stand von Wissenschaft und Praxis"* bzw. *„Stand der Technik*" („hard law") ausrichten.

Auf der regulatorischen Seite ist Kenntnis der zwingenden Anforderungen aus diversen Quellen und Erfüllung durch angemessene Maßnahmen Pflicht.[16]

Zahlreiche Einzelgesetze, (z.B. IT-Sicherheitsgesetz, Digitalisierungs-Gesetze, KI-Verordnung...), einschlägige öffentlich- und privat-rechtliche Regulierung, Straf- und Ordnungswidrigkeitenrecht, Rechtsprechung, u.v.m. beschäftigen sich mit sich z.T. überschneidenden zwingend zu beachtenden Themen aus Nachhaltigkeit (ESG) und Governance (GRC), im Zusammenhang mit Informations-Technologien[17].

[13] Vgl. *Scherer, Ketelsen*, Technical Product-Compliance-Managementsystem, Bavarian Journal of Applied Sciences, (BJAS), 2022, S. 16-18 und ISO 37000:2021 (Governance of Organizations), 6.8 Daten und Entscheidungen

[14] Akronym für Environmental, Social, Governance (Nachhaltigkeit)

[15] Akronym für Governance, Risk & Compliance (Compliance- und risikobasierte Unternehmensführung)

[16] Vgl. *Scherer*, Compliance-Managementsystem nach DIN ISO 37301:2021 erfolgreich implementieren, integrieren, auditieren, zertifizieren, Beuth-Verlag, 2022, Kapitel 4.5.

[17] Vgl. *Scherer, Grötsch, Romeike*, Forschungsbedarf bei Nachhaltigkeit (CSR / ESG), Governance und Digitalisierung / KI, Bavarian Journal of Applied Sciences, (BJAS), 2022, S.16-18.

**Beispiel 1:**
Noch in 2023 soll die **EU-KI-Verordnung**[18] in Kraft treten[19].

Eine KI-Anwendung ist – wie auch andere IT-Anwendungen stets – *rechtlich* zu beurteilen, ob sie zulässig? sicher? dem „Stand der Technik" entsprechend? ist:

Als Informationsgrundlage dienen zu beachtende fixe Sollgrößen / Referenzgrößen / Pflichtenmaßstäbe, z.B. Gesetze, Rechtsprechung „Technikklauseln" (nach BVerfG), etc.

Auch die demnächst beschlossene Verordnung zur Regulierung von KI („*KI-Verordnung*")[20] mit Inhalten, wie z.B. Verbot des Einsatzes von KI in bestimmten Anwendungsszenarien, Technisch-organisatorische Voraussetzungen für den Einsatz von KI, etc., zählt dazu, regelt die Thematik aber bei weitem nicht abschließend.

**Kernstück der KI-Verordnung ist eine „(Compliance-) Risiko-Analyse[21]" mit folgenden Inhalten:**

1. **KI-Systemtransparenz**
   Kategorisierung der eingesetzten / geplanten KI-Systeme und KI-Compliance-Relevanz

2. **Technische Risiko-Folgenabschätzung**
   bzgl. des konkret geplanten Systems mit „angemessenen" und „wirksamen" Risikobewertungs-Methoden nach „Stand der Technik"

3. **„Ethics by Design" (systemimmanente Ethik) als zwingende Verpflichtung**

4. **Assessments / Freigaben / Kontrollpunkte in den beteiligten Prozessen**

5. **KI – System – Testing**
   auf Angemessenheit und Wirksamkeit, Risikobewertung unter Simulationen, Penetration-Test-Verfahren (nach Stand der Technik)

6. **Nachweis durch Audits / Zertifikate**
   (*z.B. „AIC 4 Zertifikat" / Fraunhofer „KI-Prüfsiegel", TÜV? etc*.) ist *nicht* in der Verordnung enthalten, aber u.a. vom TÜV-Verband gefordert.

Aufgrund der „Legalitätspflicht" der Geschäftsleitung und der Anforderungen an einen „gewissenhaften" Geschäftsführer, Vorstand, Aufsichtsrat, Kaufmann (§§ 43 GmbHG, 91, 93, 107, 116 AktG, 347 HGB), sowie der Pflicht nach §§ 130, 30, 9 OWiG, Vorsorge gegen

[18] Englisch: AI-Act
[19] Vgl. *Aktuelles Europäisches Parlament*, KI-Gesetz: Ein Schritt näher an ersten Regeln für künstliche Intelligenz Pressemitteilung vom 11.05.2023, abrufbar im Internet.
[20] Vgl. *Mackert / Makowicz*, Nachhaltige menschenzentrierte Implementierung neuer Technologien - KI Compliance, *Comply 3, 2021.*
[21] Vgl. TÜV-Verband fordert Risikoanalyse von KI-Anwendungen, Redaktion Risknet, 03.09.2021, Risknet.de und *Scherer*, Nachhaltigkeits- (ESG-/CSR-) Compliance- und -Risikomanagement – die wesentlichen Pfeiler, auch für Resilenz, 2021, zum kostenlosen Download auf scherer-grc.net.

Pflichtverstöße im Unternehmen zu treffen, muss eine entsprechende, angemessene (KI-) Compliance-Organisation, die rechtssichere, nachhaltige Unternehmensführung und -übewachung ermöglicht, vorgehalten werden.
Diesbezüglich kann es auch nützlich sein, sich an gängigen aktuellen Standards („soft law“) zu orientieren, um den Versuch der Einhaltung des „Anerkannten Standes von Wissenschaft und Praxis“ zu dokumentieren; auch, um auf Audits, Abschlussprüfung oder Zertifizierung gut vorbereitet zu sein. Standards können zudem laut dem Vorsitzenden Richter des 1. Strafsenats des *BGH „strafbarkeitskonstituierend*“ sein.[22]
Im Bereich der von der KI-Verordnung abstrakt und allgemein, oft auch über sogenannte *„unbestimmte Rechtsbegriffe“* gesetzten Anforderungen, fehlen noch entsprechende „Leitfäden“ / Standards, die der Praxis helfen, einheitliche Maßnahmen zur Erfüllung der Anforderungen umzusetzen.

**Beispiel 2:**

**Entwurf der neuen EU-Produkthaftungsrichtlinie mit Bezug zu KI[23]**

Das Produkthaftungs-Gesetz statuiert eine Gefährdungshaftung, also eine verschuldensunabhängige Haftung des Herstellers.

Die EU-Kommission hat im September 2022 einen Entwurf für eine neue EU-Produkthaftungs-Richtlinie beschlossen.
Auslöser war, dass in immer mehr Produkten Software und künftig auch KI-Komponenten enthalten sein werden.
Während im Rahmen der deliktischen Produzentenhaftung nach § 823 BGB die vorherrschende Meinung annimmt, dass IT und Software (inkl. KI) auch von dieser Norm umfasst sei, war dies im Bereich des Produkthaftungsgesetzes noch umstritten.

Insofern erfolgt nun eine Klarstellung, dass IT und KI als Produkt im Sinne des ProdHaftG gelten soll.
Die Länder der EU müssen nach Inkrafttreten der Richtlinie diese europäischen Vorgaben auch in ihre Produkthaftungsgesetze umsetzen.

Durch die Änderungen werden erhebliche neue Risiken im Zusammenhang mit Digitalisierung und KI auf die Hersteller von Produkten, zu denen u.a. auch Importeure, Labeler, Quasi-Hersteller und künftig ebenfalls Bevollmächtigte des Herstellers im Sinne des Produktsicherheitsrechts und Fulfillment-Dienstleister[24] gehören, zukommen.

Diese Entwicklung beeinflusst damit die KI-Compliance und natürlich auch die Product Compliance einer Organisation.[25]

Die Produkthaftung in den zur EU gehörigen Ländern wird sich damit auch auf digitale Produktions-Dateien und Software erstrecken, wobei unter Software auch Systeme künstlicher Intelligenz fallen.

---

[22] Vgl. *Raum*, in: Hastenrath, Compliance-Kommunikation, 2017.
[23] Vgl. *Depping, Pöhls*, Zum Umgang mit dem Risiko der Produkthaftung und dessen Verschärfung, 12.4.2023.
[24] Vgl. Artikel 4 Abs. 14 des Richtlinienentwurfs
[25] Vgl. *VDMA*, Leitfaden Product Compliance, 2023

Die Fehlerhaftigkeit im Sinne des Produkthaftungsgesetzes bezieht sich in erster Linie auf die Sicherheit, die durchschnittliche Kunden unter Berücksichtigung aller Umstände, auch naheliegender Fehlanwendungen berechtigterweise erwarten dürfen.

Damit sind künftig die Gefahren für Cyber-, IT, Datenschutz-, Informations- Sicherheit und vieles mehr enthalten.
Der angemessene Sicherheitsstandard lässt sich nur aus einer angemessenen Risikobewertung ableiten.
Selbst bei Billigprodukten ist eine Basis-Sicherheit unter Berücksichtigung der schwächsten Nutzergruppe zu gewährleisten.

Während früher ab In-Verkehr-bringen des Produktes bei zu diesem Zeitpunkt bestehender Sicherheit nach dem ProdHaftG eine rechtliche Zäsur eintrat, sieht die Richtlinie eine fortbestehende Haftung vor, wenn der Hersteller sein Produkt nach diesem Zeitpunkt beispielsweise durch Software-Updates kontrollieren kann.

Auch Beweiserleichterungen für Geschädigte sind in der Richtlinie enthalten:

Der Entwurf der Richtlinie sieht vor, dass in Produkthaftungsfällen ähnlich einer „Disclosure of Documents“ künftig auch in den europäischen Ländern vom Hersteller die in seinem Besitz befindlichen Beweismittel wie Konstruktionsdokumentation oder Erkenntnisse aus Reklamationen oder Feld-Versuchen etc. herauszugeben sind und bei unvollständiger Herausgabe schon aus diesem Grund der Hersteller den Prozess verlieren könne.

Nach dem ProdHaftG bestand bisher keine Haftung, wenn das Produkt nur deshalb fehlerhaft war, weil sich die Regeln zum Stand der Technik in nicht absehbarer Weise geändert haben, nachdem das Produkt auf den Markt gebracht wurde.

Dass bei dieser sehr jungen Technologie der KI nicht absehbar wäre, dass der „Stand der Technik“[26] sich nach Inverkehrbringen noch ändern würde, ist kaum vorstellbar.
Insbesondere reicht hier schon aus, wenn der Fehler aufgrund eines besseren Standes der Technik nach Inverkehrbringen durch ein Sicherheitssoftware-Update abgestellt werden kann.
Insofern kommt auch der Bereitstellung von Sicherheitsupdates für Produkte über eine lange Zeit, mindestens bis zum Ende der längsten Verjährungsfrist, eine neue Bedeutung zu.[27]

### 1.3 Ergänzende Maßnahmen

Intern bedarf es daher aufgrund der Abstraktheit der diversen (künftigen) gesetzgeberischen Vorgaben, vieler „unbestimmter Rechtsbegriffe“ und aktuell noch fehlender Standards gesonderter Richtlinien (Policies / Betriebsvereinbarungen / etc.)[28] und Aktivitäten in den relevanten Prozessabläufen zur Erfüllung dieser Anforderungen.

