die KI in den USA entwickeln oder nutzen, bedeutet das: Ein bundesweit einheitlicher US-Rahmen mag Compliance vereinfachen, doch gleichzeitig könnten Konflikte mit dem EU-Rechtsrahmen (KI-VO) und insgesamt die Rechtsunsicherheit in den USA zunehmen. Die Strategien und Methoden der KI-Regulierung in den USA und der EU laufen weiter auseinander und nicht aufeinander zu.

Dr. Axel Spies
ist Rechtsanwalt und Partner bei Potomac Law in Washington DC sowie Mitherausgeber der MMR und ZD.

Beiträge

Thomas Hoeren/Stefan Pinelli

KI-Compliance im Unternehmen

Anforderungen, Strukturen und Herausforderungen unter der KI-VO

Die KI-VO der Europäischen Union etabliert erstmals einen umfassenden, horizontalen Rechtsrahmen für den Einsatz künstlicher Intelligenz und stellt Unternehmen vor erhebliche neue Compliance-Anforderungen. Der Beitrag analysiert die rechtlichen Grundlagen und praktischen Herausforderungen einer unternehmensinternen KI-Compliance mit besonderem Fokus auf den Einsatz von KI-Agenten. Im Zentrum steht die Frage, wie die Vorgaben der KI-VO systematisch in bestehende Compliance- und Governance-Strukturen integriert werden können. Auf dogmatischer Grundlage wird gezeigt, dass KI-Systeme zwar keine eigenständigen Rechtssubjekte sind, ihr zunehmender Autonomiegrad jedoch gesteigerte Organisations-, Kontroll- und Überwachungspflichten auslöst. Der Beitrag versteht sich als Brücke zwischen europäischem Regulierungsrecht und Unternehmenspraxis und entwickelt Leitlinien für eine rechtssichere und zugleich innovationsfreundliche KI-Compliance.

I. Einleitung

Die Regulierung künstlicher Intelligenz (KI) steht mit der KI-VO der Europäischen Union[1] an einem Wendepunkt. Erstmals wurde ein umfassender, horizontaler Rechtsrahmen geschaffen, der sich nicht nur auf einzelne Sektoren oder spezifische Risiken beschränkt[2], sondern die Entwicklung, Bereitstellung und Nutzung von KI in ihrer gesamten Breite adressiert. Damit geht die KI-VO über bestehende Regulierungsinstrumente wie zB die DS-GVO[3] oder das Produktsicherheitsrecht hinaus und markiert einen Paradigmenwechsel im europäischen Regulierungsmodell: KI wird nicht länger als bloßes technisches Werkzeug verstanden, sondern als sozio-technisches System, das spezifische Governance- und Compliance-Strukturen erfordert. Dieser Perspektivenwechsel wirft grundlegende Fragen nach der normativen Steuerungsfähigkeit des Rechts im Angesicht autonomer, selbstlernender Systeme auf.

Parallel dazu zeigt sich in der Unternehmenspraxis, dass KI-Agenten eine immer bedeutendere Rolle einnehmen.[4] Sie agieren zunehmend – gerade in Cloud-geprägten Infrastrukturen – als Akteure in Entscheidungsprozessen, sei es bei der automatisierten Vertragsgestaltung[5], in der Risikoanalyse oder bei internen Verwaltungs- und Steuerungsaufgaben. Diese Entwicklung verschärft die Diskussion um die dogmatische Einordnung solcher Systeme: Sind sie lediglich komplexe Werkzeuge, deren Handlungen dem menschlichen Nutzer zurechenbar bleiben, oder begründen sie eine neue Form rechtlich relevanter Autonomie? Daraus resultieren weitreichende Implikationen für Fragen der Haftung, der Verantwortungszuschreibung und der dogmatischen Ver-

1 VO (EU) 2024/1689 des Europäischen Parlaments und des Rates v. 13.6.2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz).

2 So etwa der seinerzeitige Entwurf einer KI-Haftungsrichtlinie, Vorschlag für eine RL des europäischen Parlaments und des Rates v. 28.9.2022 zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstliche Intelligenz (RL über KI-Haftung), COM(2022) 496 final.

