Smart Structures for Smart Systems: Die Integration der KI-VO in bestehende Compliance-Strukturen

Rechtsanwältin Dr. Carolin Raspé und Rechtsanwalt Dr. Benedikt *

A. Einleitung

Der technologische Wandel durch Künstliche Intelligenz (KI) verändert nicht nur Arbeitsprozesse, sondern auch Strukturen, Verantwortung und Kompetenzen. Unternehmen, die KI einsetzen, profitieren von Effizienzgewinnen, müssen jedoch gleichzeitig neue regulatorische Risiken und Pflichten berücksichtigen.

Die Verordnung (EU) 2024/1689 vom 13.6.2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (KI-VO) schafft einen neuen Compliance-Risikobereich und stellt Unternehmen vor eine Vielzahl rechtlicher Herausforderungen. Hierbei muss das Rad jedoch nicht neu erfunden werden: Betroffene Unternehmen können sich auf bereits bestehende Compliance-Systeme stützen, wie eine Betrachtung der Compliance-Pflichten der KI-VO aus der Perspektive des Prüfungsstandards IDW PS 980 zeigt.

Dieser Aufsatz richtet sich an Betreiber[1] von KI-Systemen und soll ihnen helfen, die rechtlichen Anforderungen der KI-VO erfolgreich in ihrem Unternehmen umzusetzen. Die Betreiberpflichten werden im Folgenden systematisch dargestellt, mit bestehenden Compliance-Grundelementen verknüpft und praxisorientierte Ansätze zur Implementierung aufgezeigt.

Am 19.11.2025 hat die Europäische Kommission das sog. Digital Omnibus-Paket vorgestellt, durch das unterschiedliche Rechtsakte – wie auch die KI-VO – in Teilen vereinfacht, gebündelt und angepasst werden sollen. Die Rechtslage befindet sich also in einem dynamischen Prozess; Entwicklungen sollten fortlaufend beobachtet werden.

B. Anwendbarkeit der KI-VO

Zunächst sollten Unternehmen feststellen, ob sie als Adressaten in den Anwendungsbereich der KI-VO fallen und welche Pflichten im Einzelnen daraus für sie resultieren. Dies kann in vier Schritten[2] geprüft werden:

I. Prüfungsschritt 1: Handelt es sich um ein KI-System?

Die erste Frage lautet: Handelt es sich bei den entwickelten oder genutzten KI-Anwendungen überhaupt um ein KI-System im Sinne der KI-VO? Dies wird anhand von sieben Kriterien (basierend auf der 2023 aktualisierten OECD-Definition) geprüft: Ein KI-System ist nach Art. 3 Nr. 1 KI-VO ein maschinengestütztes System (1), das für einen unterschiedlich autonomen Betrieb konzipiert ist (2), nach seiner Inbetriebnahme anpassungsfähig sein kann (3) und für explizite oder implizite Ziele (4) aus den erhaltenen Eingaben ableitet (5), wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden (6). Die Ausgaben können dabei physische oder virtuelle Umgebungen beeinflussen (7).[3]

Zentrales Merkmal von KI-Systemen ist ihre Fähigkeit zur Ableitung (ErwG 12 KI-VO). Sie müssen aus erhaltenen Eingaben durch Lern-, Schlussfolgerungs- oder Modellierungsprozesse auf Ergebnisse schließen können. Damit grenzt sich KI klar von der einfachen Datenverarbeitung – wie sie bei herkömmlichen Softwaresystemen und Programmierungsansätzen erfolgt – ab, die strikt regelbasiert erfolgt.[4]

Häufige Unsicherheiten ergeben sich bei der Bestimmung des Grades der Autonomie („in unterschiedlichem Grade autonom“, gem. Art. 3 Nr. 1 KI-VO). Nach ErwG 12 KI-VO agiert ein KI-System autonom, wenn es in einem bestimmten Maß unabhängig von menschlichen Eingriffen arbeitet. Menschliche Unabhängigkeit meint damit nicht vollständige Autonomie; vielmehr ist Autonomie als Spektrum zu verstehen. Sie liegt vor, sobald die Ableitung von Ergebnissen zumindest in geringem Umfang unabhängig von vorprogrammierten Regeln erfolgt.[5]

Zuletzt sind bestimmte KI-Systeme nach Art. 2 KI-VO von dem Anwendungsbereich ausgenommen, etwa solche, die ausschließlich zur Verteidigung oder für militärische Zwecke oder solche der nationalen Sicherheit eingesetzt werden, sowie teilweise Systeme mit freien und quelloffenen Lizenzen.

II. Prüfungsschritt 2: In welche Risikoklasse fällt das KI-System?

Die KI-VO folgt im Sinne eines Produktsicherheitsgesetzes einem risikobasierten Ansatz: Die rechtlichen Anforderungen richten sich nach dem individuellen Risiko des jeweiligen KI-Systems (ErwG 26 KI-VO). Um den Umfang der Pflichten und somit auch das Maß der Compliance-Vorgaben zu bestimmten, muss daher zunächst die Risikoklasse des betreffenden KI-Systems ermittelt werden.

Die KI-VO unterscheidet vier Risikokategorien:

- unannehmbares Risiko – grundsätzlich verboten (Art. 5 KI-VO)
- hohes Risiko – strenge, umfangreiche Anforderungen (Art. 6 ff. KI-VO)
- geringes Risiko – spezifische Transparenzpflichten für bestimmte KI-Systeme (vgl. Art. 50 KI-VO)
- minimales Risiko – wenigstens Sicherstellung von KI-Kompetenz (vgl. Art. 4 KI-VO).

Besonders weitreichend sind für Betreiber die Vorgaben hinsichtlich Hochrisiko-KI-Systemen, gem. Art. 6 ff. KI-VO. Grundsätzlich legen Art. 6 Abs. 1 iVm Anhang I KI-VO sowie Art. 6 Abs. 2 iVm Anhang III KI-VO fest, welche Systeme als hochriskant einzustufen sind, wobei in Einzelfällen Ausnahmen möglich sind.

Nach Art. 6 Abs. 1 iVm Anhang I KI-VO gilt ein KI-System als hochriskant, wenn es seiner Zweckbestimmung nach als Sicherheitsbauteil eines in Anhang I aufgeführten Produkts (zB Spielzeug, Maschinen, Aufzüge, Medizinprodukte) verwendet wird oder selbst ein solches Produkt darstellt – und für dieses Produkt nach einschlägigen EU-Produktsicherheitsvorschriften eine Konformitätsbewertung durch Dritte erforderlich ist.[6]

Art. 6 Abs. 2 iVm Anhang III KI-VO definiert Hochrisiko-KI-Systeme zudem für Bereiche, in denen ihre Nutzung potenziell erhebliche Auswirkungen auf Gesundheit, Sicherheit oder Grundrechte natürlicher Personen hat – ebenso wie auf kritische Infrastrukturen oder demokratische Prozesse. Typische Beispiele sind KI-Systeme zur Emotionserkennung, in der Strafverfolgung, zur Kreditwürdigkeitsprüfung, im Bildungsbereich oder im Personalmanagement zur Auswahl, Bewertung und Überwachung von Mitarbeitenden.

Entscheidend für die Bewertung ist stets die Zweckbestimmung des KI-Systems, dh die von dem Anbieter des KI-Systems intendierte Verwendung, wie sich diese aus den bereitgestellten Informationen, Betriebsanleitung oder Werbe- und Verkaufsmaterial ergibt.[7] Maßgeblich ist also nicht die tatsächliche Nutzung oder Eignung des Systems, sondern die von dem Anbieter vorgesehene Verwendung (Art. 3 Nr. 12 KI-VO).[8]

III. Prüfungsschritt 3: Ist mein Unternehmen Betreiber des KI-Systems?

Als „Betreiber“ iSd Art. 3 Nr. 4 KI-VO gilt jede natürliche oder juristische Person, Einrichtung oder sonstige Stelle mit Sitz oder Präsenz in der EU, die ein KI-System in eigener Verantwortung verwendet. Ausgenommen ist die private, nicht berufliche Nutzung.