---

[26] Vgl. *Bundesverfassungsgericht*, Kalkar-Entscheidung, 1978 und *Scherer, Fruth*, „Technik-Governance“, BCM-Sonderdruck.
[27] Vgl. *Scherer, Ketelsen*, Technical-Product-Compliance-Managementsystem, Bavarian Journal of Applied Sciences, (BJAS), 2022, S. 16-18 und ISO 37000:2021 (Governance of Organizations), 6.8 Daten und Entscheidungen
[28] Vgl. z.B. zur Nutzung von ChatGPT in Lehre und Forschung – eine Einschätzung der AIDAHO-Projektgruppe, Uni Hohenheim

## 2. Integration des KI-CMS in das allgemeine CMS

Durch Integration des KI-CMS in das allgemeine Compliance- oder ESGRC-Managementsystem werden idR. die beschriebenen Anforderungen umgesetzt und zugleich eine enthaftende Wirkung erzeugt.
Bzgl. eines allgemeinen Compliance-Managementsystems hat die ISO weltweit und die DIN für Deutschland die DIN ISO 37301:2021 (Compliance-Managementsystem) veröffentlicht. Insbesondere deren Normkapitel 4.5 (Compliance-Anforderungen) und 4.6 (Compliance-Risikoanalyse) eignen sich gut, auch KI-Compliance-Anforderungen und -Risiken zu identifizieren, zu bewerten und risikobasiert zu steuern.

### 2.1 Das Management aktueller, neuer und geänderter zwingender KI-Compliance-Anforderungen[29]

Um KI-Compliance-Verstöße vermeiden zu können, müssen zunächst relevante KI-Compliance-Verpflichtungen aus unterschiedlichsten Quellen (Gesetze, Rechtsprechung, Richtlinien, etc.) mit angemessenen Analysen identifiziert, bewertet und in angemessene Maßnahmen „übersetzt“ werden.

Neue oder geänderte Verpflichtungen aus KI-Compliance-Anforderungen müssen ebenso behandelt werden.

#### 2.1.1 Normtext DIN / ISO 37301 : 2021

4.5 Compliance-Verpflichtungen

Die Organisation muss systematisch ihre aus ihren Aktivitäten, Produkten und Dienstleistungen resultierenden Compliance-Verpflichtungen identifizieren und deren Auswirkung auf ihren Betrieb beurteilen.

Die Organisation muss über Prozesse verfügen, um:
a) neue und veränderte Compliance-Verpflichtungen zu identifizieren, um kontinuierlich Compliance sicherzustellen;

b) die Auswirkungen der identifizierten Änderungen zu bewerten und alle notwendigen Änderungen des Managements der Compliance-Verpflichtungen einzuführen.

Die Organisation muss dokumentierte Informationen ihrer Compliance-Verpflichtungen aufrechterhalten.

[29] *Scherer*, Compliance-Managementsystem nach DIN ISO 37301:2021, Kapitel 4.5, Beuth, 2022.

### 2.1.2 Identifikation der Verpflichtungen und deren Risiken

Die Identifikation muss sicherstellen, dass sämtliche einzuhaltende KI-Anforderungen, auch internationale, soweit relevant[30], bekannt sind.

Diese Vorgaben lassen sich in einem agilen und sich ständig weiterentwickelnden prozessbezogenen Rechtskataster abbilden.[31]

Dabei ist sicherzustellen, dass alle derzeit geltenden und zukünftigen (neue und sich ändernde) Anforderungen erkannt und nachweisbar eingehalten werden, wenngleich dies eine komplexe Aufgabe darstellt.[32]

Und auch hier gilt: *Nichtwissen schützt vor Strafe nicht.*

**Grundlegende Methodik zur Identifikation verpflichtender KI-Anforderungen[33]:**

Zunächst müssen wohl viele der bereits identifizierten und ebenso auf Basis eines entsprechenden Prozesses fortlaufend neu identifizierten KI-Anforderungen in eine (nicht nur für die Juristen und Techniker) verständliche Sprache „übersetzt" werden.

Dabei kommt es zu einer allgemeinen auftretenden Schwierigkeit *„Unbestimmte Rechtsbegriffe"[34].* Deren Auslegung erfolgt durch Rechtsprechung. Hilfreich dafür sind stets anerkannte Standards / Normierungen.

**Implementierung von Aktivitäten zur Erfüllung der Anforderungen in die Prozesse:**

Wenn nun feststeht oder entschieden wurde, welche *konkrete* Anforderung (priorisiert) zu erfüllen ist, müssen noch Prozessschritte, Aktivitäts- und Kompetenzvermittlungs-Maßnahmen abgeleitet, in die Prozesse implementiert und zur Wirksamkeit gebracht werden, um sicherzustellen, dass die Anforderung messbar, revisionssicher und dokumentiert erfüllt wird/wurde.

Dies gelingt mit führenden Workflows, Automation, digitalen Prozess-Zwillingen[35] und Unternehmenskultur, Awareness, Kompetenz (Wissen, Verstehen, Können und Wollen) sowie einem wirksamen „Lines of defense"-Steuerungs- und Überwachungssystem.

---

[30] Vgl. *Scherer/Butt/Reimertshofer*, Risiken der internationalen Produkthaftung aus der Sicht eines deutschen Unternehmers in: Der Betrieb, Heft 9 vom 5.3.1998, S. 469–474.

[31] Vgl. *Scherer/Fruth* (Hrsg.), Integriertes Compliance-Managementsystem mit GRC (4.0), 2. Auflage, 2017, S. 71.

[32] Vgl. *Raum*, Artikel „Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten", in: Hastenrath (Hrsg.), Compliance-Kommunikation, 2017, S. 33.

[33] Vgl. *Scherer/Ketelsen*, Technical-Product Compliance Managementsystem, Bavarian Journal of Applied Sciences, 2022.

[34] Vgl. BVerfG, Beschluss vom 08.08.1978 – 2 BvL 8/77 und Detterbeck, Allgemeines Verwaltungsrecht mit Verwaltungsprozessrecht, 18. Auflage, 2020, S. 105 f. sowie *Scherer/Ketelsen*, Technical-Product Compliance Managementsystem, Bavarian Journal of Applied Sciences, 2022.

[35] Vgl. *Scherer/Rieger*, Der Digitale Prozess-Zwilling im Gesundheitswesen – auch als Beitrag zu Nachhaltigkeit

Dabei kann es im Falle eines Rechtstreits auch zu einer Beweislastumkehr bzw. sekundären Darlegungslast des Unternehmens kommen, nach der nachgewiesen werden muss, *unter welchen Bedingungen* und *von wem* Entscheidungen getroffen wurden.[36]

**Digital Decision Management:**

Um sicherzustellen, dass die benötigten Informationen vorliegen, eignet sich ein *Digital Decision Management-Tool*, das den Entscheidungsprozess mit (semi-)künstlicher Intelligenz unterstützt und zur gleichen Zeit getroffene Interpretationen und Definitionen von „unbestimmten Rechtsbegriffen" revisionssicher dokumentiert.[37]

**Risikobasierter Ansatz**

Als effektive und effiziente Vorgehensweise bewährt sich möglicherweise zunächst, funktional/ aufbauorganisationsbezogen die Unternehmensbereiche oder (moderner) ablauforganisationsbezogen die Prozesse des Unternehmens zu definieren.

Sodann sind diesen Bereichen bzw. Prozessen die dort relevanten Anforderungen bzgl. KI-Einsatz aus Rechtsgebieten und aber auch sonstigen verpflichtenden Anforderungen (aus anderen Quellen) zuzuordnen. Dabei ist ein risikobasierter Ansatz zu wählen.

Da es sehr schwierig ist, stets sämtliche KI-Compliance-Verpflichtungen zu identifizieren und zu erfüllen, sollte auf Basis einer KI-Compliance-Risiko-Analyse mit den risiko- behaftetsten Verpflichtungen begonnen werden.

„Risikobasiert" heißt in diesem Kontext aber nicht, dass weniger wichtige Verpflichtungen dauerhaft unbeachtet bleiben dürfen.

Dazu heißt es in der DIN ISO 37301:2021 im Kapitel A.4.5 – *Compliance-Verpflichtungen*:

Ein risikobasierter Ansatz sollte gewählt werden, d.h. Organisationen sollten mit der Identifizierung der wichtigsten Compliance-Verpflichtung, die für das Geschäft relevant ist, beginnen und sich anschließend auf alle anderen Compliance-Verpflichtungen konzentrieren (Pareto-Prinzip).

(ESG, CSR), systemische Existenzsicherung (Resilienz) und Governance in: Journal für Medizin- und Gesundheits recht, Ausgabe 2-2021 (zum kostenlosen Download auf scherer-grc.net/publikationen).

[36] Vgl. *Beck Aktuell* – Heute im Recht, Dieselklagen – Sekundäre Darlegungslast und Prognose über die Gesamtlaufleistung, 17. August 2021, https://rsw.beck.de/aktuell/daily/meldung/detail/bgh-dieselklagen-sekundaere-dar- legungslast-und-prognose-ueber-die-gesamtlaufleistung (zuletzt geprüft: 25.09.2021).

[37] Vgl. *Scherer,* Digital Decision Management – die Verknüpfung von Digitalisierung, Nachhaltigkeit und GRC mit Entscheidungsmanagement, Strategieentwicklung, Zielerreichung und Berichterstattung „Aligning GRC with S (Strategy) & P (Performance)", 25.11.2020, online verfügbar unter: https://www.scherer-grc.net/publikationen/digital-decision-management (zuletzt geprüft: 25.09.2021) und Taylor, Digital Decisioning: Using Decision Management to Deliver Business Impact from AI, 2. Auflage, 2019.

### 2.1.3 Rechtsgebiete-Matrix/Rechtskataster:

Für das Thema KI-*Compliance-Managementsystem* sollte eine Art (prozess-)themenbezogenes (Einkauf, Vertrieb etc.) „Rechtskataster" angelegt und gepflegt werden. Dieses stellt den für diesen Bereich maßgeblichen rechtlichen Rahmen dar.

Schon bei der Zuordnung von Rechtsgebieten zu den Bereichen/Prozessen zeigt sich, dass manche Rechtsgebiete/Anforderungen (z.B. KI-IT-Sicherheits-Anforderungen) in nahezu jedem Bereich/Prozess vorkommen, andere KI-Anforderungen/Rechtsthemen schwerpunktmäßig jedoch in nur einzelnen Bereichen/Prozessen.

Bei der Zuordnung von verpflichtenden Anforderungen zu Prozessen sollte wieder an die sogenannte *RACI-Methode* gedacht werden: Die jeweiligen Prozessanwender, die „Responsibles" (R) sollten die Anforderungen in ihrem Prozess kennen und beachten. Die „Prozesseigner", also die für Aktualität, Konformität etc. Verantwortlichen („Accountables" (A), z.B. Leitung Vertrieb für die Vertriebsprozesse) sollten mit Unterstützung durch die Fachspezialisten („Consulted" (C)) dafür sorgen, dass der jeweilige Prozess stets allen relevanten Anforderungen entspricht.