3 VO (EU) 2016/679 des Europäischen Parlaments und des Rates v. 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

4 Vgl. dazu Legner KIR 2025, 183 (183).

5 Wolffskeel MMR 2024, 921 (923 f.).

ortung von „human in the loop"-Erfordernissen. Vor diesem Hintergrund verfolgt der vorliegende Beitrag die Zielsetzung, die rechtlichen Rahmenbedingungen und praktischen Herausforderungen einer unternehmensinternen KI-Compliance systematisch zu analysieren. Dabei wird untersucht, inwieweit die KI-VO als neuer Ordnungsrahmen in bestehende Compliance-Strukturen integriert werden kann, welche spezifischen Anforderungen sich aus dem Einsatz von KI-Agenten ergeben und welche offenen Forschungsfragen für Wissenschaft und Praxis bestehen. Der Beitrag versteht sich damit zugleich als dogmatische Bestandsaufnahme und als Impuls für die Weiterentwicklung eines kohärenten Rechtsrahmens, der technologische Innovation ermöglicht, ohne rechtsstaatliche Grundprinzipien wie Transparenz, Verantwortlichkeit und Rechtssicherheit preiszugeben.

II. Rechtsrahmen für KI-Compliance

Der Rechtsrahmen für KI-Compliance entwickelt sich dynamisch auf verschiedenen Ebenen. Auf europäischer Ebene steht die KI-VO im Zentrum, die ein System von Risikoklassen vorsieht und daraus abgestufte Pflichten für Anbieter, Nutzer sowie für GPAI-Modelle (General Purpose AI – GPAI)[6] ableitet. Dabei ergeben sich vielfältige Bezüge zu weiteren Digitalrechtsakten der EU wie dem Digital Services Act (DSA)[7], dem Digital Markets Act (DMA)[8], dem Data Act (DA)[9], dem Data Governance Act (DGA)[10], dem Cyber Resilience Act (CRA)[11] sowie der NIS2-Richtlinie[12], die jeweils ergänzende Anforderungen an Sicherheit, Datenzugang und Plattformverantwortung regeln. Auf nationaler Ebene eröffnen sich mehr oder minder Spielräume für die Umsetzung der europäischen Vorgaben, etwa in Deutschland oder anderen Mitgliedstaaten, wobei die konkrete Ausgestaltung je nach Rechtskultur variieren kann. Gleichzeitig treten Überschneidungen mit bereits bestehenden Vorschriften auf, etwa mit der DS-GVO, dem Produkthaftungsrecht oder allgemeinen zivilrechtlichen Regelungen. Diese Mehrfachverbindungen stellen Unternehmen vor die Herausforderung, Compliance-Strategien kohärent zu entwickeln und Doppelregulierungen zu vermeiden.

Über die EU hinaus ist auch die internationale Perspektive entscheidend. In den USA existiert bislang kein umfassender Rechtsrahmen, sondern es gibt bislang lediglich sektorale Ansätze und regulatorische Initiativen einzelner Bundesstaaten.[13] China verfolgt einen stärker zentralistisch geprägten Ansatz mit spezifischen Regeln zur Algorithmus-Aufsicht und KI-Sicherheit.[14] Das Vereinigte Königreich wiederum hat mit dem AI White Paper[15] einen risikobasierten, flexiblen Regulierungsansatz vorgestellt, der stärker auf bestehende Institutionen aufbaut. Ergänzend spielen Gesetzgebungsprozesse wie die Data Protection and Digital Information Bill[16] eine Rolle. Damit entsteht ein global fragmentiertes Regelungsumfeld, in dem sich Unternehmen je nach Branche auf unterschiedliche Compliance-Anforderungen einstellen müssen.

III. Unternehmensinterne KI-Compliance-Strukturen

Unternehmensinterne KI-Compliance-Strukturen müssen so ausgestaltet sein, dass sie sowohl regulatorische Anforderungen als auch unternehmensspezifische Risiken abdecken. Zentrale Voraussetzung ist eine klare Compliance-Organisation mit eindeutig zugewiesenen Verantwortlichkeiten. Auf oberster Ebene trägt die Unternehmensleitung die strategische Verantwortung für den rechtskonformen und ethischen Einsatz von KI. Häufig wird die Umsetzung über den Chief Compliance Officer (CCO) gesteuert, mitunter ergänzt um spezialisierte Funktionen wie einen AI-Compliance Officer (AI-CO), der als Schnittstelle zwischen Technik, Recht und Geschäftsbereichen fungiert.