Damit müssen Unternehmen, die ihren Mitarbeitenden KI-Systeme bereitstellen, prüfen, ob hierdurch nicht schon die Betreibereigenschaft begründet wird. Denn schon die Nutzung von einlizenzierten KI-Softwareprogrammen kann die besonderen Betreiberpflichten der KI-VO auszulösen.[9]

Beispiel: Gewährt ein Unternehmen Mitarbeitenden Zugang zur kostenpflichtigen Version „ChatGPT for Work“, wird es als „Betreiber“ eingestuft, da ChatGPT gezielt für betriebliche Zwecke eingesetzt wird. Bei einer reinen Google-Suche mit KI-generierten Übersichten dürfte dies hingegen anders zu beurteilen sein, da die Zugänglichmachung der Google-Suche nicht zielgerichtet, sondern als Teil des öffentlichen Internets erfolgt.

Die zentralen Betreiberpflichten ergeben sich aus Art. 26 KI-VO und gelten ab dem 2.8.2026 (Art. 113 S. 1 KI-VO). Im Rahmen des Digital Omnibus-Pakets soll diese Umsetzungsfrist für Hochrisiko-KI-Systeme iSd Anhang III KI-VO um 6 Monate sowie für Hochrisiko-KI-Systeme iSd Anhang I KI-VO um 12 Monate verlängert werden.[10] Die Betreiberpflichten umfassen unter anderem:

- Maßnahmen zur typengerechten Nutzung (Art. 26 Abs. 1 KI-VO)
- Einsetzen einer kompetenten, geschulten Aufsichtsperson (Art. 26 Abs. 2 KI-VO)
- Überwachung des Betriebs (Art. 26 Abs. 5 KI-VO)
- Aufbewahrung automatisch erzeugter Protokolle (Art. 26 Abs. 6 KI-VO)
- Informationspflichten (Art. 26 Abs. 7 und Abs. 11 KI-VO).

Darüber hinaus kann für bestimmte Betreiber[11] eine Pflicht zur Durchführung einer Grundrechte-Folgenabschätzung nach Art. 27 KI-VO bestehen.

IV. Prüfungsschritt vier: Gilt mein Unternehmen als Anbieter?

In bestimmten Fällen gilt ein Betreiber nach Art. 25 Abs. 1 KI-VO als Anbieter eines KI-Systems und unterliegt damit den deutlich umfassenderen Anbieterpflichten nach Art. 16 KI-VO. Dies ist der Fall, wenn er:

- das KI-System mit seinem Namen oder seiner Handelsmarke versieht,
- eine wesentliche Veränderung an dem Hochrisiko-KI-System vornimmt oder
- die Zweckbestimmung so ändert, dass ein zuvor nicht als hochriskant eingestuftes KI-System nun als solches iSd Art. 6 KI-VO gilt.

Besonders praxisrelevant ist die Änderung der Zweckbestimmung (Art. 25 Abs. 1 lit. c KI-VO), da hierfür vergleichsweise geringe Anpassungen ausreichen können. Wird bspw. ChatGPT von der HR-Abteilung verwendet, um Bewerbungen in Tabellenform zu sortieren, nach bestimmten Merkmalen zu filtern und Bewerber mittels Scores zu bewerten, gilt das Unternehmen bereits als Anbieter eines Hochrisiko-KI-Systems (vgl. Art. 6 Abs. 2 iVm Anhang III Nr. 4 lit. a KI-VO).[12]

Wenn die KI-VO Anwendung findet und ihre Pflichten greifen, können Rechtsverstöße weitreichende Konsequenzen für Unternehmen haben. Bei einer Nichteinhaltung der Betreiberpflichten aus Art. 26 oder Art. 50 KI-VO drohen Bußgelder von bis zu EUR 15.000.000 oder 3 % des weltweiten Jahresumsatzes (Art. 99 Abs. 4 lit. e und lit. g KI-VO). Im Extremfall kann somit bereits eine unzureichende Überwachung des Betriebs eines Hochrisiko-KI-Systems ausreichen, um entsprechende Sanktionen auszulösen und das nicht nur, wenn das Geschäftsmodell auf der KI-Technologie basiert. Umso wichtiger ist es daher, potenzielle Risikofaktoren frühzeitig zu erkennen und Vorkehrungen zu treffen, welche die Wahrscheinlichkeit von Verstößen gegen Betreiberpflichten wirksam verringern.

C. Organisation von Compliance im Unternehmen

Eine effektive Compliance-Struktur hilft Unternehmen, solche Sanktionsrisiken zu minimieren und sicherzustellen, dass gesetzliche Vorgaben sowie interne Richtlinien eingehalten werden. Ziel ist es nicht nur, Rechtsverstöße zu vermeiden, sondern auch, Risiken frühzeitig zu erkennen, ihnen gezielt

entgegenzuwirken und das Unternehmen so zu schützen.[13] Hierfür sind präzise, gut organisierte Maßnahmen unerlässlich.

Compliance ist nicht nur eine Obliegenheit der Geschäftsführung, sondern Teil ihrer Legalitätspflicht, rechtlich verankert in § 43 Abs. 1 GmbHG und § 93 Abs. 1 S. 1 AktG.[14] Unabhängig von der Unternehmensgröße muss jedes Unternehmen sicherstellen, dass die Rechtmäßigkeit seines Handelns – insbesondere die korrekte Nutzung von KI-Systemen – durch alle Mitglieder des Unternehmens gewährleistet ist.[15]

Compliance-Management-Systeme („CMS“) sind das organisatorische Rückgrat unternehmensweiter Rechtskonformität. Sie bündeln Maßnahmen, Prozesse und Strukturen in einem einheitlichen Konzept, um unternehmensspezifische Ziele zu erreichen und gesetzliche Pflichten zu erfüllen – unabhängig vom Regelungsbereich.[16] Ein universelles Modell gibt es nicht: Die Ausgestaltung eines CMS richtet sich nach dem individuellen Risikoprofil

des Unternehmens, beeinflusst durch Faktoren wie Produktportfolio, Geschäftsmodell, internationale Aktivitäten, Branche oder Unternehmensgröße.[17]

Um das oft abstrakt wirkende Compliance-Management greifbarer zu machen, wurden Standards entwickelt, die als Leitfaden für eine wirksame Implementierung dienen. Für den Bereich der KI ist dies der „International Standard – Artificial Intelligence Management System“ (AIMS) ISO/IEC 42001:2023 (ISO 42001). Er definiert Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines KI-spezifischen CMS. Ziel ist eine verantwortungsvolle Entwicklung und Nutzung von KI,[18] wobei der Standard sowohl relevante organisatorische Aspekte als auch potenzielle Risiken abdeckt und konkrete Umsetzungs- bzw. Implementierungsleitlinien bietet.

Zwar bestehen die Pflichten der KI-VO auch unabhängig von der ISO 42001, doch in vielen Punkten überschneiden sich deren Anforderungen. Die ISO 42001 kann daher – neben allgemeinen Standards – als Leitfaden dienen, um CMS-Strukturen für eine verantwortungsvolle Nutzung von KI zu gestalten. Sie ersetzt jedoch nicht die Prüfung der spezifischen Anforderungen der KI-VO.