### 2.1.4 Risiko-*Bewertung* bzgl. verpflichtender KI-Anforderungen:

Eine Nichteinhaltung der verpflichtenden KI-Anforderungen kann je nach Ausmaß – z. B. bei Gefahr für Leib und Leben Dritter oder Umweltgefährdung – für die Organisation und die verantwortlichen Organe und/oder Mitarbeiter zu existenzvernichtender Wirkung, Freiheitsstrafen, Geldstrafen und Schadensersatzforderungen einschließlich Reputationsverlust führen.[38]

Die Risiko-Bewertung hat auch für KI-Compliance-Risiken (!) *angemessen*, also nach anerkanntem Stand von Wissenschaft und Praxis, zu erfolgen: Quantifizierung, Aggregation und die Betrachtung der Risikotragfähigkeit ist Standard.[39]

Zur Risiko-Steuerung ist es notwendig, die Ausrichtung und Compliance-Kultur des Unternehmens über regelmäßige Schulungen und den „Tone-from-the-Top" den Mitarbeitern kontinuierlich ins Bewusstsein zu rücken, damit diese stets im Sinne des KI-CMS handeln.[40]

Die Implementierung und Wirksamkeit von Aktivitäten zur Sicherstellung der Verpflichtungen in die Prozesse ist wesentlich effektiver als lediglich Richtlinien und dergleichen zu erlassen.

---

[38] Vgl. *BAG*, Urteil vom 29.04.2021, Az.: 8 AZR 246/20 und United States District Court for the District of Columbia, Consent Decree Civil Action Nos. 1:20-cv-2564, 1:20-cv-2565, 14. September 2020, S. 41 f., online verfügbar unter:https://www.epa.gov/enforcement/daimler-ag-and-mercedes-benz-usa-llc-clean-air-act-civil-settlement-consent-decree (zuletzt geprüft: 25.09.2021).

[39] Vgl. *Institut Deutscher Wirtschaftsprüfer*, Prüfungsstandard 340:2020 und vgl. Scherer/Romeike/Gursky, Mehr Risikokompetenz für eine Neue Welt in: Journal für Medizin- und Gesundheitsrecht, Ausgabe, 3-2021, S. 159–165.

[40] Vgl. *Scherer/Fruth* (Hrsg.), Governance-Management Band II (Standard & Audit), 1. Auflage, 2015, S. 130.

Durch das „Lines-of-Defense"-Modell mit Compliance, Risikomanagement, IKS und Revision[41], die Einrichtung von (KI-gestützten) Monitoring-Prozessen[42], neutralen Ombudspersonen[43] und die Zertifizierung des KI-CMS als Bestandteil eines Integrierten Risiko- und Compliance-Managementsystems sollte die Überwachung und Reifegradbewertung des KI-Compliance-Prozesses und der Komponenten des KI-CMS gewährleistet werden. Dadurch werden auch Risiken der Abweichungen von Vorgaben identifiziert und Aktivitäten zu Verbesserungen des Prozesses und der Komponenten abgeleitet.

### 2.1.5 Intern verpflichtende KI-Anforderungen und KI-Richtlinienmanagement[44]

Hinweis: In Unternehmen herrscht oft ein Begrifflichkeits-Chaos: Begriffe, wie Konzern-, Geschäfts-, Handlungsanweisungen, Handbücher, Guidelines, Richtlinien, Policies u. v. m. sind deshalb klar zu definieren und abzugrenzen.

Dabei sollte auch eine Art Hierarchie bzw. „Verhaltensregel-Pyramide" festgelegt werden. Dafür eignet sich der Code of Conduct als *„Mutter aller Richtlinien".*

Richtlinien werden auf freiwilliger Basis von Unternehmen entwickelt. Innerhalb des Unternehmens sollten die Richtlinien unter Einbindung der Beschäftigtenvertretung (z.B. Betriebs- / Personalrat) als verbindlich beschlossen werden, außerhalb der Unternehmensgrenzen sind sie allerdings nicht allgemein gültig.

Richtlinien müssen klar definiert, dokumentiert, kommuniziert und im Unternehmen gelebt werden, um Compliance-Verstöße zu vermeiden. Maßnahmen zur Erfüllung der Anforderungen aus KI-Richtlinien sollten in die Unternehmensprozesse implementiert werden. Die Einhaltung von Richtlinien hat eine enthaftende Wirkung, dazu unten.

Die Herausforderung beim KI-Richtlinienmanagement:

Es ist unbestritten, dass die Herausforderungen im Bereich von Richtlinien für Unternehmen im Zeitalter der Digitalisierung wachsen. Anforderungen von Kunden, Behörden, Industrie-standards und Auditoren werden immer komplexer.

Häufig müssen Kenntnisnahmen und Kommunikation von Richtlinien und Regelungen nachgewiesen sowie vielschichtige Analysen, Bewertungen und Steuerungsmaßnahmen erstellt werden.

---

[41] Vgl. ebenda, S. 188 f.

[42] Vgl. *Noack*, Künstliche Intelligenz und die Unternehmensleitung in: Festschrift für Christine Windbichler zum 70. Geburtstag am 8. Dezember 2020, S. 956.

[43] Vgl. *Scherer/Fruth* (Hrsg.), Governance-Management, Band I, 2015, S. 186.

[44] Unter einer „Richtlinie" (Synonyme: Policy, Verhaltensregel, Konzern-, Betriebs-, etc.-Anweisung) versteht man eine „unternehmensinterne verpflichtende Regelung für das Verhalten von Management und Mitarbeiter*innen in einem bestimmten Themenbereich. Eine Richtlinie kann ein bereits allgemein durch Gesetz, Rechtsprechung, Standards etc. geregeltes Thema (z.B. Strafbarkeit von Korruption) noch spezifischer (z.B. durch Zuwendungs- Richtlinie mit Angaben von Wertgrenzen) oder ein bisher nicht geregeltes Thema (z.B. die Benutzung von unternehmenseigener Hard- und Software für private Zwecke) erstmals verbindlich regeln.

In der Rechtsprechung wird vieles, was früher noch toleriert oder nicht konsequent verfolgt wurde, mittlerweile empfindlich geahndet.

*„Business as usual"* nur, weil bisher alles gutgegangen ist, wird juristisch nicht toleriert: insbesondere, wenn Führungskräfte als schlechtes Vorbild ihre eigenen Richtlinien nicht befolgen.

FALLBEISPIEL

*OLG Hamm*, Urteil vom 29. Mai 2019 (Az. 8 U 146/18): Außerordentliche Kündigung eines Geschäftsführers, weil er Compliance-Vorgaben umgangen hat

In dem vom *OLG Hamm* entschiedenen Fall wurde die fristlose Kündigung eines Geschäftsführer-Anstellungsvertrages aufgrund des Verstoßes des Geschäftsführers gegen die unternehmensinternen Compliance-Vorschriften als wirksam erachtet:

*„Aus Sicht des Gerichts stellte der Verstoß gegen die Compliance-Vorschriften an sich, [...] einen gravierenden Pflichtverstoß des Klägers dar, der die sofortige Beendigung des Dienst- vertrags rechtfertigte."*[45]

Der besagte Geschäftsführer hatte mit seiner Unterschrift die Auszahlung einer Gutschrift angestoßen, die materiell unberechtigt war und lediglich zur Verschleierung einer hohen Provisionszahlung dienen sollte. Eine Provisionszahlung in der angestrebten Höhe wäre jedoch zustimmungsbedürftig gewesen; diese Zustimmungsbedürftigkeit wurde mittels der Gutschrift letztlich umgangen.

Das Urteil des *OLG Hamm* enthält dabei einige wichtige, grundsätzlich gültige Aussagen *„Hält sich sogar ein Vorgesetzter erkennbar nicht an aus- drückliche und schriftliche Compliance-Regeln, so verlieren diese erst recht gegenüber den Mitarbeitern ihre „Autorität". [...] Im Übrigen ist aber darauf hinzuweisen, dass die Benachrichtigung der zuständigen Compliance-Stellen geboten war. Der Mitgeschäftsführer H 2 war schon deswegen nicht gehalten, gemeinsam mit dem Kläger und anderen Beteiligten das „Missverständnis" auszuräumen, da er nicht von einem Missverständnis ausgehen musste. Zudem lief er bei diesem Vorgehen Gefahr, sich selbst in einen Compliance-Verstoß zu verstricken. Wenn der Kläger auch im Prozess noch Unverständnis über das Vorgehen des Herrn H 2 äußert, offenbart er damit ein anhaltendes Unverständnis über seine eigenen Pflichten. Er wäre selbst gehalten gewesen, so vorzugehen wie sein Mit-Geschäftsführer, und die Problematik offen zu legen."*

Sowie*: „Wer die Compliance-Regeln seines eigenen Unternehmens und die Sanktionen, mit denen sie bewehrt sind, nicht kennt, ist von vornherein ungeeignet, dieses zu führen."*

Und ferner:*„Hinzu kommt, dass der Kläger mit seinem Vorgehen Compliance-Regeln von zentraler Bedeutung für die Beklagte verletzt hat. [...] Gerade von Führungskräften ist insoweit ein hohes Maß an Befolgung zu verlangen."*

Auch grundsätzlich ist das Urteil sehr informativ, da es auch Aussagen über den Ablauf und die Planungen interner Ermittlungen betrifft.

Entscheidend ist insbesondere auch, dass in dem ausgeurteilten Fall der betroffene Geschäftsführer bereits im Vorfeld aufgrund anderer Vorkommnisse ermahnt und darauf hingewiesen wurde, die Compliance-Regeln des Unternehmens zu befolgen.

[45] Vgl. *Haufe*, Sofortige Kündigung eines Geschäftsführer-Dienstvertrags bei Compliance-Verstößen, 23.08.2019, abrufbar unter: https://www.haufe.de/recht/weitere-rechtsgebiete/wirtschaftsrecht/kuendigung-des-geschaeftsfuehrers-wegen-compliance.verstoessen_210_497384.html (letzter Zugriff: 27.08.2020).

### 2.1.6 KI-Compliance-Verpflichtungen in jeder „Managementsystem-Insel“ und *jedem* Standard!

Bei einem *Umwelt*-Managementsystem (ISO 14001) *muss* für die Einhaltung umwelt*rechtlicher* Anforderungen gesorgt werden, bei einem *Informationssicherheits*-Managementsystem (ISO/IEC 27001 ff.) sind es informationssicherheits*rechtliche* Anforderungen. Beim *Qualitäts*- Managementsystem wäre beispielsweise „Product-*Compliance*“ ein zwingendes Thema. Überall wird künftig auch KI eine nicht nur untergeordnete Stellung einnehmen.

Dadurch werden künftig auch bei sämtlichen „Managementsystem-Themen“ (QM, Risk, Umwelt, Energieeffizienz etc.) die jeweiligen KI-Compliance-Verpflichtungen eine wesentliche Rolle spielen.

In der Praxis jedoch findet dies häufig mangels entsprechender Compliancemanagement-Kompetenzen nur wenig Beachtung.