Ein wesentliches Element bilden systematische Risk Assessments, mit denen die Risiken KI-basierter Systeme identifiziert, bewertet und priorisiert werden. Auf dieser Grundlage lassen sich Governance-Strukturen entwickeln, die Kontrollmechanismen, Eskalationswege und unabhängige Prüfungen vorsehen. Entscheidend ist dabei, dass Risikoanalysen nicht nur einmalig, sondern fortlaufend erfolgen, um mit der Dynamik technischer Entwicklungen Schritt zu halten.

Hinzu kommen umfangreiche Dokumentations- und Transparenzpflichten.[17] Dazu gehört ein technisches Dokumentationsregime, das die Funktionsweise, Trainingsdaten, Modelle und Ergebnisse nachvollziehbar beschreibt. Sog. Audit Trails dienen als Beleg für den Entwicklungs- und Einsatzprozess von KI-Systemen und ermöglichen sowohl interne Überprüfungen als auch externe Kontrollen.

Schließlich spielen Zertifizierung, Konformitätsbewertung und interne Kontrollsysteme eine zentrale Rolle. Unternehmen müssen sicherstellen, dass ihre KI-Anwendungen den regulatorischen Anforderungen entsprechen, zB durch inter-

6 Damit gemeint sind KI-Modelle mit allgemeinem Verwendungszweck gem. Art. 3 Nr. 63 KI VO.

7 VO (EU) 2022/2065 des Europäischen Parlaments und des Rates v. 19.10.2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG.

8 VO (EU) 2022/1925 des Europäischen Parlaments und des Rates v. 14.9.2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828.

9 VO (EU) 2023/2854 des Europäischen Parlaments und des Rates v. 13.12.2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828.

10 VO (EU) 2022/868 des Europäischen Parlaments und des Rates v. 30.5.2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724.

11 VO (EU) 2024/2847 des Europäischen Parlaments und des Rates v. 23.10.2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828.

12 RL (EU) 2022/2555 des Europäischen Parlaments und des Rates v. 14.12.2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148; Gesetz zur Umsetzung der NIS2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, BGBl. 2025 I Nr. 301.

13 Beispiele dazu s. bei Determann NVwZ 2016, 561 (564).

14 S. Wu, How to Interpret China's First Effort to Regulate Generative AI Measures, China Briefing v. 27.7.2023, abrufbar unter: https://www.china-briefing.com/news/how-to-interpret-chinas-first-effort-to-regulate-generative-ai-measures/.

15 GOV UK, Policy Paper: A pro-innovation approach to AI regulation, 3.8.2023, abrufbar unter: https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper.

16 UK Parliament, Data Protection and Digital Information Bill, 23.9.2024, abrufbar unter: https://bills.parliament.uk/bills/3430.

17 Insb. aus Art. 11–19, 50 KI-VO.

ne Pre-Checks, externe Zertifizierungen oder die Integration von Standards in bestehende Qualitätsmanagementsysteme. Diese Maßnahmen erhöhen nicht nur die Rechtssicherheit, sondern stärken auch das Vertrauen von Kunden, Geschäftspartnern und Aufsichtsbehörden in den verantwortungsvollen Umgang mit KI.