Als allgemeiner Standard für die Bewertung der Wirksamkeit von CMS hat sich in Deutschland der Prüfungsstandard IDW PS 980 etabliert und dient als anerkannter Maßstab für die Beurteilung, ob ein CMS angemessen konzipiert, implementiert und wirksam ist. Er definiert sieben Grundelemente: (1) Compliance-Kultur, (2) Compliance-Ziele, (3) Compliance-Risiken, (4) Compliance-Programm, (5) Compliance-Organisation, (6) Compliance-Kommunikation und (7) Compliance-Überwachung und -Verbesserung.[19] Wie im Folgenden gezeigt wird, finden sich diese Grundelemente auch in den Anforderungen der KI-VO wieder, sodass sich die Pflichten dort systematisch einordnen lassen.

D. Implementierung konkreter KI-Pflichten in bestehende Compliance-Management-Systeme

Die geschilderten Betreiberpflichten nach der KI-VO lassen sich den Grundelementen eines CMS nach IDW PS 980 zuordnen und können damit bruchfrei in bestehende Prozesse eingebunden werden. Dies erspart den betroffenen Unternehmen den Aufbau von parallelen CMS und sichert die effiziente Umsetzung der Compliance-Vorgaben.

I. Compliance-Kultur: Verständnis und Bekenntnis im Unternehmen zu verantwortungsvoller KI-Nutzung

Die Grundlage wirksamer Compliance ist eine gelebte Compliance-Kultur als integraler Bestandteil der Unternehmensethik. Sie schafft ein gemeinsames Verständnis für Normen- und Rechtsbewusstsein im Unternehmen.[20] Das Ziel ist eine freiwillige Selbstverpflichtung aller Mitarbeitenden sowie ein Wertekompass, der die eigenständige Erkennung von Compliance-Risiken ermöglicht und regelkonformes Verhalten auch ohne detaillierte Vorgaben unterstützt.[21]

Die Unternehmensführung hat eine zentrale Rolle: Durch Vorbildwirkung („Tone from the top“) kann sie das Verhalten ihrer Mitarbeitenden nachhaltig beeinflussen. Ein klares Bekenntnis zu integrer, werteorientierter und verantwortungsvoller Unternehmenspraxis erhöht die Bereitschaft zur Einhaltung von Regeln erheblich.[22]

Es empfiehlt sich, regelmäßig zu kommunizieren, dass die Verwendung von KI im Unternehmen in geeigneten Bereichen erwünscht und gefördert wird, gleichzeitig aber ein risiko- und verantwortungsbewusster Umgang unerlässlich ist und nicht zuletzt die strikten Vorgaben der KI-VO einzuhalten sind.

Als Orientierung für ethische Leitlinien bietet ErwG 27 KI-VO sieben Grundsätze vertrauenswürdiger KI: (1) menschliches Handeln und Aufsicht, (2) technische Robustheit und Sicherheit, (3) Datenschutz und Datenverwaltung, (4) Transparenz, (5) Vielfalt, (6) Nichtdiskriminierung und Fairness, (7) gesellschaftliches und ökologisches Wohlergehen und (7) Rechenschaftspflicht.

Diese Grundsätze können auf verschiedene Weise in der Unternehmenskultur verankert werden, etwa durch interne Newsletter, regelmäßige Meetings oder schriftliche Fixierung in einem Verhaltenskodex (Code of Conduct).

Praxistipp:

Eine offene Fehler- und Lernkultur unterstützt die verantwortungsvolle KI-Nutzung. Eigene Erfahrungen, etwa mit KI-Halluzinationen oder unerwarteten Ergebnissen, sollten transparent geteilt werden, um die Notwendigkeit menschlicher Aufsicht zu verdeutlichen. Unternehmensinterne Austauschformate wie KI-Schulungen, Prompting Workshops, oder auch eine IT Security Fortbildungen können das Bewusstsein für Risiken und Chancen von KI im Unternehmen schärfen.

II. Compliance-Ziele: Mehrwert von KI-Compliance

Ein weiteres Grundelement eines wirksamen CMS ist die Festlegung klarer Compliance-Ziele durch die Unternehmensführung, die durch das CMS erreicht werden sollen.[23] Die Motivation für Compliance kann dabei unterschiedlich sein: Schutz vor straf- und zivilrechtlicher Haftung, Einhaltung regulatorischer Anforderungen oder sonstiger gesetzlicher Vorgaben, Erfüllung von Anforderungen der Geschäftspartner, Wahrung der Unternehmensreputation, Stärkung und Bewahrung der Unternehmenskultur, Prävention von Compliance-Vorfällen oder Unterstützung unternehmensinterner Veränderungspro-

zesse (zB bei einem Börsengang).[24] Compliance-Ziele sollten dabei auf die für das Unternehmen charakteristischen Aktivitäten fokussiert werden, um Schwerpunkte zu setzen und mit den übrigen Unternehmenszielen abgestimmt zu sein.[25]

Ein zentrales Anliegen vieler Betreiber von KI-Systemen wird die Einhaltung der KI-VO sein, um Sanktionen nach Art. 99 Abs. 4 KI-VO zu vermeiden.[26] In der Praxis zeigt sich jedoch auch ein erheblicher Compliance-Druck von Seiten der Unternehmens-Kunden, die sich KI-Compliance ihrer Vertragspartner gewährleisten lassen.

Hochrisiko-KI-Systeme zeichnen sich zudem dadurch aus, dass ihre Verwendung potenziell erhebliche Gefahren für zentrale Rechtsgüter birgt – etwa Gesundheit, Sicherheit, Grundrechte und das Vertrauen in demokratische sowie rechtsstaatliche Strukturen. Insofern kann auch der Schutz dieser Rechtsgüter ein Compliance-Ziel darstellen. In diesen besonders schutzwürdigen Bereichen sind Risiken eng zu begleiten und bestmöglich zu mitigieren. Wird ein KI-System beispielsweise im medizinischen Bereich zur Krebsdiagnose eingesetzt, liegt die potenzielle Gefahr für das Leben der Patienten auf der Hand. In solch

hochkritischen Szenarien sollte das KI-System regelmäßig auf Robustheit und Zuverlässigkeit getestet werden, etwa durch ungewöhnliche oder unwahrscheinliche Inputs. Technisch sollte das System in der Lage sein, eigene Unsicherheiten zu erkennen und bei Bedarf gezielt menschliche Unterstützung einzufordern. In besonders sensiblen Fällen kann die Implementierung eines Vier-Augen-Systems sinnvoll sein.

Gleichzeitig bietet die verantwortungsvolle Nutzung von KI im Einklang mit der KI-VO Chancen: Prozesse können optimiert und effizienter gestaltet werden, sodass Compliance-Maßnahmen nicht nur Pflicht, sondern auch ein nicht zu unterschätzender unternehmerischer Mehrwert sein können. Zuletzt zeigt sich Compliance auch zunehmend als Qualitätssiegel für digitale Produkte, deren Verlässlichkeit Kunden sonst nicht ohne Weiteres bewerten könnten.

Praxistipp:

Unternehmen sollten individuell festlegen, welche Ziele sie mit der Umsetzung von KI-Compliance verfolgen, und diese schriftlich dokumentieren. Hierfür sind keine zusätzlichen Gremien oder formellen Prozesse notwendig. Verantwortliche sollten vielmehr ihre bestehende Compliance-Agenda um die spezifischen Themen zur Festlegung und Umsetzung von KI-Zielen ergänzen.

III. Compliance-Risiken

Ein zentrales Element eines funktionierenden CMS ist die systematische Identifizierung und Bewertung unternehmensspezifischer Compliance-Risiken (Risikomanagement). Dieser Prozess ist strukturiert und methodisch einheitlich gestaltet und zielt darauf ab, im Wege von typisierter Einzelfallbetrachtung erkannte Risiken zu steuern und geeignete Gegenmaßnahmen zu implementieren.[27] Da ein CMS maßgeblich an den individuellen Risiken eines Unternehmens ausgerichtet ist, bildet das Risikomanagement das Fundament für die gesamte Compliance-Struktur.