### 2.2 Das KI-Compliance-*Risiko*management (für interne und ausgelagerte (!) Prozesse)

Durch den (KI-Compliance-)Risikomanagement-Prozess werden Gefahren, die durch KI-Pflichtverletzungen verursacht werden und die die Erreichung der Unternehmensziele beeinträchtigen würden, frühzeitig identifiziert, bewertet und gesteuert. Ebenso auch Chancen, die durch den Nachweis regelkonformen Verhaltens entstehen: Beispielsweise Zugang zu Märkten und Kunden, die den Nachweis von KI-Compliance verlangen oder die mögliche Teilnahme an Ausschreibungen.

Eine KI-Compliance-Risiko-Analyse ist die systematische Suche nach möglichen Ursachen und Gefahren für KI-Compliance-Vorfälle. Sie dient als Grundlage für die Bewertung und Entwicklung von Compliance-Steuerungsmaßnahmen. Es gibt diverse (Compliance-)Risiko-Bewertungsmethoden, vgl. IEC 31010 (Risk Assessment).

Relevante (KI-Compliance-)Risiken müssen mit der richtigen Methode richtig bewertet werden.

Jeder Mitarbeiter sollte über ein Basis-Wissen in der (KI-Compliance-)Risikobewertung und „gesunden Menschenverstand“ verfügen. Dies ist einer „Bewertung nach Bauchgefühl“ oder dem Weglassen einer Bewertung vorzuziehen.

Auch ausgegliederte/outgesourcte oder durch Dritte erbrachte Leistungen müssen den rechtlichen KI-Anforderungen entsprechen: Die Pflicht zu Supplier-screening/Überwachung des Delegationsempfängers (auch in Hinsicht auf KI-Compliance) ist umfassend in Gesetzen und Standards gefordert.

Ein wirksames, gelebtes, ggf. zertifiziertes „(Integriertes) KI-Compliance-Managementsystem“ beim Delegationsempfänger ist für diesen und für den Delegierenden zugleich ein möglicher Nachweis für die Erfüllung der Anforderungen.

Für Rest-Risiken ist ein Business Continuity-Managementsystem vorzuhalten.

Es gehört zu den Pflichten eines gewissenhaften Geschäftsführers, Vorstands, Aufsichtsrates und Unternehmers (§§ 43 GmbHG, 93, 116, 107 AktG, 347 HGB), ein (KI-Compliance-)Risiko-Managementsystem vorzuhalten.

Die Früherkennung existenzgefährdender (Compliance-)Risiken ist auch gemäß § 1 StaRUG und § 91 Abs. 2 (und für börsennotierte Gesellschaften: Abs. 3 neu) AktG Pflicht.

### 2.2.1 Normtext DIN / ISO 37301:2021

4.6 Compliance-Risikobeurteilung

Die Organisation muss ihre Compliance-Risiken auf der Grundlage einer Compliance-Risikobeurteilung identifizieren, analysieren und bewerten.

Die Organisation muss ihre Compliance-Risiken identifizieren, indem sie ihre Compliance-Verpflichtungen zu ihren Aktivitäten, Produkten, Dienstleistungen und relevanten Aspekten ihrer Geschäftstätigkeit in Beziehung setzt.

Die Organisation muss Compliance-Risiken in Verbindung mit ausgegliederten oder durch dritte Parteien ausgeführten Prozessen beurteilen.

Die Compliance-Risiken müssen regelmäßig und immer dann bewertet werden, wenn wesentliche Veränderungen der Umstände oder des Kontexts der Organisation auftreten.

Die Organisation muss dokumentierte Informationen über die Compliance-Risikobeurteilung und die Maßnahmen zur Behandlung ihrer Compliance-Risiken aufbewahren.

### 2.2.2 Der (KI-Compliance-)Risikomanagement-Prozess

Der KI-Compliance-Risikomanagement-Prozess muss *implementiert* sowie *wirksam* sein und umfasst das *Erkennen* (die Identifikation), das *Bewerten* und das *Steuern* von Gefahren und Chancen (Risiken), die für das Erreichen der KI-Compliancemanagement-Ziele (= die Einhaltung zwingender KI-Anforderungen) eine Unsicherheit darstellen.

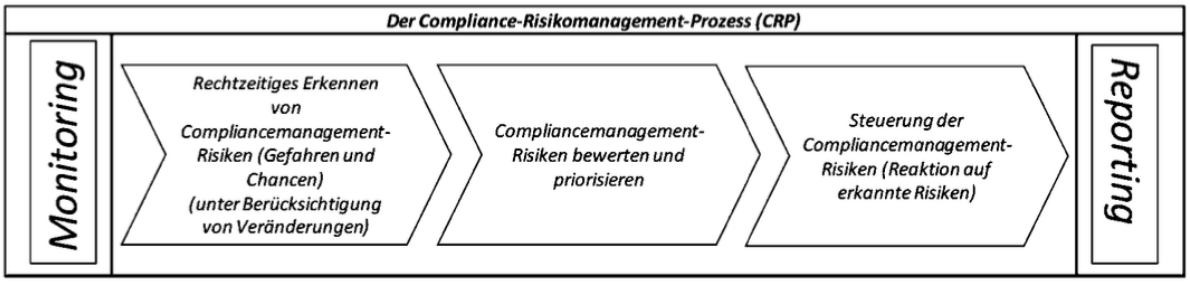



Abb. Der KI-Compliance-Risikomanagement-Prozess

### 2.2.3 Der Unterschied zwischen „KI-Risiko-Melder“, „KI-Risiko-Manager (-Beauftragter/ Officer/-Funktion etc.)“ und „KI-Risiko-Eigner“

Die Abgrenzung dieser Begriffe ist nicht klar geregelt, es gibt hier keine gesetzlichen (Legal-) Definitionen. Deshalb müssen auch diese Begriffe in der Organisation definiert, dokumentiert und geschult werden. Ein – nichtwissenschaftlicher – Vorschlag zur Definition könnte lauten:

**KI-Risiko-Melder (Risk Reporter):**

Ein Risiko-Melder sollte jeder (!) Mitarbeiter in der Organisation zu jeder Zeit (!) (also nicht nur quartalsweise oder einmal zum Jahresende) sein können.

Nur wenn das Wissen „aller Köpfe“ der Organisation bezüglich möglicher Gefahren (und Chancen) auch bzgl. eingesetzter KI-Anwendungen jederzeit zur Verfügung steht und auch genutzt wird, kann frühzeitig auf Risiken reagiert werden.

Ein einziger Risikobeauftragter kann – auch bei periodischer Befragung der Fachabteilungen – nie so effektiv sein wie das gesamte Personal (sofern dies entsprechend sensibilisiert, geschult und (mittels einfacher Tools) in die Lage versetzt wird, Risiken zu entdecken und zu melden).

**KI-(Compliance-)Risikobeauftragter:**

Ein (Compliance-)Risikobeauftragter hat in der Praxis eine Vielzahl von Bezeichnungen und eine herausgehobene Stellung, in der sich seine Aufgaben aus seiner Stellenbeschreibung ergeben. Diese Funktion bündelt Fach- und Kommunikationskompetenz.

**KI-(Compliance-)Risikoeigner (Risk owner):**

Die Rolle/Funktion eines (Compliance-)Risikoeigners (Risk owners) ist in der ISO 31000:2018, Kapitel 2.7 definiert:

> Person oder Stelle mit der Verantwortung und Befugnis, hinsichtlich eines Risikos zu handeln.

In der Praxis finden sich zum Teil jedoch auch abenteuerliche „Ernennungen zu Risikoeignern nach Gießkannenprinzip“, oft leider ziemlich unstrukturiert und ineffektiv. Dies stellt in der Regel ein sehr hohes (!) KI-Compliance-Risiko dar.

Möglichkeiten, Verantwortung und Befugnisse zu verteilen:

Es bestehen vielfältige Möglichkeiten, Verantwortung und Befugnisse zu verteilen. Insofern könnten KI-Compliance-Risikoeigner beispielsweise Abteilungen (gemäß funktionalen Organigrammen) verteilt werden.

Im Zeitalter der prozessorientierten Organisation und der Digitalisierung sollte sich jedoch auch die Zuordnung der „Risikoeigner-Rolle“ zunächst nach dem allgemeinen *„Organisations-, Rollen-, Aufgaben- und Berechtigungs-Konzept“* der Organisation/des Unternehmens richten.

Hinweis: Es ist sinnvoll, analog RACI die für den jeweiligen Prozess Verantwortlichen (A: „Accountable“) auch zu Prozess-Risikoeignern zu machen mit der Verantwortung, auch die KI-Prozess-(Compliance)-Risiken mithilfe der Spezialisten (C: „Consulted“, also z.B. KI-Compliance-Officer oder spezialisierte Rechtsanwälte) zu identifizieren, zu bewerten und zu steuern.

Sofern die Prozesslandschaft der Organisation nicht alle möglichen Ziele bzw. KI-Compliance-Risikofelder abdeckt (z. B: Strategie, Reputation etc.), sind natürlich auch bzgl. dieser Themen/ Ziele Risikoeigner verbindlich zu benennen.

Ein wichtiger Hinweis: Es genügt natürlich nicht, „lediglich Verantwortung zu verteilen“: Da es sich hier um ein Delegationsthema handelt, sind die Anforderungen an Pflichten-Delegation als *wesentliches Compliance-Element* zu beachten und zu dokumentieren:

### 2.2.4 KI-Compliance-Risiko-Managementsystem mit „lines-of-defense“-Modell

1: Über Risiko-Workshops und Analyse-/Bewertungs-Tools werden die relevanten KI-(Compliance) Risiken identifiziert und bewertet.

2: Nach angemessener, risikobasierter Priorisierung werden Risiken gesteuert.

3: Über das „lines of defense“-Modell sollen Gefahren frühzeitig erkannt und verhindert werden,

3.1 (Rechtzeitiges) Erkennen von KI-Compliance-Risiken (Gefahren und Chancen) unter Berücksichtigung von Veränderungen (Risk-Assessment)

Mithilfe eines Risk-Assessment (z.B. nach IEC 31010:2018) müssen Compliance-Risiken ermittelt und bezüglich möglicher Ursachen und Auswirkungen beschrieben werden. Risi- ken aus künftigen Entwicklungen sind über ein „Risks-of-changes-Management“[46] zu eruieren.

Dazu heißt es in DIN ISO 37301:2021 im Kapitel 4.6:

Die Compliance-Risiken müssen regelmäßig und immer dann bewertet werden, wenn wesentliche Veränderungen der Umstände oder des Kontexts der Organisation auf- treten.

Beispiele für *„Top-Risks“* im Bereich „KI-Compliance“ sind:

- Fehlende Übereinstimmung zwischen Unternehmenszielen/Strategie und KI-Compliance- Managementsystem-Zielen/-Strategie
- „Scheinsicherheit“ durch zwar vorhandenes implementiertes, aber *nicht gelebtes* KI-Compliance-Managementsystem
- Keine oder nicht angemessen mit KI-Compliance-Komponenten angereicherte Prozessabläufe/Workflows, die verhindern könnten, dass Compliance-Vorgaben nicht gelebt werden

[46] Vgl. *Scherer*, Good Governance und ganzheitliches strategisches und operatives Management: Die Anreicherung des „unternehmerischen Bauchgefühls“ mit Risiko-, Chancen- und Compliancemanagement, in: Corporate Compliance Zeitschrift (CCZ), 6/2012, S. 201–211, zum kostenlosen Download unter scherer-grc.net.