IV. Besondere Herausforderungen beim Einsatz von KI-Agenten

Der Einsatz von KI-Agenten wirft eine Reihe besonderer rechtlicher und praktischer Fragen auf. Zunächst stellt sich die Herausforderung der Definition und Abgrenzung: Unter einem KI-Agenten versteht man idR ein System, das nicht nur auf Eingaben reagiert, sondern Daten analysiert, Entscheidungen trifft und Handlungen im digitalen oder physischen Raum ausführt.[18] Damit unterscheidet er sich von KI-Anwendungen, die stärker deterministisch und eng an vorgegebene Aufgaben gebunden sind.[19]

Die zunehmende Integration von KI in betriebliche Strukturen kann in nächster Zeit denkbar dazu führen, dass Führungskräfte selbst künftig hybride Teams leiten, die sich aus Mitarbeitern und KI-Agenten zusammensetzen. Während KI-Agenten nach geltendem Recht als technische Werkzeuge gelten und damit keine eigenständigen Rechtssubjekte sind,[20] verschiebt sich die praktische Verantwortung für Compliance und Ergebnisqualität in diesen Konstellationen dennoch in komplexer Weise. Die juristische Verantwortung verbleibt grundsätzlich bei den handelnden natürlichen Personen sowie bei der Organisation, die KI-Systeme bereitstellt und deren Einsatz regelt (vgl. den sachlichen Anwendungsbereich Art. 3 Nr. 3–4 KI-VO). Hieraus erwächst insbesondere die Pflicht zur Implementierung wirksamer Kontroll- und Überwachungsmechanismen,[21] um etwaige Rechtsverstöße durch fehlerhafte Eingaben oder Outputs zu vermeiden. Dies gilt in besonderem Maße, wenn Mitarbeiter eigene Daten in unternehmensseitig bereitgestellte KI-Agenten einspeisen und dadurch etwaig rechtswidrige Ergebnisse erzeugen. In solchen Fällen trifft den Mitarbeiter – im Verhältnis zum Arbeitgeber nach den Grundsätzen der Arbeitnehmerhaftung[22] – eine individuelle Verantwortung, während das Unternehmen ein Organisationsverschulden trifft,[23] sofern keine angemessenen Richtlinien, Prüfmechanismen und Nachvollziehbarkeitssysteme implementiert wurden.

Die Frage, ob KI-Agenten künftig auch als Whistleblower fungieren könnten, stellt eine weitere relevante Facette dieser Diskussion dar. Nach derzeitigem Rechtsstand schützt das Hinweisgeberschutzgesetz (HinSchG) ausschließlich natürliche Personen, die in einem beruflichen Kontext Verstöße melden.[24] Ein KI-Agent könnte zwar Unregelmäßigkeiten automatisiert erkennen und melden, wäre damit jedoch nicht selbst Whistleblower im rechtlichen Sinne, sondern lediglich ein technisches Instrument, das Hinweise generiert. Die Schutzmechanismen des Whistleblower-Rechts – insbesondere das Verbot von Repressalien – greifen somit nicht.[25] Gleichwohl ist denkbar, dass sich in der wissenschaftlichen und rechtspolitischen Diskussion die Frage stellt, ob KI-Systemen zumindest eingeschränkte rechtliche Rollen zugewiesen werden könnten, ähnlich der Konstruktion juristischer Personen.[26]

Für die Unternehmenspraxis folgt hieraus, dass Compliance-Governance-Frameworks erweitert und für KI präzisiert werden müssen, wo noch nicht entsprechend eingerichtet. Führungskräfte sind nicht nur technisch, sondern vor allem im Hinblick auf Risikoabschätzung, Kontrollmechanismen und Rechenschaftspflichten zu schulen. Darüber hinaus wird eine klare Dokumentation der Verantwortlichkeiten im Zusammenspiel von Mensch und KI erforderlich sein, um sowohl haftungsrechtliche Risiken zu minimieren als auch regulatorische Vorgaben aus der KI-VO einzuhalten.[27] Langfristig wird sich die Frage stellen, ob KI-Agenten in eine eigene rechtliche oder quasi-rechtliche Stellung hineinwachsen können. Kurz- bis mittelfristig bleibt jedoch die Verantwortung eindeutig bei den Mitarbeitern und Unternehmen verortet, während KI-Systeme lediglich als technische Werkzeuge und unterstützende Instrumente zu betrachten sind.