Der typische Ablauf umfasst mehrere aufeinander folgende Schritte: Risikoanalyse, Risikobewertung, Risikobehandlung sowie die fortlaufende Überwachung der Risiken.[28]

1. Risikoanalyse anhand der Klassifizierung des verwendeten KI-Systems

Bestehende Prozesse zur Risikoanalyse sollten im Hinblick auf die neuen Anforderungen der KI-VO überprüft und angepasst werden.

Da die KI-VO einen risikobasierten Ansatz verfolgt[29] und die einzuhaltenden Pflichten von dieser Risikoklassifizierung des KI-Systems abhängen, ist eine gezielte Analyse der im Unternehmen eingesetzten KI-Systeme unerlässlich.

Als erster Schritt empfiehlt sich eine Bestandsaufnahme der verwendeten KI-Systeme.[30] Dabei sollten die Merkmale erfasst werden, die für die Einstufung im Rahmen der KI-VO und zur Bestimmung der unternehmensbezogenen Rolle relevant sind. Die Erhebung kann bspw. über Interviews oder strukturierte Fragebögen bei Mitarbeitenden erfolgen. Für jedes KI-System sollten die Merkmale einzeln abgefragt werden, um eine differenzierte Klassifizierung vornehmen zu können.

Beispielhafte Fragen:

- Welche KI-Systeme werden genutzt?
- Wer interagiert mit diesem KI-System?
- Wurde das KI-System intern entwickelt, zugekauft oder von einem Drittanbieter bezogen?
- In welchem Bereich wird das KI-System eingesetzt (zB Personalwesen, Gesundheitswesen, Strafverfolgung, kritische Infrastrukturen)?
- Werden biometrische Daten verwendet oder verarbeitet (zB Gesichts- oder Emotionserkennung)?

– Kommuniziert das KI-System direkt mit Menschen? Wenn ja, können Betroffene erkennen, dass sie mit einem KI-System interagieren?

Bestehende regelmäßige Risikoerhebungen lassen sich durch einen KI-spezifischen Fragenblock erweitern. Die Ergebnisse sollten systematisch dokumentiert und in einem Verzeichnis zusammengefasst werden.

Praxistipp:

Vorhandene Infrastrukturen wie ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSG-VO oder eine Configuration Management Database (CMDB) können genutzt werden, um relevante Systeme zu identifizie-

ren.[31] Außerdem ist es möglich, die Strukturen der Verzeichnisse um die KI-System-Inventarisierung zu erweitern. Durch die Ergänzung um KI-spezifische Attribute lässt sich eine gezielte Filterung und Auswertung ermöglichen.

2. Risikobewertung und -behandlung

Im nächsten Schritt des Risikomanagements sollten die relevanten Pflichten der KI-VO für jedes identifizierte KI-System festgestellt werden. Grundlage hierfür ist die Auswertung der erhobenen Daten, also die Klassifizierung des KI-Systems sowie die Bestimmung der Unternehmensrolle nach der KI-VO.[32] Es ist wichtig, dass diese Bewertung für jedes System separat durchgeführt wird, da die Pflichten je Risikoklasse und Rolle unterschiedlich ausfallen können.

Das Verfahren kann auch eine Gap-Analyse umfassen. Im Rahmen der Risikobehandlung sind die einschlägigen Pflichten der KI-VO herauszuarbeiten (Erhebung Soll-Zustand) und zu prüfen, ob gewisse Pflichten noch nicht erfüllt werden (Erhebung Ist-Zustand).

3. Überwachung

Abschließend ist eine fortlaufende Überprüfung und regelmäßige Wiederholung dieses Prozesses erforderlich. Der KI-Bereich unterliegt einer zunehmenden Regulierungsdichte, sodass Unternehmen flexibel und informiert bleiben müssen.

Insbesondere ist die Europäische Kommission nach Art. 7 Abs. 1 KI-VO befugt, delegierte Rechtsakte zur Änderung von Anhang III durch Hinzufügung oder Änderung von Anwendungsfällen für Hochrisiko-KI-Systeme zu erlassen. Das bedeutet: Auch Einsatzbereiche, die derzeit nicht vom Anwendungsbereich der KI-O erfasst sind oder aktuell nicht mit einem hohen Risiko eingestuft werden, könnten durch eine Erweiterung von Anhang III künftig in den Geltungsbereich der Pflichten einbezogen werden – ohne dass ein reguläres Gesetzgebungsverfahren erforderlich ist.

IV. Compliance-Programm: Maßnahmen zur Sicherstellung eines typengerechten Gebrauchs

Das Compliance-Programm setzt unternehmensspezifische Steuerungsmaßnahmen zur Risikobegrenzung und Schadensvermeidung um. Das Ziel ist es, Mechanismen und Instrumente – etwa Richtlinien, Arbeitsanweisungen und Schulungen – zu entwickelt, um festgelegte Compliance-Ziele zu erreichen und deren Umsetzung im Unternehmen sicherzustellen.[33] Erfasst sind außerdem Maßnahmen zur frühzeitigen Erkennung, Meldung, Aufklärung und Ahndung von Verstößen.[34]

1. Implementierung von technischen und organisatorischen Maßnahmen

Nach Art. 26 Abs. 1 KI-VO sind Betreiber von Hochrisiko-KI-Systemen dazu verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, um eine zweckgemäße Verwendung des KI-Systems sicherzustellen. Diese hängt wiederum maßgeblich von den Vorgaben des Anbieters in der

Betriebsanleitung des KI-Systems ab (Art. 13 Abs. 2 KI-VO); Anbieter müssen dem Betreiber in einer Betriebsanleitung präzise, vollständig, korrekt und eindeutig die wichtigsten Merkmale, Fähigkeiten und Leistungsgrenzen des KI-System mitteilen. Zur Sicherstellung des typengerechten Gebrauchs eines Hochrisiko-KI-Systems müssen Betreiber zudem dafür sorgen, dass die Eingabedaten des Hochrisiko-KI-Systems, sofern diese ihrer Kontrolle unterliegen, der Zweckbestimmung des KI-Systems entsprechen und ausreichend repräsentativ sind (Art. 26 Abs. 4 KI-VO).

Maßnahmen zur Sicherstellung der spezifischen Funktionsweise eines KI-Systems sind also individuell anhand des jeweiligen KI-Systems auszugestalten und mit der Betriebsanleitung abzustimmen.

Technische Möglichkeiten zur Umsetzung dieser Pflicht sind beispielsweise Zugriffs- und Benutzerkontrollen, Lösch- und Korrekturmechanismen oder eine Notfallabschaltung. Ein rollenbasiertes Zugriffssystem ermöglicht, dass ausschließlich geschultes Personal bestimmte KI-Systeme verwenden oder gewisse Funktionen aufrufen kann. Die Implementierung einer Input-Validierung dient dem Zweck, dass lediglich geeignete, vorgesehene Daten als Eingabe verwendet werden und fehlerhafte Formate abgelehnt werden. Zur Vermeidung erheblicher Betriebsabweichungen kann eine automatische Deaktivierung des KI-Systems vorgesehen werden, sobald ein definierter Schwellenwert überschritten wird. Eine automatisierte Protokollierung von Eingabedaten und Resultaten hilft zudem, Missbrauch, Fehlanwendung oder Systemfehler zu identifizieren.

In organisatorischer Hinsicht können unter anderem Maßnahmen zum Schutz vor Missbrauch, Störfall- und Sicherheitspläne, ein Risikomeldesystem sowie Schulungs- und Sensibilisierungsmaßnahmen für Mitarbeitende entwickelt und umgesetzt werden.