- Realisierung erheblicher Risiken aus vielfältigsten Pflichtverstößen, weil die entsprechenden KI-Compliance-Anforderungen (vgl. oben) nicht bekannt, bewertet, gesteuert sind.[47]

  Beispiele für Auswirkungen *(„Worst-Case-Szenarien")* wären:

  - Sanktion von Unternehmen (§130 OWiG) und (persönliche zivil- und strafrechtliche) Haftung von Management, Aufsichtsgremien, Gesellschaftern, Mitarbeitern wegen Compliance-Verstoßes
  - Insolvenz/Unternehmenskrise durch Compliance-Fälle[48]
  - Reputationsverlust[49]
  - Ausschluss von Vergabeverfahren
  - Betriebsuntersagung[50]
  - Rechtsstreitigkeiten[51]
  - Strafzahlungen, Geldbußen, sonstige Sanktionen für das Unternehmen (Unternehmenssanktionsrecht!

3.2 KI-Compliance-Risiken bewerten und priorisieren

Bezüglich der Compliance-Risikobewertung gibt es zahlreiche qualitative und quantitative Methoden bis hin zur Bandbreitensimulation.

Beim Einsatz von komplexen Methoden ist auf professionelle Anwendung und zusätzlich auf den gesunden Menschenverstand zu achten!

| Hinweis: Mehr zum Thema Risikobewertungs-Methoden findet sich im Standard IEC 31010:2018 *Risk Assessment* |
|---|

3.3 Steuerung der KI-Compliance-Risiken (Reaktion auf erkannte Risiken)

Zu den Steuerungsmaßnahmen gehören

• die Installation von Prophylaxemaßnahmen und Compliance-Risiko-Früherkennung sowie

• ein Reaktionssystem für erkannte Risiken.

Die Sicherstellung der Durchführung der beschlossenen Maßnahmen (*„Do"*) (Aufgaben/ Projektmanagement), ein Abweichungscontrolling (Feststellung von Abweichungen und Korrekturmaßnahmen) (*„Check"*/ *„Act"*) („Compliance-Steuerungs- und Überwachungssystem") und eine angemessene Reaktion bei Verstößen sind hierbei unverzichtbar.

[47] z. B.: Richtlinien „schlummern ohne Beachtung in Schubladen".
[48] z. B. „Müller Brot", „Sieber-Fleisch" etc.
[49] Hierzu gibt es zahllose Beispiele im Internet.
[50] z. B. „Müller Brot".
[51] Sogar große deutsche Banken finden sich z. T. regelmäßig mit Compliance-Verstößen in den Medien.

3.4 Installation eines Reaktionssystems auf erkannte Compliancemanagement-Risiken (Gefahren und Chancen):

Sofern relevante Compliancemanagement-Risiken identifiziert und bewertet wurden, müssen angemessene Steuerungsmaßnahmen (z.B. daraus abgeleitete To-Dos oder Projekte) konsequent und in angemessener Zeit abgearbeitet werden.

### 2.2.5 KI-(Compliance-)Business Continuity Management (Notfall-, Krisen-, und Betriebsfortführungsmanagement)

Für den stets drohenden Fall, dass sich erhebliche KI-Compliance-Risiken realisieren, ist ein Business Continuity-Managementsystem als Bestandteil des (KI-Compliance-)Risiko-Managementsystems vorzuhalten.

Hinweis: Risiko- und Compliancemanagement gehören zusammen!

Unverzichtbar ist, dass die Disziplinen Risiko- und Compliancemanagement nicht isoliert, sondern mit enger Vernetzung/proaktiver Kommunikation betreut werden (anders als oft in der Praxis) und die Verantwortlichen über angemessene Kompetenzen in beiden Fachgebieten verfügen.

### 2.2.6 Business Partner Screening bzgl. KI-Compliance

Der Begriff des *Business Partner Screening* ist u.a. neben „Know your customer“ auch dem Bereich der „Einkaufs-Compliance“ zuzuordnen, ebenso die „Know your supplier“-Themen. Bei der Beschaffung bzw. Bereitstellung von Prozessen, Leistungen oder Produkten von dritter Seite sind besondere Maßnahmen zu ergreifen:

Je nach Relevanz und Risikobewertungsergebnis bzgl. ausgegliederter Leistungen sind unterschiedliche Anforderungen zu erfüllen und Maßnahmen zu ergreifen. Eine der ersten Maßnahmen, die sich erst seit Kurzem in den moderneren Unternehmen etabliert, ist das „Business- Partner-Screening“, bei dem der externe Leistungserbringer einem Rating/Audit unterzogen wird: Er wird also bezüglich Qualität, Service, Liefertreue, Preis, Ausfallsicherheit, Compliance, Risikomanagement, Nachhaltigkeit u.v.m. genauestens untersucht, zum Teil mittels *„Lieferantenaudits“* oder der *Einforderung diverser Zertifikate.*

Compliance-Risiken in Verbindung mit ausgegliederten oder durch dritte Parteien ausgeführte Prozesse:

Hierzu heißt es in der DIN ISO 37301:2021 im Kapitel 4.6 – *Compliance-Risikobeurteilung:*

Die Organisation muss Compliance-Risiken in Verbindung mit ausgegliederten oder durch dritte Parteien ausgeführten Prozessen beurteilen. [...]

**Überwachungspflichten bei Delegation von Aufgaben an Externe: Supplier Screening:**

Eine „make or buy“-Analyse führt häufig zu einer Entscheidung für die Auslagerung/Delegation von Aufgaben an Externe.

In der arbeitsteiligen, globalen und vernetzten Welt werden sehr viele Leistungen, wie die Lieferung von Material, die Erstellung von Komponenten, aber auch die Erbringung von sonstigen Leistungen ausgelagert.

Externe Leistungserbringer haben natürlich ebenfalls alle für sie geltenden Compliance-Vorgaben zu beachten. Dies ist vertraglich und faktisch (z. B. durch Audits bzw. die Vorlage von Zertifikaten) sicherzustellen, vgl. auch das Lieferketten-Sorgfaltspflichten-Gesetz (LkSG).

Als Ergebnis ist festzuhalten: Es besteht mittlerweile nicht nur die Befugnis, sondern sogar die Pflicht, bei Delegationen auch auf Selbstständige (!) diese sorgfältig auszusuchen, zu instruieren, zu kontrollieren, zu überwachen und mit ihnen eng zu kommunizieren.

Zahlreiche Maßnahmen wurden mittlerweile – auch über die Verbreitung als Anforderungen in QM-Standards – zum „anerkannten Stand in Wissenschaft und Praxis“. Im Bereich der Organisations- und Delegations-Gesetzgebung und -Rechtsprechung ist dies längst verbreitet.

Bei Delegationen/Auslagerungen bestehen auch gegenüber Selbstständigen Kontroll-, Überwachungs-, Informations- und gegebenenfalls auch Weisungsrechte oder sogar auch -Pflichten.[52]

## 3. KI-Compliance-Managementsystem als relevanter Teil von Governance

Die international anerkannte ISO 37000 **„Governance of Organizations“** stellt als Bindeglied zwischen ES***G*** und ***G***RC unter Punkt 6.8 die Anforderungen an einen angemessenen Umgang mit Informationen und Daten – auch unter dem Aspekt des Einsatzes von KI - als Basis für *„gute unternehmerische Entscheidungen“* dar[53].

***ISO 37000 Governance of organizations — Leitfaden[54]***

***6.8 Daten und Entscheidungen***

***6.8.1 Grundsatz***
*Das Leitungsgremium sollte Daten als wertvolle Ressource für die Entscheidungsfindung des Leitungsgremiums, der Organisation und anderer anerkennen.*

***6.8.2 Begründung***

*Letztendlich dienen Daten dazu, Informationen für die Entscheidungsfindung bereitzustellen, entweder direkt durch Menschen oder durch Automatisierung.*

*Aufgrund der Allgegenwärtigkeit der Technologie nimmt der Wert von Daten als strategische und wesentliche Ressource für Unternehmen immer mehr zu. Dies bringt die Verantwortung mit sich, mit ihren potenziellen strategischen und betrieblichen Auswirkungen angemessen umzugehen.*

---

[52] Siehe hierzu auch den Artikel von *Scherer:* Business Partner Screening versus Scheinselbstständigkeit

[53] Vgl. Scherer, Digital Decision Management - die Verknüpfung von Digitalisierung, Nachhaltigkeit und GRC mit Entscheidungsmanagement, Strategieentwicklung, Zielerreichung und Berichterstattung, 2020, zum kostenlosen Download auf www.gmrc.de.

[54] Originaltext in Englisch: Die deutsche Übersetzung stammt vom Verfasser dieses Artikels.

*Daten sind das Rohmaterial, aus dem Informationen abgeleitet werden und aus dem Erkenntnisse für die Entscheidungsfindung gewonnen werden. Die Informationen, die aus den Daten extrahiert werden, variieren je nach Technologie, Thema und organisatorischen Anforderungen. (…)*
*Der Wert von Daten für die Entscheidungsfindung kann aus verschiedenen Blickwinkeln betrachtet werden, z. B.*
*a) Entscheidungsfindung innerhalb der Organisation:*

*1) Entscheidungsfindung innerhalb des Leitungsgremiums.*
*Die Lebensfähigkeit einer Organisation hängt von den Daten ab, auf die sich das Leitungsorgan stützt, um Entscheidungen zu treffen.*

*2) Entscheidungsfindung in der gesamten Organisation.*
*Das Funktionieren einer Organisation hängt von Strukturen und Praktiken ab, die eine effektive Entscheidungsfindung gewährleisten. Eine solche Entscheidungsfindung basiert auf vertrauenswürdigen Informationen und darauf, dass Entscheidungen mit der für sie angemessenen Kompetenz und Verantwortung getroffen werden: (…)*

### *6.8.3 Wichtige Aspekte der Umsetzung*

#### *6.8.3.1 Allgemein*

*Das Leitungsorgan sollte sicherstellen, dass die Organisation die Art und den Umfang ihrer Datennutzung identifiziert, verwaltet, überwacht und kommuniziert (siehe 6.5.3).*

*Das Leitungsorgan sollte insbesondere sicherstellen, dass die Organisation Daten als strategische Ressource anerkennt und dass die Organisation Daten verantwortungsvoll und ethisch korrekt nutzt.*

#### *6.8.3.2 Sicherstellung einer effektiven Entscheidungsfindung*

##### *6.8.3.2.1 Sicherstellung einer effektiven Entscheidungsfindung innerhalb des Leitungsgremiums*

*Das Leitungsgremium sollte Entscheidungen in der erforderlichen Qualität treffen und sicherstellen, dass seine Entscheidungen auf angemessener Grundlage getroffen werden.*

*Das Leitungsgremium sollte:*

*a) ein angemessenes Gleichgewicht zwischen der Leitung der Diskussionen und der Sicherstellung, dass jedes Mitglied die Möglichkeit hat, seine unabhängige Einschätzung zu äußern, wahren;*

*b) sicherstellen, dass die Verpflichtung besteht, die kollektive Entscheidung zu unterstützen und danach zu handeln;*