Ein zentrales Thema ist der Autonomiegrad solcher Systeme und die damit verbundene Verantwortungszuschreibung.[28] Je selbstständiger ein KI-Agent agiert, desto schwieriger wird es, klare Haftungsstrukturen zu etablieren. Die KI-VO ergänzt bestehende und bevorstehende Regelungen, indem sie bei Hochrisiko-KI-Systemen wie autonomen Systemen spezifische Pflichten zur Risikobewertung, Dokumentation und menschlichen Aufsicht vorsieht.[29] Damit stellt sich die zentrale Frage, in welchem Umfang ein „human in the loop"[30] rechtlich zwingend verankert werden muss, um Verantwortungsdiffusion und Haftungslücken zu vermeiden.

Hinzu treten spezifische Risiken: KI-Agenten können aufgrund von Verzerrungen in den Trainingsdaten Bias (unter einem Bias wird eine „verzerrende Darstellung objektiver Werte"[31] verstanden) reproduzieren und diskriminierende

18 Thurow BC 2025, 342; Bähr/Vorbau ArbRAktuell 2025, 202; IBM, Was sind AI Agents?, abrufbar unter: https://www.ibm.com/de-de/think/topics/ai-agents.
19 Vgl. die Legaldefinition zu KI-System in Art. 3 Nr. 1 KI-VO.
20 Hoeren/Sieber/Holznagel, HdB Multimedia-Recht/Willecke, 62. EL Juni 2024, Teil 29.3 Rn. 15.
21 Art. 4 KI-VO, dazu Hoeren/Pinelli, Datenrecht, 2025, S. 307.
22 MHdB ArbR/Reichold, 6. Aufl. 2024, § 93 Rn. 24 ff.; MüKoBGB/Henssler, 9. Aufl. 2023, BGB § 619a Rn. 1 ff.
23 MHdB ArbR/Reichold, 6. Aufl. 2024, § 93 Rn. 20, 21; Jauernig/Kern, 19. Aufl. 2023, BGB § 823 Rn. 32.
24 § 1 Abs. 1 HinSchG; zum Schutz natürlicher Personen durch das HinSchG s. EU Artificial Intelligence Act, Whistleblowing und das EU AI Gesetz, 11.8. 2025, abrufbar unter: https://artificialintelligenceact.eu/de/whistleblowing-and-the-eu-ai-act/.
25 Vgl. § 36 Abs. 1 HinSchG.
26 Juristische Personen als solche können nach § 1 Abs. 1 HinSchG keine hinweisgebenden Personen sein und dadurch durch das HinSchG geschützt werden; Jedoch werden diese nach § 1 Abs. 2 HinSchG dennoch geschützt, soweit sie Gegenstand einer Meldung sind, s. dazu BeckOGK/Kämmerer/Redder, 1.10.2022, HinSchG § 1 Rn. 78.
27 ZB durch die technische Dokumentation vor dem Inverkehrbringen oder der Inbetriebnahme eines Hochrisiko-KI-Systems nach Art. 11 KI-VO.
28 Vgl. Erwägungsgrund 12 KI-VO.
29 S. zu den Anforderungen an Hochrisiko KI-Systeme Art. 8 ff. KI-VO.
30 Das „human-in-the-loop" Erfordernis meint das Erfordernis und die Möglichkeit menschlichen Eingreifens, vgl. AI HLEG, Ethics Guidelines for Trustworthy AI, 8.4.2019, S. 16, abrufbar unter: https://www.europarl.europa.eu/cmsdata/196377/AI%20HLEG_Ethics%20Guidelines%20for%20Trustworthy%20AI.pdf.
31 Sachs/Meder ZD 2024, 363 (367); Lauscher/Legner ZfDR 2022, 367 (371).