2. Erstellung einer KI-Richtlinie mit Acceptable-Use- oder Prompting Policy

Besonders empfehlenswert ist die Erstellung einer unternehmensinternen KI-Richtlinie.[35] Darin sollten ethische Grundsätze klar formuliert, zulässige Eingabedaten definiert, Datenschutz und Privatsphäre geregelt sowie Resultatkontrollen und Schulungspflichten festgelegt werden. So können Missbrauch und sonstige Schäden wirksam verhindert werden. Ergänzend bietet sich eine Acceptable-Use- oder Prompting Policy an, die festlegt, dass Prompts ausschließlich Informationen anfordern oder nutzen, die dem Zweck des KI-Systems entsprechen und Hinweise enthält, um das System möglichst effizient einzusetzen. Für den Umgang mit Störfällen sollte die Richtlinie klare Verantwortlichkeiten, Ansprechpartner sowie ein

funktionierendes Melde- oder Whistleblower-System benennen, um eine schnelle Reaktion und Aufklärung von Fehlern sicherzustellen.

Praxistipp:

Um die Verwendung eines KI-Systems im Einklang mit seiner vorgesehenen Funktionsweise zu gewährleisten, empfiehlt sich die Operationalisierung der Betriebsanleitung. Dies kann zB durch klare Arbeitsanweisungen, dokumentierte Eingabevorgaben oder Funktionsfreigaben erfolgen, die direkt in die KI-Richtlinien des Unternehmens integriert werden.

V. Compliance-Organisation: Aufbau von KI-Kompetenz und klaren Verantwortlichkeiten

Durch die Compliance-Organisation werden Rollen und Verantwortlichkeiten des Compliance-Managements im Unternehmen festgelegt, klar abgegrenzt, transparent kommuniziert und nachvollziehbar dokumentiert. Alle Verantwortlichen müssen über die erforderlichen persönlichen und fachlichen Qualifikationen verfügen und von der Unternehmensführung mit den notwendigen Ressourcen ausgestattet werden, um ihre Aufgaben zuverlässig wahrnehmen zu können.[36]

Art. 4 Abs. 1 KI-VO verpflichtet Betreiber von KI-Systemen – unabhängig von der Risikoklassifizierung – dazu, sicherzustellen, dass ihr Personal sowie alle Personen, die in ihrem Auftrag mit Betrieb und Nutzung der KI-Systeme betraut sind, über ein angemessenes Maß an KI-Kompetenz verfügen. Unter „KI-Kompetenz" wird die Fähigkeit verstanden, die es Anbietern, Betreibern und Betroffenen ermöglicht, KI-Systeme sachkundig einzusetzen und sich der Chancen, Risiken und potenziellen Schäden bewusst zu sein, die von KI ausgehen können (vgl. Art. 3 Nr. 56 KI-VO).

Das erforderliche Maß an KI-Kompetenz richtet sich im Einzelfall nach den technischen Kenntnissen, Erfahrungen, dem Aus- und Weiterbildungsstand der beteiligten Personen sowie dem Kontext, in dem die Systeme eingesetzt werden. Die KI-VO verfolgt einen ganzheitlichen Kompetenzansatz: Vermittelt werden müssen nicht nur rechtliche Anforderungen, sondern auch technische und ethische Aspekte – nur so kann der geforderte „sachkundige Einsatz" sichergestellt werden.[37]

Um dieser Pflicht nachzukommen, sollte ein Unternehmen zunächst den erforderlichen Maßstab an KI-Kompetenz im Detail festlegen. Der interne Schulungsbedarf hängt dabei von der Zielgruppe (zB Datenanalysten, Mitarbeitende mit Kundenkontakt, Entscheidungsträger, HR-Mitarbeitende), dem jeweiligen Wissensstand und den eingesetzten KI-Systemen ab. Idealerweise wird dieser Bedarf differenziert ermittelt und gezielt berücksichtigt.[38]

1. Durchführung von KI-Schulungen

KI-Richtlinien können zunächst dazu dienen, theoretisches Wissen über Chancen, Risiken und Grenzen der Nutzung von KI-Systemen zu vermitteln. Ein zentrales Instrument zur Umsetzung der Pflicht sind darüber hinaus praxisnahe Schulungen,[39] die in unterschiedliche Module unterteilt werden sollten. Die Gestaltung und Durchführung dieser Schulungen können bei Bedarf an externe Dienstleister ausgelagert werden.

Ein Grundlagenmodul sollte sich an alle Mitarbeitenden richten und auf Einsteiger-Niveau konzipiert sein. Die Inhalte können von ethischen Fragestellungen, technischen Grundlagen und den Auswirkungen von KI auf Arbeit und Gesellschaft bis hin zu einer kompakten Darstellung der Vorgaben der KI-VO reichen. Diese Wissensvermittlung kann dabei über E-Learnings, Videos und interaktive Quizze erfolgen.

Ein zweites Anwendungsmodul sollte zielgruppen- und wissensorientiert gestaltet sein, um KI-Kompetenz gezielt im jeweiligen Tätigkeitsbereich zu fördern. So kann ein Managementmodul für Führungskräfte den Fokus auf rechtliche Rahmenbedingungen und den strategischen Einsatz von KI als Business-Case legen, während ein Modul für HR-Mitarbeitende vermittelt, wie KI-Tools verantwortungsvoll und effizient in Recruiting, Personalentwicklung und administrativen HR-Prozessen eingesetzt werden können.

Ein anwendungsbezogenes Schulungsprogramm trägt zudem dazu bei, die Anforderungen aus Art. 26 Abs. 2 KI-VO zu erfüllen. Betreiber von Hochrisiko-KI-Systemen sind danach verpflichtet, eine wirksame menschliche Aufsicht sicherzustellen – und zwar durch hinreichende Unterstützung und Qualifizierung der Aufsichtsperson. Das Ziel ist es, Risiken für Gesundheit, Sicherheit und Grundrechte wirksam zu minimieren.

2. Benennung eines KI-Beauftragten – Doppelrolle als Datenschutzbeauftragter zulässig?

Zwar schreibt die KI-VO die Benennung eines KI-Beauftragten nicht zwingend vor, dennoch kann es in der Praxis sinnvoll sein, Verantwortung und Expertise zentral zu bündeln – zB bei einer Person in einer spezialisierten Abteilung. Ein KI-Beauftragter kann als beratende und überwachende Instanz fungieren und sollte über ausreichendes technisches Verständnis verfügen, um u. a. die Einhaltung regulatorischer Vorgaben, das Risikomanagement, die Entwicklung interner Richtlinien und die Organisation von Schulungen – kurz: die KI-Compliance – wirksam zu unterstützen.[40]

Auch die Doppelbenennung eines bereits nach Art. 38 DSG-VO bestellten Datenschutzbeauftragten als KI-Beauftragter kann in Betracht gezogen werden. Dabei ist jedoch zu berücksichtigen, dass die jeweils erforderlichen Fachkompetenzen nicht deckungsgleich sind. Zudem muss die Unabhängigkeit der Datenschutzfunktion gewahrt und

Interessenkonflikte strikt vermieden werden.[41] Ein solcher Konflikt bestünde beispielsweise dann, wenn die Person zusätzlich Funktionen übernimmt, die eine Festlegung von Mitteln und Zwecken der Verarbeitung personenbezogener Daten beinhaltet.[42]

Im Fall einer Doppelfunktion als KI- und Datenschutzbeauftragter ist besondere Vorsicht geboten, etwa bei der Mitwirkung an der Auswahl oder Einführung von KI-Tools im HR-Bereich – zB zur automatisierten Analyse von Mitarbeiterbefragungen oder zur Bewerbervorauswahl. Angesichts der empfindlichen Bußgeldandrohung bei DSG-VO-Verstößen (Art. 83 Abs. 4 lit. a DSG-VO) sollten Unternehmen der Rollenabgrenzung besondere Aufmerksamkeit schenken.