*c) den Grad seiner Unabhängigkeit und die Auswirkung dieses Grades auf seine Entscheidungsfindung, einschließlich finanzieller Interessen, Stellung, Verbindungen, Beziehungen, Voreingenommenheit und Allianzen, berücksichtigen;*
*d) Interessenkonflikte bei der Entscheidungsfindung sorgfältig berücksichtigen;*

*e) auf die Dynamik des Leitungsgremiums achten, z. B. auf die übermäßige Abhängigkeit von einem einzelnen Mitglied bei der Entscheidungsfindung;*

*f) sein Recht und seine Verantwortung wahrnehmen, die von ihm benötigten Informationen bestimmen und erhalten, einschließlich der Festlegung geeigneter Datenerhebungsmethoden, der Vorbereitung und der rechtzeitigen Bereitstellung von Informationen;*

*g) sicherstellen, dass die Integrität der erhaltenen Daten und Informationen, insbesondere ihre Richtigkeit und Vollständigkeit, gewährleistet ist;*

*h) sicherstellen, dass verschiedene Beiträge zu einem rigorosen, offenen und transparenten Entscheidungsfindungsprozess geliefert werden und dass die erzielbaren Ergebnisse, die Optionen zu deren Erreichung und deren Auswirkungen verstanden werden. (…)*

#### *6.8.3.2.2 Sicherstellung einer effektiven Entscheidungsfindung in der gesamten Organisation*

*Die Entscheidungsfindung in der gesamten Organisation sollte durch eine angemessene Delegation unterstützt werden. Diese Delegation sollte zusammen mit geeigneten Sicherungsverfahren formalisiert werden.*

*Darüber hinaus sollte das Leitungsorgan sicherstellen, dass:*

*a) die Befugnis dem Grad der Verantwortung, der mit den Entscheidungen verbunden ist; entspricht*

*b) die Grenzen der Entscheidungsbefugnis auf der Grundlage des damit verbundenen Risikos angewandt werden, insbesondere wenn eine automatisierte Entscheidungsfindung eingesetzt wird;*

*c) die Informationsstrukturen, einschließlich des Zugangs zu Informationen, der Überwachung und der möglichen Abmilderung von Fehlentscheidungen ausreichend sind, um die Einhaltung der organisatorischen Anforderungen zu gewährleisten.*

#### *6.8.3.3 Erkennen von Daten als strategische Ressource*

*Auf Basis der Erkenntnis, dass Daten einen strategischen Vorteil (oder Nachteil) darstellen können, sollte das Leitungsorgan folgendes tun:*

*a) sicherstellen, dass die Organisation einen formalen Ansatz für ihr Datenmanagement einführt und, falls erforderlich, für angemessen Sicherheit sorgt;*

*b) die Nutzung und potenzielle Nutzung von Daten durch die Organisation und andere (z. B. Lieferanten, Kunden, Aufsichtsbehörden und andere relevante Interessengruppen sowie Konkurrenten und Personen, die die Daten missbrauchen könnten) verstehen;*

*c) die Komplexität und wachsende Bedeutung von Daten anerkennen und Governance-Richtlinien und -Prozesse festlegen, die auf die Bedürfnisse des Unternehmens und den Grad der erforderlichen Veränderungen abgestimmt sind;*

*d) sicherstellen, dass der Informationsbedarf der Organisation durch die derzeitigen und künftigen technologischen Möglichkeiten ausreichend gedeckt wird;*

*e) Art und Umfang der Datennutzung durch die Organisation als Nachweis der Verantwortlichkeit für diese Ressource mitteilen.*

#### *6.8.3.4 Verantwortungsvolle Datennutzung sicherstellen*

*Neue Technologien führen zu einer Zunahme des Datenvolumens und -werts und zu einer Verantwortung der Leitungsorgane, folgendes zu gewährleisten, dass:*

*— die Daten ethisch korrekt verwendet werden;*

*— wertvolle Chancen genutzt werden;*

*— sensible Daten geschützt und gesichert sind.*

*Das Leitungsorgan sollte die Verwendung von Daten und der sie unterstützenden Informationstechnologie steuern und ausreichend überwachen, um sicherzustellen, dass die Organisation ihre Risikotragfähigkeit und den organisatorischen Risikorahmen einhält.*

*Dies kann Folgendes beinhalten:*

*a) die Einführung eines Systems, das sicherstellt, dass die Rechte, Pflichten und Anforderungenin Bezug auf die Datensätze verstanden und verfolgt werden , z. B. die Verpflichtungen in Bezug auf den Schutz der Privatsphäre und die Rechte an geistigem Eigentum;*

*b) die Einführung eines risikobasierten Informationssicherheitsmanagementsystems (ISMS);*

*c) angemessene Prüfung und Überwachung der Informationstechnologie, um sicherzustellen, dass sie verantwortungsvoll und ethisch vertretbar eingesetzt wird und den Absichten und Erwartungen des Leitungsorgans sowie den Compliance-Verpflichtungen der Organisation entspricht;*

*d) Innovationsprozesse, um sicherzustellen, dass Veränderungen in der Informationstechnologie schnell bewertet werden können und, falls erforderlich und angemessen, die Governance-Politik aktualisiert werden kann, um neue Möglichkeiten zu nutzen;*

*e) Sicherstellung, dass menschliches Verhalten bei der Anwendung von Informationstechnologie berücksichtigt wird, einschließlich der Aspekte Sicherheit, Zweckmäßigkeit und Ausrichtung auf den Unternehmenszweck;*

*f) Sicherstellung, dass bei der Nutzung der Informationstechnologie durch das Unternehmen, insbesondere im Zusammenhang mit dem Humankapital, die Interessengruppen des Unternehmens berücksichtigt werden.*

## 4. Enthaftende Wirkung eines KI-Compliance-Managementsystems nach höchstrichterlicher Rechtsprechung[55]

### 4.1 Allgemeine, internationale Rechtsfigur und gefestigte Rechtslage in Deutschland: Enthaftende Wirkung einer Compliance-Organisation[56]

In jüngster Zeit bestätigten die höchstrichterliche deutsche Rechtsprechung (vgl. *BGH*-Entscheidungen „KMW“ und „Selbstreinigung“[57]), Gesetzgeber[58] und Exekutive[59] die allgemein anzuerkennende Rechtsfigur, dass organisatorische Vorkehrungen zur Vermeidung von Pflichtverstößen unter Umständen im Einzelfall den Vorwurf vorsätzlichen Handelns entfallen lassen oder bei der Strafzumessung zu berücksichtigen sind.

Auch der Gesetzesentwurf des *Bundesjustizministeriums* zur Unternehmenssanktion bei Compliance-Verstößen[60] ging in diese Richtung.[61]

Dies gibt es in den USA seit den 1980er Jahren in Form der *US Sentencing Guidelines*.

---

[55] Ausführlicher hierzu: *Scherer, Grötsch, Fruth*, Enthaftendes Compliance- und Whistleblowing-Managementsystem nach aktueller Rechtslage –Ein „Must have“ für alle Führungskräfte!, Risknet, 2023.

[56] *Scherer*, Compliance-Managementsystem nach DIN ISO 37301 erfolgreich implementieren, integrieren, auditieren, zertifizieren, 1. Auflage 2022, Herausgeber: DIN, Beuth-Verlag, S. 21 ff.

[57] *BGH*, Urteil vom 09.05.2017 - 1 StR 265/16 und *BGH*, Urteil vom 27.04.2022 – 5 StR 278/21, sowie demnächst wohl auch der *EuGH* (Az. C 807/21)

[58] Vgl. § 38 Einführungsgesetz zur AO (EGAO), § 125 Gesetz gegen Wettbewerbsbeschränkungen (GWB), etc.

[59] Vgl. z. B. Rundschreiben des *Bundesministeriums für Finanzen* (BMF) zu § 153 AO vom 23.05.2016, DStR 2016, 1218: „Tax Compliance“ und die Pressemitteilung, vgl. *Beyer*, Bayern: Einbeziehung der Compliance in die Steuerprüfung, nwb.de vom 1.2.2023 des *Bayerischen Ministeriums für Finanzen* 2022 über die künftige Einbeziehung von Steuerkontrollsystemen in die steuerliche Prüfung

[60] Referentenentwurf: Gesetz zur Förderung der Unternehmensintegrität vom September 2020

[61] Die Justizminister Konferenz der Länder bat im Mai 2023, einen neuen Entwurf für die aktuelle Legislaturperiode vorzulegen.

In anderen Ländern ist die Rechtslage abhängig vom Haftungsmodell der jeweiligen Rechtsordnung.[62]

Internationale Standards verweisen ebenfalls auf diese Wirkungen.[63]

Dass Compliance- / Kontroll-Systeme tatbestandsausschließend oder bei der Strafzumessung positiv zu berücksichtigen sind, ist in Deutschland nunmehr gefestigte Rechtslage[64], wenngleich bei Instanzgerichten, (Verfolgungs-) Behörden und auch in Wissenschaft und Praxis hierzu noch u.U. für Transparenz gesorgt werden muss.

### 4.2 Ausgangslage: Die haftungsbewehrte Pflicht für Leitungs- und Aufsichtsorgane zur Einrichtung eines angemessenen und wirksamen Compliance- / Kontroll-Systems

Das Thema ist nicht nur für Konzerne, sondern auch für den Mittelstand höchst virulent.
Das *OLG Nürnberg*[65] stellte jüngst fest, dass die Pflicht zur Einrichtung eines angemessenen und wirksamen Internen Kontroll- (IKS) und Compliance-Managementsystems auch bereits für Geschäftsführer kleinerer Unternehmen gilt.[66]

---

[62] *Trüg*, Die Verteidigung von Unternehmen, NZWiSt 2022, S. 106 f.:
***„(…) Ob und inwieweit solche Compliance-Maßnahmen bereits auf tatbestandlicher Ebene oder jedenfalls strafmildernd zu berücksichtigen sind, hängt zunächst maßgeblich von dem der Unternehmensverantwortlichkeit zu Grunde gelegten Modell ab****.*
*Eine eher ablehnende Haltung der Milderung aufgrund etablierter Compliance ist etwa in* ***Frankreich*** *verbreitet; (…)*
*Eine entlastende Wirkung von Compliance-Maßnahmen kann beispielsweise als Korrektiv einer extensiven strafrechtlichen Verantwortlichkeit wie in den* ***USA*** *auf der Grundlage der respondeat-superior-Doktrin fungieren, vor allem aber mit Blick auf den Vorwurf eines Organisationsversagens des Verbandes wirken (wie dies nach der* ***Schweizer*** *Rechtslage möglich ist).*
*Entsprechend sind derartige Präventionsmaßnahmen in der* ***österreichischen*** *Regelung ausdrücklich als Milderungsgrund anerkannt. (…)"*

[63] Vgl. Einleitung zur (DIN) ISO 37301:2021: *„In verschiedenen Rechtsordnungen* ***haben Gerichte bei der Strafzumessung*** *für Gesetzesverstöße* ***das Bekenntnis einer Organisation zu Compliance durch das Compliance-Managementsystem berücksichtigt.*** *Aus diesem Grund können auch Regulierungsbehörden und Gerichte von diesem Dokument als Bezugspunkt profitieren."*