Entscheidungen verstärken.[32] Intransparenz entsteht, weil die Entscheidungslogik neuronaler Netze heute noch zum Teil schwer nachvollziehbar bleibt.[33] Gerade im Kontext autonomer Systeme kann dies gravierende Folgen haben, wenn fehlerhaft interpretiert wird. Solche „Halluzinationen" gefährden nicht nur die Sicherheit, sondern werfen auch Fragen der Beweislast und Nachvollziehbarkeit im Haftungsrecht auf. Die DS-GVO spielt zudem insoweit eine Rolle, wenn personenbezogene Daten verarbeitet werden, wodurch Transparenz- und Informationspflichten relevant werden.[34] Zur Risikominimierung sind technische und organisatorische Maßnahmen erforderlich. Diese ergeben sich nicht nur aus allgemeinen Sorgfaltspflichten, sondern künftig auch aus den Vorgaben der KI-VO. Nach Art. 26 Abs. 1 KI-VO sind Anbieter und Betreiber verpflichtet, geeignete technische und organisatorische Maßnahmen umzusetzen, um die Konformität des KI-Systems mit den Anforderungen der Verordnung sicherzustellen. Technische Maßnahmen umfassen dabei Vorkehrungen, die auf die Robustheit und Sicherheit des Systems abzielen, insbesondere gem. Art. 15 Abs. 4 KI-VO durch technische Redundanzen, Störungs- und Sicherheitspläne oder Umschaltmechanismen auf regelbasierte Verfahren bzw. menschliche Kontrolle. Organisatorische Maßnahmen betreffen hingegen die Gestaltung der betrieblichen Abläufe, etwa durch Protokollierungs- und Überwachungspflichten, das Vier-Augen-Prinzip oder den Aufbau wirksamer Compliance-Strukturen.[35] Die Erfüllung dieser Pflichten wirkt haftungsrechtlich entlastend, da diese iRd sicherheitsrelevanten Pflichten als Sorgfaltsmaßstab herangezogen werden können.

Schließlich müssen Kontroll- und Interventionsmöglichkeiten gewährleistet sein. Mechanismen wie ein „Kill Switch" oder vergleichbare Notfallfunktionen sind nicht nur technische Best Practices, sondern können auch rechtlich geboten sein, um die Anforderungen an menschliche Aufsicht iSd KI-VO sowie die allgemeinen Verkehrssicherungspflichten zu erfüllen.[36] Ebenso ist die Auditierbarkeit von zentraler Bedeutung: Nur wenn Systementscheidungen und Systemreaktionen nachvollziehbar dokumentiert sind, lassen sich Beweislastfragen in zivilrechtlichen Verfahren verbindlich klären.

Insgesamt zeigt sich, dass der Einsatz von KI-Agenten einen komplexen Mehrebenen-Rahmen erfordert, der europäische Vorgaben, nationale Sonderregelungen und internationale Standards integriert. Ohne eine klare Verzahnung dieser Regelungsstränge droht ein fragmentierter Rechtsrahmen, der die Rechtssicherheit insbesondere für Hersteller, Anbieter, Betreiber und Nutzer erheblich beeinträchtigen würde.

V. KI-Compliance als Teil der Gesamt-Compliance

KI-Compliance darf nicht isoliert betrachtet werden, sondern muss in bestehende Unternehmens-Compliance-Systeme integriert werden. Viele der grundlegenden Mechanismen sind aus anderen Regulierungsbereichen bekannt, etwa aus dem Kartellrecht (Art. 101–102 AEUV), dem Datenschutzrecht (insbesondere der DS-GVO), der Exportkontrolle (Dual-Use-Verordnung (EU) 2021/821) oder im Bereich Anti-Fraud (zB Art. 325 AEUV sowie nationale Korruptions- und Betrugsstrafnormen). So wie Unternehmen dort Risikobewertungen, Kontrollmechanismen und interne Berichtslinien etabliert haben, müssen vergleichbare Strukturen auch für den Einsatz von KI-Systemen geschaffen werden. Die Einbettung von KI-Compliance in bestehende Systeme vermeidet Redundanzen und ermöglicht Synergien, etwa durch zentrale Schulungsprogramme.

Ein zentrales Feld der Schnittstellenarbeit betrifft die IT- und Informationssicherheit. Die KI-VO verweist in vielen Punkten ausdrücklich auf flankierende Rechtsakte wie die NIS2-RL, die Vorgaben zur Cybersicherheit kritischer Infrastrukturen macht,[37] sowie den Cyber Resilience Act (vollständig in Kraft ab September 2027), der spezifische Anforderungen an die Produktsicherheit vernetzter Systeme vorsieht.[38] Ergänzend spielt auf nationaler Ebene das IT-Sicherheitsgesetz 2.0[39] eine wichtige Rolle, das Pflichten für Betreiber kritischer Infrastrukturen und digitale Dienste normiert. Unternehmen sind damit verpflichtet, nicht nur regulatorische Mindeststandards einzuhalten, sondern auch organisatorische Maßnahmen zu etablieren, die den sicheren Betrieb von KI-Systemen gewährleisten.[40] Die Anknüpfung an Informationssicherheitsmanagementsysteme nach ISO/IEC 27001 oder branchenspezifische Sicherheitsstandards (B3S) stellt eine praktikable Umsetzungsmöglichkeit dar.