Zudem bestehen inhaltliche Spannungsfelder zwischen DSG-VO und KI-VO. Während die DSG-VO Grundsätze wie Datenminimierung[43], Zweckbindung[44] und Datenrichtigkeit[45] betont, setzt die Entwicklung von KI-Modellen wie insbesondere Large Language Models (LLMs) das Training mit großen Datenmengen voraus und basiert auf Wahrscheinlichkeiten. Während die KI-VO einen Ausgleich von Innovation und gesellschaftlichen Risiken durch KI-Nutzung bezweckt, regelt die die DSG-VO wie zB in Art. 12 ff. Betroffenenrechte in Ausfüllung des Grundrechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG. Zuletzt verlangt die DSG-VO nach Art. 5 Abs. 2 eine klare Verantwortungszuordnung mit Nachweispflichten sowie Transparenz.[46] KI-Modelle werden jedoch auch als „Black Box“ bezeichnet, weil deren selbstlernenden Vorgänge teilweise sogar für ihre Entwickler nicht vollständig nachvollziehbar sind.[47]

Praxistipp:

Ein Datenschutzbeauftragter kann grundsätzlich auch Aufgaben eines KI-Beauftragten übernehmen – vorausgesetzt, Interessenkonflikte werden konsequent ausgeschlossen und seine Unabhängigkeit bleibt gewahrt. Eine Prüfung der Vereinbarkeit beider Rollen ist daher im Vorfeld zwingend anzuraten.

VI. Compliance-Kommunikation: Transparenter Umgang mit KI-Systemen

Das Grundelement der Compliance-Kommunikation meint einen strukturierten Ansatz, betroffene Mitarbeitende aller Ebenen im Unternehmen oder auch Dritte über Unternehmenswerte, Aus- und Weiterbildungen, erwartete Verhaltensweisen, zu beachtende Regelungen oder festgelegte Rollen zu informieren. In repressiver Hinsicht sollte auf Berichtswege und -pflichten hingewiesen und Krisenmanagement mitberücksichtigt werden.[48] Im Wesentlichen sollen betroffene Personen über die für sie maßgeblichen Bestandteile des CMS sensibilisiert und auf Compliance-relevanten Informationen hingewiesen werden. Klassische Umsetzungsmaßnahmen zur Kommunikation über Compliance sind Richtlinien, Schulungen und ein Code of Conduct.

Art. 26 Abs. 7 KI-VO verpflichtet Betreiber dazu, vor einer Inbetriebnahme oder Nutzung des Hochrisiko-KI-Systems am Arbeitsplatz die Arbeitnehmervertreter und die betroffenen Arbeitnehmer über die Verwendung zu informieren. Diese Norm soll als Auffangtatbestand sicherstellen, dass die Information unabhängig davon erfolgt, ob sie bereits nach anderen zB betriebsverfassungsrechtlichen Vorschriften erforderlich ist, vgl. ErwG 92 KI-VO.

Außerdem statuieren Art. 50 Abs. 3 und Abs. 4 KI-VO weitere Informations- und Transparenzpflichten. Entsprechende Informationspflichten betreffen zunächst Betreiber von KI-Systemen zur Emotionserkennung und biometrischen Kategorisierung. Betreiber von KI-Systemen, welche zur Erzeugung von Deepfakes oder zur Erstellung bzw. Manipulation veröffentlichter Texte eingesetzt werden, unterliegen in bestimmten Konstellationen einer Offenlegungspflicht.

Praxistipp:

Hinsichtlich spezifischer Informationspflichten nach Art. 26 Abs. 7 KI-VO bietet sich ein Anknüpfen an bestehende Strukturen zur Erfüllung von Betroffenenrechten nach Art. 12 DSG-VO an. Entsprechend den dort festgelegten Anforderungen sollte die Information präzise, transparent, verständlich und in leicht zugänglicher Form sowie in klarer, einfacher Sprache erfolgen. Inhaltlich kann auf die Informationen aus der Betriebsanweisung nach Art. 13 KI-VO (Kontaktangaben des Anbieters sowie Merkmale, Fähigkeiten und Leistungsgrenzen des KI-Systems usw.) zurückgegriffen werden.[49]

VII. Compliance-Überwachung und -Verbesserung: Ganzheitliches Life-Cycle-Management von KI-Systemen

Zuletzt sollte zur Compliance-Überwachung und -Verbesserung regelmäßig überprüft werden, ob die implementierten Maßnahmen angemessen und wirksam ausgestaltet sind. Dieser Vorgang ist hinreichend zu dokumentieren, um eine sorgfältige Auswertung zu ermöglichen. Falls Prozessschwächen oder Lücken identifiziert werden, sollten diese behoben werden.[50]

Art. 26 Abs. 5 KI-VO begründet eine Pflicht zur Überwachung der Funktionsweise eines Hochrisiko-KI-Systems. Insbesondere haben Betreiber ein Hochrisiko-KI-System anhand seiner Betriebsanleitung zu kontrollieren und, sofern erforderlich, den Anbieter gem. Art. 72 KI-

VO zu informieren. Ferner müssen sie die Nutzung des KI-Systems aussetzen und den Anbieter, Händler und die zuständige Behörde informieren, wenn der Verdacht besteht, dass die Nutzung des Hochrisiko-KI-Systems gemäß der Betriebsanleitung ein Risiko gem. Art. 79 Abs. 1 KI-VO darstellt oder ein schwerwiegender Vorfall festgestellt wurde.

Um diesen Betreiberpflichten nachkommen zu können, bietet es sich an, bestehende Audit-, Monitoring- und Review-Prozesse um KI-relevante Kontrollen zu erweitern. Die ordnungsgemäße Verwendung des KI-Systems lässt sich bspw. durch einen Abgleich der dokumentierten Use Cases mit den Einsatzgrenzen der Gebrauchsanweisung überprüfen. Zudem kann eine Kommunikationsplattform geschaffen werden, auf der Probleme oder Fehler bei der KI-Nutzung im Unternehmen zum Nutzen aller Mitarbeitenden gemeldet oder dokumentiert werden können.

Zur Gewährleistung eines strukturierten Krisenmanagements im Falle eines schwerwiegenden Vorfalls kann ein gesonderter Störfall-Leitfaden erstellt werden. Dieser sollte Schritt für Schritt darlegen, wie sich Mitarbeitende im konkreten Fall verhalten sollen, wer die zuständigen Ansprechpartner sind (einschließlich ihrer Kontaktdaten) und welche internen Stellen, Personengruppen oder Behörden informiert werden müssen.

Im Weiteren sind Betreiber gem. Art. 26 Abs. 6 KI-VO dazu verpflichtet, die automatisch erzeugten Protokolle ihrer Hochrisiko-KI-Systeme mindestens sechs Monate aufzubewahren, wenn sie unter ihrer Kontrolle stehen.

Die beiden vorbezeichneten Pflichten kennzeichnen den ganzheitlichen Ansatz des Gesetzgebers, wonach ein angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit von Hochrisiko-KI-Systemen während ihres gesamten Lebenszyklus zu gewährleisten ist.[51]

Dieser Prozess kann als Life-Cycle-Management bezeichnet werden und meint die Gestaltung, Anpassung und Kontrolle des gesamten KI-Lebenszyklus. Umfasst ist zum einen die technische Überwachung von Treffsicherheit sowie das Ausfindigmachen von Anomalien und Bias, was durch Tests und Validierungen erreicht werden kann.[52] Es sollte darüber hinaus regelmäßig geprüft werden, ob sämtliche rechtlichen und

ethischen Anforderungen (auch abseits der KI-VO, aus dem Datenschutzrecht oder branchenspezifischen Regelungen) eingehalten werden und die implementierten Compliance-Maßnahmen wirksam sind.