[64] *Trüg*, Die Verteidigung von Unternehmen, NZWiSt 2022, S. 106 f.:
*„(…)* ***dass gerade das Vorliegen von zwei BGH Entscheidungen im Abstand von fünf Jahren nach Sicht des Verfassers durchaus eine in diesem Sinne gefestigte Rechtsprechung darstellt.*** *Dabei ist zu berücksichtigen, dass es gerade nicht einer Vielzahl von bestätigenden BGH-Rechtsprechung bedarf, um eine gefestigte Rechtsprechung zu bilden. Entscheidungen des Bundesgerichtshofs kommen nach den Vorschriften über die Zulassung der Revision (vergleiche § 543 ZPO) nur dann infrage,* ***wenn eine Rechtssache grundsätzliche Bedeutung hat*** *oder die Fortbildung des Rechts oder die Sicherung einer einheitlichen Rechtsprechung eine Entscheidung erfordert. Daher kann auch hier von einer gefestigten Rechtsprechung ausgegangen werden, an die sich die Instanzgerichte gebunden fühlen sollten."*

[65] *OLG Nürnberg*, Endurteil vom 30.03.2022, 12 U 1520/19 (Tankstellenpächter)

[66] Dies stellte im *Siemens-Fall* das *Landgericht München* („Neubürger") bereits 2013 fest. Gesetzlich vorgeschrieben ist ein Compliance-Managementsystem in bestimmten Branchen (vgl. §§ 29 VAG, 25a KWG) bzw. für alle „großen" Unternehmen
(§ 91 AktG) seit langem

Der *Bundesfinanzhof*[67] bekräftigte jüngst die ständige Rechtsprechung[68], dass eine rechtskonforme (enthaftende) Pflichtendelegation auch die kontinuierliche Überwachung des Delegationsempfängers voraussetzt und Geschäftsführer ohne diese (Compliance-) Kompetenzen das Amt gar nicht antreten oder niederlegen sollten.

Sehr interessant ist auch bezüglich der Abgrenzung der Aufgaben des Leitungsorgans und der „*ausdrücklich Beauftragten*“[69] das Urteil des *Arbeitsgerichts Heilbronn*[70]:
Primär verantwortlich für die organisatorische Umsetzung von technischen und organisatorischen Maßnahmen (TOM) zur Herstellung eines angemessenen Datenschutzniveaus sei der Arbeitgeber und nicht der Datenschutzbeauftragte als „ausdrücklich Beauftragter“, sofern diese Verantwortlichkeit nicht klar anders in der Beauftragung geregelt sei („*ordnungsgemäße Übertragung von Unternehmerpflichten*“).

Darüber hinaus bräuchten Beschäftigte, die als (Datenschutz-) „ausdrücklich Beauftragte“ benannt werden, ausreichend zeitliche Ressourcen, um ihrer Verantwortung gerecht zu werden.
Angemessene (zeitliche) Ressourcen zur ordnungsgemäßen Wahrnehmung des Amtes stellten eine wesentliche Voraussetzung für eine ordnungsgemäße, enthaftende Übertragung von Unternehmerpflichten dar.

### 4.3 Haftung der Organisation, der Leitungs- und Aufsichtsorgane und der gemäß § 9 Abs. 2 OWiG[71] ausdrücklich Beauftragten[72] für eigene oder fremde schuldhafte Pflichtenverletzung

#### 4.3.1 Haftung für eigene schuldhafte Pflichtverletzungen

##### 4.3.1.1 Haftung der Organisation

[67] *BFH*, Beschluss vom 15.11.2022, VII R 23/19 (Haftung bei inkompetentem Geschäftsführer)

[68] Vgl. *Scherer,* Business Partner Screening, 2017, gmrc.de, mit weiteren Nachweisen

[69] Vgl. §§ 30, 9 Abs. 2 OWiG

[70] *ArbG Heilbronn*, Urteil vom 29.9.2022, 8 Ca 135 / 22 („nachlässiger Datenschutzbeauftragter und Justiziar?“)

[71] § 9 Abs. 2 OWiG: „Ist jemand von dem Inhaber eines Betriebes oder einem sonst dazu Befugten (…)
1.beauftragt, den Betrieb ganz oder zum Teil zu leiten, oder
2.ausdrücklich beauftragt, in eigener Verantwortung Aufgaben wahrzunehmen, die dem Inhaber des Betriebes obliegen,
und handelt er auf Grund dieses Auftrages, so ist ein Gesetz, nach dem besondere persönliche Merkmale die Möglichkeit der Ahndung begründen, auch auf den Beauftragten anzuwenden, wenn diese Merkmale zwar nicht bei ihm, aber bei dem Inhaber des Betriebes vorliegen. (…)“; vgl. auch § 13 Abs. 2 ArbSchG, § 15 Abs. 1 Nr. 1 SGB VII, § 13 BGV A1

[72] Vgl. „Übertragung von Unternehmerpflichten“, zum Beispiel auf Risiko-, Compliance-, Datenschutz-, Arbeitssicherheits-, Informationssicherheits-, etc.- Beauftragte, vgl. *Scherer*, Haftung eines Risikomanagers, 2018, zum Download auf risknet.de

Die Organisation haftet in der Regel nur, wenn ihr eine schuldhafte Pflichtverletzung ihrer Organe oder besonders Beauftragten zugerechnet werden kann.[73]

Eine verschuldensunabhängige Haftung („strict liability" / Gefährdungshaftung) der Organisation besteht in der Regel nicht. [74]
Ein Unternehmensstraf- oder Unternehmenssanktionsrecht, wie in anderen Ländern oder in der letzten Koalition entworfen,[75] gibt es bisher in Deutschland nicht.

#### 4.3.1.2 Haftung der Leitungsorgane und „ausdrücklich Beauftragter" bei eigenem, aktiven Tun

Sofern der schuldhafte Pflichtverstoß[76] von Leitungsorgan oder „ausdrücklich Beauftragtem" selbst begangen wurde, haften diese nach allgemeinen Grundsätzen der Innen- und Außen-Haftung. Es erfolgt dann auch eine Zurechnung des schuldhaften Pflichtverstoßes an die Organisation.
Auch Mitglieder des Aufsichtsorgans können wegen Verletzung ihrer Aufsichtspflichten, z.B. wegen eines fehlenden angemessenen und wirksamen Risiko-, Compliance-, Internen Kontroll-Systems, persönlich haften (§§ 116, 107 AktG).

### 4.3.2 Haftung der Leitungsorgane und „ausdrücklich Beauftragten" bei schuldhaften Pflichtverletzungen von *Beschäftigten unterhalb der Leitungsebene*

Eine schuldhafte *Pflichtverletzung von Beschäftigten unterhalb der Leitungsebene* kann zur eigenen schuldhaften Pflichtverletzung der Leitungsorgane oder „ausdrücklich Beauftragten" führen, wenn ein Mangel des Kontroll- und Überwachungs-Systems (mit-)ursächlich für den schuldhaften Pflichtverstoß des/der Beschäftigten war (mittelbare Verantwortung durch Aufsichtspflichtverletzung / Organisationspflichtverletzung).

Diese Pflichtverletzung der Leitungsorgane oder „ausdrücklich Beauftragten" kann wiederum der Organisation haftungsbegründend zugerechnet werden.

---

[73] Vgl. §§ 130, 30 OWiG, 84 DSGVO, etc.

[74] Vgl. Schlussantrag des Generalanwalts des EuGH vom 27.4.2023, Aktenzeichen C 807 / 21 („DSGVO-Bußgeld gegen Vonovia").
Die Entscheidung des EuGH wird auf europäischer Ebene diese bereits in Deutschland geltende Rechtslage klären und ist aufgrund der wachsenden Anzahl von Regulierungen durch die EU (Nachhaltigkeits-, KI-, Product-, etc.-Compliance) besonders beachtenswert.

[75] Vgl. Referentenentwurf zum Unternehmenssanktionsrecht („Entwurf eines Gesetzes zur Stärkung der Integrität in der Wirtschaft") vom 16.06.2020

[76] Z.B. Tax-, Product-, DSGVO-, IT-, Informationssicherheits-, etc.- Compliance-Verstoß

Auch die Mitglieder von Aufsichtsgremien können in diesen Fällen u.U. haften.

### 4.4 Enthaftende Wirkung auf Tatbestandsebene durch Einrichtung eines (KI-) Compliance- / Kontroll-Systems *vor* der Tat

Das Leitungsorgan kann bei ordnungsgemäßer Pflichtendelegation und / oder Übertragung von Unternehmerpflichten auch Verantwortung auf „ausdrücklich Beauftragte“ delegieren. Primär- und Letzt-(Überwachungs-) Verantwortung bleibt in der Regel beim Leitungsorgan.

Die Einrichtung eines angemessenen und wirksamen Kontroll- und Überwachungs-Systems (ESGRC- Compliance-, Tax-, Risiko-, IKS-, etc.- Managementsystems) lässt bei Pflichtverletzungen durch Beschäftigte unterhalb der Leitungsebene i.d.R. die Pflichtverletzung durch Organisations- oder Überwachungsverschulden beim Leitungsorgan oder „ausdrücklich Beauftragten“ bereits auf der Tatbestandsebene entfallen.[77]
Dann kann auch keine Zurechnung einer schuldhaften Pflichtverletzung zulasten der Organisation / des Unternehmens zur Haftung[78] derselben führen.

Ebenso ist in diesen Fällen auch den Mitgliedern von Aufsichtsgremien kein Vorwurf zu machen.

### 4.5 Strafbefreiende Maßnahmen *nach* der Tat

*Nach* der Tat könnten Selbstanzeige[79], „tätige Reue“ oder Kronzeugenregelungen (vgl. Kartellrecht) zur Strafbefreiung führen.

---

[77] Vgl. Trüg, Die Verteidigung von Unternehmen, NZWiSt 2022, S. 106 f.:

*Überzeugend ist, Compliance-Bestrebungen bereits auf Tatbestandsebene jdfs. in solchen Konstellationen von Zuwiderhandlungen entscheidende Bedeutung beizumessen, in denen kein Unternehmensrepräsentant aus dem Anwendungsbereich von* § 9 OWiG *verantwortlich beteiligt war. Dann steht noch eine Aufsichtspflichtverletzung gemäß* § 130 OWiG *in Rede. Wenn aber der Betriebs- oder Unternehmensinhaber die gesetzlich vorgesehenen Organisations- und Aufsichtspflichten erfüllt, also im Rahmen eines Compliance-Programms gerade jene Maßnahmen ergriffen und umgesetzt hat, welche zur Erfüllung der gesetzlich vorgesehenen Organisations- und Aufsichtspflichten erforderlich sind, scheidet eine Verantwortlichkeit nach § 130 OWiG aus. Denn ein den betrieblichen Anforderungen genügendes Compliance-System ist als erforderliche Aufsichtsmaßnahme im Sinne des § 130 Abs. 1 OWiG anzusehen.*

*Compliance ist daher unmittelbarer Ausfluss des durch § 130 OWiG geforderten Pflichtenprogramms, weil Compliance ein rechtmäßiges Verhalten der Unternehmensmitarbeiter gewährleisten soll. Effiziente Compliance führt also in dieser Konstellation zu* ***einer vollständigen Enthaftung (auf Tatbestandsebene)****. Es liegt dann keine Ordnungswidrigkeit im Sinne des § 130 OWiG vor. Nach oben dargelegten Grundsätzen fehlt es an einer Anknüpfungstat im Sinne des § 30 OWiG. (…)*

*So gesehen stellt ein etabliertes und effizientes Compliance-Programm auch ein zu berücksichtigendes* ***(milderndes) Vortatverhalten*** *dar. Verdeutlicht wird dies anhand solcher Einrichtungen wie etwa* ***Whistleblower-Hotlines, Audits*** *oder Maßnahmen der Transparenzförderung (Vier-Augen-Prinzip, Funktionstrennung oder sogenanntes Businesspartner-Screening). Diese Maßnahmen dienen dazu, Fehlverhalten zu verhindern bzw. im Falle erfolgten Fehlverhaltens eine effektive Aufarbeitung zu ermöglichen.*

[78] §§ 130, 30 OWiG, 84 DSGVO, etc.