Darüber hinaus gewinnt das Verhältnis von KI-Compliance zu ESG- und CSR-Reporting erheblich an Bedeutung. Der Einsatz von KI wirkt unmittelbar auf Nachhaltigkeit, Diversität und soziale Verantwortung.[41]

VI. Praxisorientierte Handlungsempfehlungen

Der Aufbau eines KI-Compliance-Frameworks erfordert einen systematischen Ansatz, der sowohl regulatorische Anforderungen als auch unternehmensspezifische Risiken berücksichtigt. Best Practices orientieren sich auch an etablierten Compliance-Strukturen, müssen jedoch um KI-spezifische Elemente ergänzt werden. Ausgangspunkt ist die Entwicklung eines kohärenten Rahmens, der auf einer Risikoanalyse basiert und klare Verantwortlichkeiten sowie Kontrollmechanismen vorsieht. Dabei sollte das Framework an internationale Standards angelehnt sein, um die Anschlussfähigkeit an unterschiedliche Märkte und Aufsichtsregime zu gewährleisten.

32 Lauscher/Legner ZfDR 2022, 367 (371).
33 S. dazu Chibanguza/Kuß/Steege, Künstliche Intelligenz/Dieckmann, 2. Aufl. 2025, Teil 2 § 5 Rn. 17 f.
34 S. Art. 12–14 DS-GVO.
35 Beck OK KI-Recht/Denga, 4. Ed. 1.11.2025, KI-VO Art. 26 Rn. 23-27.
36 Zum „Kill Switch" s. BeckOK KI-Recht/Spittka, 4. Ed. 1.11.2025, KI-VO Art. 20 Rn. 10.
37 Hoeren/Pinelli, Datenrecht, 2025, S. 239 ff.
38 Hoeren/Pinelli, Datenrecht, 2025, S. 249 ff.
39 Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, BGBl. 2021 I, S. 1122.
40 Hornung/Schallbruch, IT-Sicherheitsrecht/Fischer, 2. Aufl. 2024, Teil 2 § 13 Rn. 40.
41 Vgl. Moosmayer/Lösler, Corporate Compliance/Thoms, 4. Aufl. 2024, § 17. Rn. 6 ff.

Ein zentrales Element ist die Implementierung von Policies und internen Richtlinien. Diese dienen der Übersetzung der KI-VO in konkrete Handlungsanweisungen für die Unternehmenspraxis. Dazu gehören Vorgaben für den Entwicklungsprozess, die Nutzung von Trainingsdaten, die Dokumentation von Modellen sowie Verfahren für den Umgang mit Vorfällen. Solche Richtlinien sollten verbindlich sein und regelmäßig überprüft sowie an technologische und regulatorische Entwicklungen angepasst werden.

Ergänzend ist die Schulung und Sensibilisierung von Mitarbeitern entscheidend. Da KI-Systeme in zahlreichen Unternehmensbereichen eingesetzt werden, müssen nicht nur Entwickler und Compliance-Beauftragte, sondern auch Fachabteilungen wie Einkauf, Vertrieb oder Personalwesen ein Grundverständnis für die Risiken und Pflichten im Umgang mit KI entwickeln. Schulungsprogramme, E-Learning-Module und praxisnahe Fallstudien tragen dazu bei, ein „KI-Compliance-Mindset" im gesamten Unternehmen zu verankern.