Praxistipp:

Automatisch erzeugte Protokolle können nach datenschutzrechtlicher Prüfung meist ohne großen Mehraufwand mittels bestehenden Logging- bzw. Archivierungslösungen aufbewahrt werden. Darüber hinaus können sie als Grundlage für ein Log-Review dienen und in ein Frühwarnsystem über definierte Trigger eingebunden werden, um bspw. fehlerhafte Resultate, Treffsicherheit oder Bias festzustellen. Als Referenz für die Auswahl geeigneter Trigger kann insbesondere die Betriebsanleitung des KI-Systems herangezogen werden.

VIII. Überblick

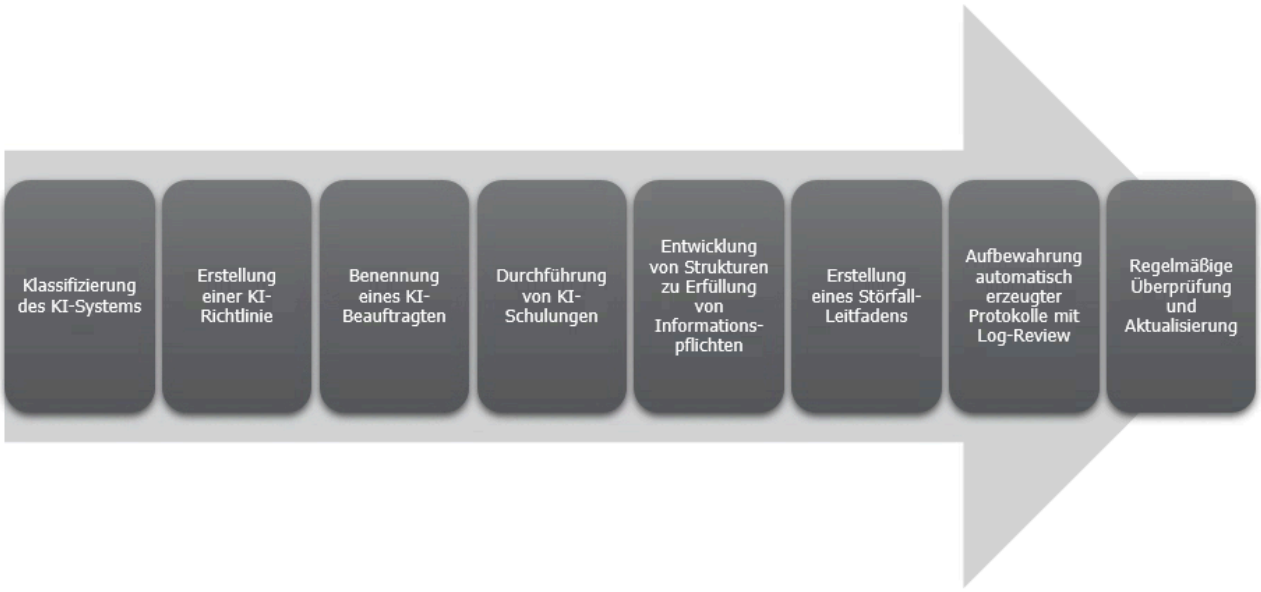
Der folgende Überblick illustriert das Ineinandergreifen von Compliance-Elementen mit Betreiberpflichten der KI-Verordnung und ergänzt konkrete Praxistipps

CMS-Grundelement	Betreiberpflicht	Praxistipps[1]
Compliance-Kultur		✓ Klares Bekenntnis zu KI-Ethikleitlinien, ErwG 27 KI-VO ✓ Einführung von "Prompts der Woche" oder „Fun- bzw. Hard Truth-Facts" in internen Meetings
Compliance-Ziele		✓ Erweiterung der Agenda bestehender Entscheidungsgremien um KI-Compliance-Ziele
Compliance-Risiken	Klassifizierung des KI-Systems	✓ Erweiterung vorhandener IT-Verzeichnisse, z.B. durch KI-Kennzeichnungen mit zusätzlichen Attributen
Compliance-Programm	Treffen von Maßnahmen zum typengerechten Gebrauch, Art. 26 Abs. 1 KI-VO	✓ Operationalisierung der Betriebsanleitung des KI-Systems mit Verankerung in KI-Richtlinie
	Qualitätsmanagement von Eingabedaten, Art. 26 Abs. 4 KI-VO	✓ Erweiterung der KI-Richtlinie um eine *Acceptable-Use-* oder *Prompting-Policy*
Compliance-Organisation	Aufbau von KI-Kompetenz, Art. 4 KI-VO	✓ Durchführung von KI-Schulungen (ggf. Auslagerung auf externe Dienstleister)
	Einsetzen einer Aufsichtsperson, Art. 26 Abs. 2 KI-VO	✓ Durchführung anwendungsspezifischer Schulungen ✓ Benennung eines KI-Beauftragten (ggf. Doppelrolle eines Datenschutzbeauftragten nach rechtlicher Prüfung der Vereinbarkeit beider Tätigkeiten)
Compliance-Kommunikation	Informations- und Transparenzpflichten, 26 Abs. 7, Abs. 11 und Art. 50 Abs. 3, Abs. 4 KI-VO	✓ Anknüpfen an Anforderungen und bestehende Strukturen zur Erfüllung von Betroffenenrechten, Art. 12 DSG-VO ✓ Inhaltlich: Zurückgreifen auf Angaben der Betriebsanleitung des KI-Systems
Compliance-Überwachung und -Verbesserung	Pflicht zur Überwachung sowie Aussetzen des Betriebs, Art. 26 Abs. 5 KI-VO	✓ Durchführung einer Log-Review von automatisch erzeugten Protokollen mit Frühwarnsystem bei bestimmten Triggern
	Meldung schwerwiegender Vorfälle, Art. 73 KI-VO	✓ Entwicklung eines Störfall-Leitfadens
	Aufbewahrung automatisch erzeugter Protokolle,	✓ Nutzung bestehender Logging- bzw. Archivierungslösungen

[1] Nicht abschließend.

Zugleich begründet die KI-VO eigenständige Anforderungen, die aktives Handeln erfordern – ein bloßer Verweis auf vorhandene Prozesse, Schulungen oder Datenerfassungen genügt nicht. Auch hier kann ein Rückgriff auf bestehende Abläufe den Implementierungsaufwand senken und die laufende Überwachung erleichtern.

Sinnvoll ist ein strukturierter Fahrplan für Betreiber von Hochrisiko-KI-Systemen, der – rechtssicher ausgestaltet – die wesentlichen Pflichten abdeckt:



KONTAKT:

Dr. Carolin Raspé

YPOG GmbH & Co. KG

Oberangerstraße 28

80331 München

Tel.: 089/3779953291

carolin.raspe@ypog.law

Dr. Benedikt Flöter

YPOG GmbH & Co. KG

Kurfürstendamm 12

10719 Berlin

Tel.: 030/7675975177

benedikt.floeter@ypog.law

* Die Autoren bedanken sich herzlich bei Carla Wolf und Steffen Kootz, Wissenschaftliche Mitarbeiter:innen bei YPOG, für die wertvolle Mitarbeit bei der Erstellung dieses Beitrags.