[79] Vgl. *Hauschka/Moosmayer/Lösler-Besch/Starck*, Corporate Compliance, 3. Auflage 2016, § 33 Tax Compliance, Rn 81: „*Die Einrichtung eines Tax Compliance-Management-Systems kann ebenfalls dabei helfen, bestehende*

### 4.6 Strafmildernde Berücksichtigung eines (KI-)Compliance-Managementsystems, Hinweisgeber-Systems und eines „Selbstreinigungsprozesses“ *nach* der Tat im Straf- und Bußgeldverfahren bei Strafzumessung

Bei der Strafzumessung ist unter „Nachtatverhalten[80]“ ein Selbstreinigungsprozess, die Einrichtung eines Compliance-Managementsystems und Hinweisgebersystems aufgrund wiederholt bestätigender Rechtsprechung des *BGH,* insbesondere auch im Bereich KI-Compliance, strafmildernd bei der Strafzumessung zu berücksichtigen.[81]

### 4.7 Anforderungen an die Ausgestaltung eines strafbefreienden / haftungsmildernden KI-Compliance-Managementsystems

Die Anforderungen, die die Rechtsprechung, unter anderem der *BGH* aus dem Jahr 2017 unter Verweis auf *Raum*, an ein enthaftend / strafmildernd wirkendes Compliance-Managementsystem und Hinweisgebersystem stellt, ergeben sich aus eben diesen Quellen im Zusammenwirken mit diversen aktuellen Standards für Compliance-Managementsysteme zum Beispiel DIN ISO 37301:2021, COSO I:2017 und IDW PS 980: 2022.

### 4.8 Sinnhaftigkeit der aktuellen Rechtslage

Die „Belohnung“ von Aktivitäten einer Organisation in Richtung „rechtssichere Organisation“, Compliance- und Kontroll-System mit der Möglichkeit, dass Hinweisgeber unter Wahrung der Vertraulichkeit frühzeitig auf Missstände hinweisen können, stellt in Anbetracht der Überlastung unseres Justizsystems einen wichtigen und richtigen Schritt dar: Weg von aufwändigen Ermittlungen, die häufig im Sande verlaufen und niemandem nutzen, hin zur

---

*Risiken zu minimieren, wenn sich das Unternehmen bereits im steuerstrafrechtlich relevanten Bereich bewegt. So kann eine umfassende Vorbereitung auf den Besuch der Steuerfahndung vermeidbare negative Folgen verhindern sowie die Kenntnis und ggf.* ***Inanspruchnahme der Möglichkeit zur Selbstanzeige*** *sogar* ***zur Straffreiheit führen****.“*

[80] In älteren Prüfungsschemata findet die aktuelle Rechtslage häufig noch keine angemessene Berücksichtigung, vgl. z.B. *Schäfer / Sander / Gemmeren*, Praxis der Strafzumessung, 6. Auflage 2017, Teil 4: Die strafzumessungserheblichen Umstände, Rn. 586

[81] Vgl. *Trüg*, Die Verteidigung von Unternehmen, NZWiSt 2022, S. 106 ff. :

*„(…) Aus einer etablierten und effizienten Compliance-Maßnahme lässt sich auf Normakzeptanz und damit auf ein Bekenntnis zur Rechtstreue schließen. Denn eine ernst gemeinte Compliance-Maßnahme regelt, überwacht und sanktioniert (potentielles) Fehlverhalten von Mitarbeitern, gerade um normgemäße Verhalten der Unternehmensmitarbeiter zu gewährleisten.*

*(…) zeigt diese Überlegung deutlich,* ***dass Compliance sowohl die „Schwere der Zuwiderhandlung“ einschränkt als auch den „Vorwurf, der den Täter trifft“.*** *(…) Eine bußgeldmindernde Wirkung kommt, wie schon angedeutet, auch der Etablierung nachträglicher Compliance zu. So ergibt sich die Notwendigkeit der Berücksichtigung nachträglicher Compliance-Bestrebungen freilich nicht aus dem der Geldbuße innewohnenden Präventionsziel, sondern vielmehr aus dem die Berücksichtigung des Nachtatverhaltens gebietenden § 46 StGB selbst. Unterstrichen wird dies für Compliance-Systeme darüber hinaus von der strafgerichtlichen Rechtsprechung, welche mildernd anrechnet, dass der Täter einer Rückfallgefahr weitgehend vorgebeugt hat. Insbesondere wird generell die Bereitschaft honoriert, sich im Wege der Therapie oder Beratung mit den Ursachen der Tat auseinanderzusetzen, um einem Rückfall vorzubeugen. Auf diesen Zweck zielen schließlich (präventive und nachträgliche) Compliance-Bestrebungen.“*

Prophylaxe. Das ist eine systemische Veränderung. Ähnlich der Geschichte von chinesischen Ärzten, die nicht fürs Heilen, sondern fürs Gesund-Erhalten der Patienten bezahlt werden sollen…

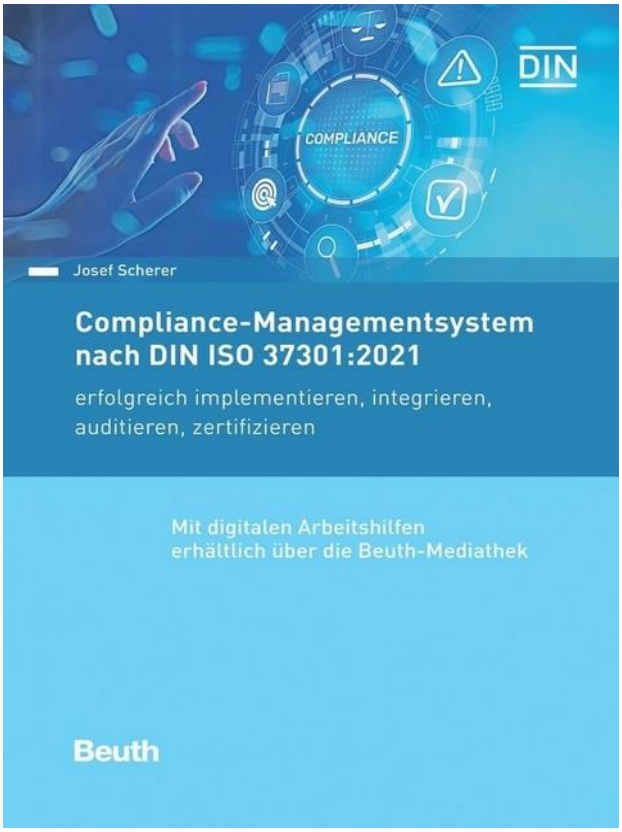
## 5. Auditierung und Zertifizierung eines KI-Compliance-Managementsystems

Viele Organisation haben bereits bemerkt, dass der Ansatz eines *Integrierten* GRC- / ESG-Managementsystems effektiver und zugleich wesentlich kostengünstiger ist, als zahllose „Insel-Systeme“ bürokratisch, mit hohen Kosten und wenig Wertbeitrag zu verwalten.
Entsprechend häufen sich Anfragen nach Kombi-Zertifikaten bei den Zertifizierenden.

Auch ein KI-Compliance-Managementsystem sollte nicht als „Insel“, sondern als integrierter Bestandteil eines CMS oder ESGRC-Managementsystems auditiert und zertifiziert werden.

**Zur Vertiefung:**

*Scherer,* Compliance-Managementsystem nach DIN / ISO 37301
erfolgreich implementieren, integrieren, auditieren, zertifizieren,
Beuth Verlag, 2022



**Prof. Dr. jur. Josef Scherer**

Rechtsanwalt und Consulter
Gründer und Leiter des Internationalen Instituts für Governance, Management, Risk- und Compliancemanagement und Leiter der Stabsstelle ESGRC der Technischen Hochschule Deggendorf THD

Rechtsanwalt Prof. Dr. Josef Scherer ist seit 1996 Professor für Unternehmensrecht (Compliance), Risiko- und Krisenmanagement, Sanierungs- und Insolvenzrecht an der Technischen Hochschule Deggendorf. Zuvor arbeitete er als Staatsanwalt an diversen Landgerichten und Richter am Landgericht in einer Zivilkammer.

Neben seiner Tätigkeit als Seniorpartner der auf Wirtschaftsrecht und Governance, Risiko- und Compliancemanagement (GRC) spezialisierten Kanzlei Prof. Dr. Scherer, Partnerschaft mbB, erstellt er wissenschaftliche Rechtsgutachten und agiert als Richter in Schiedsgerichtsverfahren.

Seit 2001 arbeitet er auch als Insolvenzverwalter in verschiedenen Amtsgerichtsbezirken.

Prof. Dr. Scherer fungiert in diversen Unternehmen / Körperschaften als Compliance-Ombudsmann sowie externer Compliance-Beauftragter / Qualitätsmanagement-Beauftragter und ist gesuchter Referent bei Managementschulungen in namhaften Unternehmen sowie im Weiterbildungsprogramm des Senders BR-alpha und der virtuellen Hochschule Bayern (VHB).

In Kooperation mit TÜV konzipierte er als Studiengangsleiter und Referent den seit 12 Jahren renommierten und akkreditierten berufsbegleitenden Masterstudiengang Risikomanagement und Compliancemanagement an der Technischen Hochschule Deggendorf und ist als externer Gutachter bei der (System-)Akkreditierung von Weiterbildungsstudiengängen tätig.

Seit 2012 leitet er als Vorstand des Direktoriums das Internationale Institut für Governance, Management, Risk- und Compliancemanagement der Technischen Hochschule Deggendorf als Kompetenzzentrum.

Außerdem ist er seit 2015 Mitglied des Beirates des Instituts für Risikomanagement und Regulierung (FIRM), Frankfurt (www.firm.fm).

Ebenso seit 2016 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 whistle blowing).

Ebenso seit 2016: Fachlicher Leiter der User Group *„Nachhaltige Unternehmensführung und Compliance“* der Energieforen Leipzig und seit 2018 Mitglied der Arbeitsgruppe 252.07 von Austrian Standards International zur Erarbeitung einer ÖNORM 4900 ff. (Risiko-Managementsystem-Standards).

Seine Forschungs- und Tätigkeitsschwerpunkte liegen auf den Gebieten Nachhaltigkeit (ESG/CSR), Managerenthaftung, Governance-, Risiko- und Compliancemanagement, 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.