Darüber hinaus gewinnen technische Standards und Zertifizierungen an Bedeutung. Internationale Normen wie ISO/IEC 22989 (Begriffe und Konzepte für KI), ISO/IEC 23894 (Risikomanagement für KI) oder die Arbeiten der europäischen Standardisierungsorganisationen CEN und CENELEC schaffen Referenzpunkte für die praktische Umsetzung regulatorischer Anforderungen. Zertifizierungen können nicht nur die Rechtssicherheit erhöhen, sondern auch iRv Konformitätsbewertungen nach der KI-VO erforderlich sein. Die Orientierung an solchen Standards ermöglicht es Unternehmen, Compliance nachweisbar und überprüfbar zu gestalten und zugleich das Vertrauen von Aufsichtsbehörden, Geschäftspartnern und Kunden zu stärken.

VII. Ausblick

Die zukünftige Rechtsentwicklung im Bereich der KI wird maßgeblich durch den europäischen Gesetzgeber geprägt werden. Nach dem Inkrafttreten der KI-VO ist mit einer Vielzahl delegierter Rechtsakte und technischer Standards zu rechnen, die den Rahmen konkretisieren, etwa zur Klassifizierung von Hochrisiko-Systemen oder zur technischen Dokumentation. Ebenso werden Durchsetzungsmechanismen eine zentrale Rolle spielen: Neben den nationalen Marktüberwachungsbehörden sind auch neue Koordinationsstellen auf EU-Ebene vorgesehen, die für die einheitliche Anwendung sorgen sollen. Damit stellt sich die Frage, wie sehr Aufsichtsbehörden tatsächlich in der Lage sein werden, komplexe KI-Systeme effektiv zu prüfen und Sanktionen durchzusetzen.

Parallel dazu entwickeln sich die technischen Möglichkeiten rasant weiter. Insbesondere generative KI und der Einsatz sog. Multi-Agent Systems, in denen mehrere KI-Agenten interagieren und kooperieren, verschärfen die Herausforderungen für Regulierung und Compliance. Diese Systeme erhöhen den Grad an Autonomie und Komplexität und werfen damit neue Fragen zu Haftung, Kontrollmechanismen und Verantwortungszuschreibung auf. Auch die Grenze zwischen Hochrisiko-KI und allgemeinen Anwendungen dürfte in der Praxis zunehmend verschwimmen, sodass eine flexible Anpassung regulatorischer Kategorien erforderlich erscheint.

Schließlich bleiben zahlreiche offene Fragen für Wissenschaft und Praxis. Dazu gehört etwa, wie sich klassische zivilrechtliche Konzepte wie Verschulden und Kausalität auf selbstlernende Systeme übertragen lassen, ob bestehende Haftungsinstrumente ausreichen oder neue Modelle – wie eine spezifische „KI-Haftung" – geschaffen werden müssen. Unklar ist auch, wie sich Datenschutz- und Transparenzanforderungen mit technischen Notwendigkeiten des maschinellen Lernens vereinbaren lassen. Für die Praxis stellt sich die Herausforderung, KI-Compliance in ein bereits komplexes Geflecht aus diversen Regulierungen zu integrieren, ohne die Innovationsfähigkeit zu hemmen. Damit bleibt der Rechtsrahmen für KI ein dynamisches Feld, das in enger Wechselwirkung zwischen Technikentwicklung, Regulierung und unternehmerischer Umsetzung steht.

Schnell gelesen...

- Die KI-VO schafft erstmals verbindliche, risikobasierte Pflichten für den Einsatz von KI in Unternehmen.
- Der Einsatz von KI-Agenten erhöht die Komplexität von Verantwortungs- und Haftungsstrukturen und macht klar definierte Kontroll- und Interventionsmeschanismen notwendig.
- KI wird nicht länger als bloßes technisches Werkzeug verstanden, sondern als sozio-technisches System, das spezifische Governance und Compliance-Strukturen erfordert.
- Wirksame KI-Compliance erfordert fortlaufende Risikoanalysen, Dokumentation und menschliche Aufsicht.
- KI-Compliance ist essenziell und integraler Bestandteil einer Compliance-Kultur in Unternehmen.

Prof. Dr. Thomas Hoeren
ist Leiter des Instituts für Informations-, Telekommunikations- und Medienrecht (ITM) an der Universität Münster.

Stefan Pinelli
ist Rechtsanwalt und Leiter des Bereichs Recht Digital im Konzernwesen der Volkswagen AG in Wolfsburg.