1 Dieser Aufsatz konzentriert sich auf Betreiberpflichten. Während Anbieter solche Unternehmen sind, die KI-Systeme selbst entwickeln oder bestehende Modelle in eigene Produkte integrieren und unter eigener Marke vertreiben, genügt es für Betreiber bereits, ein KI-System zu betrieblichen bzw. betriebsbezogenen Zwecken einzusetzen (hierzu näher unter 2., Prüfungsschritt 3). Der Kreis der Normadressaten dürfte damit weiter sein und insbesondere auch Unternehmen erfassen, bei denen KI-Systeme nicht zum unternehmerischen Kerngeschäft zählt. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

2

Zudem muss der räumliche Anwendungsbereich der KI-VO eröffnet sein. Dieser ist weit gefasst und gerade für Betreiber mit Sitz in der Union regelmäßig anzunehmen, vgl. Art. 2 Abs. 1 lit. a-c KI-VO.

3 Vgl. Europäische Kommission C(2025) 924 final, Guideline (9), abrufbar unter https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application (zuletzt abgerufen am 20.11.2025).

4 Europäische Kommission C(2025) 924 final, Guideline (26).

5 So ähnlich *Ritter/ Schaa* DSB 2025, 32 (34).

6 *Ebers/ Streitbörger* RDi 2024, 393 (395).

7 Vgl. Art. 6 Abs. 1 Lit. a KI-VO: „soll"; Anhang III KI-VO „bestimmungsgemäß"; ErwG 52 KI-VO.

8 *Ebers/ Streitbörger* RDi 2024, 393 (395).

9 *Eickmeier/ Petrasch* YPOG Briefing: Art. 4 KI-Verordnung: Die unterschätzte Herausforderung auf dem Weg zur KI-Compliance, S. 2; abrufbar unter https://9177093.fs1.hubspotusercontent-eu1.net/hubfs/9177093/Briefings/YPOG%20Briefing_Art.%204 %20KI-Verordnung_27.1.2025.pdf (zuletzt abgerufen am 20.11.2025).

10 Europäische Kommission COM(2025) 836 final, S. 18; abrufbar unter https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal (zuletzt abgerufen am 20.11.2025).

11 Einrichtungen des öffentlichen Rechts oder private Einrichtungen, die öffentliche Dienste erbringen sowie Betreiber von KI-Systemen zur Kreditwürdigkeits- und Bonitätsprüfung oder Risikobewertung und Preisbildung im Fall von Lebens- und Krankenversicherungen, gem. Art. 27 Abs. 1 KI-VO.

12 *Ebers/ Streitbörger* RDi 2024, 393 (399).

13 Moosmayer/Lösler/ *Moosmayer/ Lösler*, Corporate Compliance, 4. Aufl. 2024, § 1 Rn. 4.

14 Vgl. LG München I 10.12.2013 – 5HK O 1387/10, NZG 2014, 345 (348); BGH 9.5.2017 – 1 StR 265/16, BeckRS 2017, 114578, Rn. 118; OLG Nürnberg 30.3.2022 – 12 U 1520/19, NZG 2022, 1058 (1061 f.).

15 OLG Nürnberg 30.3.2022 – 12 U 1520/19, NZG 2022, 1058 (1061).

16 Deutsches Institut für Compliance DICO Standard Compliance-Management-Systeme 03.2021, S. 28, abrufbar unter https://www.dico-ev.de/wp-content/uploads/2021/03/STANDARD_CMS_2021.pdf (zuletzt abgerufen am 20.11.2025).

17 LG München I 10.12.2013 – 5HK O 1387/10, NZG 2014, 345 (347); Schulz BB 2017, 1475 (1476).

18 *Benraouane* AI Management System Certification Accoording to the ISO/IEC 42001 Standard, S. XXXIV f.

19 Institut der Wirtschaftsprüfer IDW EPS 980 nF 28.10.2021, Rn. 27.

20 Van Erp/Huisman/Vande Walle/*Bussmann*, The Routledge Handbook of White-Collar and Corporate Crime, 1. Aufl. 2015, S. 435 (445 ff.).

21 *Bussmann* CCZ 2016, 50 (54); Schieffer CCZ 2018, 93 (95).

22 Institut der Wirtschaftsprüfer IDW EPS 980 nF 28.10.2021 Rn. 27, Tz. A23.

23 Institut der Wirtschaftsprüfer IDW EPS 980 nF 28.10.2021 Rn. 27, Tz. A24.

24 Melot de Beauregard/Lieder/Liersch/*v. Busekist*/*Federmann*/*Lochen*, Managerhaftung-HdB, 1. Aufl. 2022, § 13 Rn. 50.

25 Moosmayer/Lösler/*Schorn*/*Viebranz*, Corporate Compliance, 4. Aufl. 2024, § 11 Rn. 2.

26 Siehe dazu näher oben: B. IV. Prüfungsschritt vier: Gilt mein Unternehmen als Anbieter?.

27 *Von Busekist*/*Schlitt* CCZ 2012, 86 (86 f.).

28 Institut der Wirtschaftsprüfer IDW EPS 980 nF 28.10.2021 Rn. 27, Tz. A25.

29 Siehe dazu näher oben: B. Anwendbarkeit der KI-VO.

30 So u. a. auch *Pepping* BB 2025, 1269 (1279); *Reese* BB 2024, 1515 (1518); *Klos*/*Taylan* CCZ 2024, 205 (211 f.).

31 *Klos*/*Taylan* CCZ 2024, 205 (211 f.).

32 Siehe dazu näher oben: B. Anwendbarkeit der KI-VO.

33 MHdB GesR IX/*Windthorst*, 6. Aufl. 2021, § 14 Rn. 69 f.; Institut der Wirtschaftsprüfer IDW EPS 980 nF 28.10.2021 Rn. 27, Tz. A26.

34 Moosmayer/Lösler/*Heißner*, Corporate Compliance, [Bitte Jahr, Auflage, Edition ergänzen], § 46 Rn. 18.

35 Vgl. hierzu auch *Pepping* BB 2025, 1269 sowie *Pepping* BB 2025, 1333.

36 Institut der Wirtschaftsprüfer IDW EPS 980 nF 28.10.2021 Rn. 27, Tz. A27.

37

Eickmeier/Petrasch, YPOG Briefing: Art. 4 KI-Verordnung: Die unterschätzte Herausforderung auf dem Weg zur KI-Compliance, S. 3; abrufbar unter https://9177093.fs1.hubspotusercontent-eu1.net/hubfs/9177093/Briefings/YPOG%20Briefing_Art.%204 %20KI-Verordnung_27.1.2025.pdf (zuletzt abgerufen am 20.11.2025).

38 *Schippel* KIR 2025, 119 (121).

39 So auch *Eickmeier/Petrasch*, YPOG Briefing: Art. 4 KI-Verordnung: Die unterschätzte Herausforderung auf dem Weg zur KI-Compliance, S. 4; abrufbar unter https://9177093.fs1.hubspotusercontent-eu1.net/hubfs/9177093/Briefings/YPOG%20Briefing_Art.%204 %20KI-Verordnung_27.1.2025.pdf (zuletzt abgerufen am 20.11.2025).

40 *Reese* BB 2024, 1515 (1517).

41 Vgl. ErwG 97 GSGVO, Art. 38 Abs. 6 S. 2 DSG-VO.

42 EuGH 9.2.2023 – C-453/21 (X-FAB Dresden) Rn. 44, 46; BAG 6.6.2023 – 9 AZR 383/19, BeckRS 2023, 12617 Rn. 23.

43 Art. 5 Abs. 1 lit. c DSG-VO.

44 Art. 5 Abs. 1 lit. b DSG-VO.

45 Art. 5 Abs. 1 lit. d DSG-VO.

46 Art. 5 Abs. 1 lit. a Var. 3 DSG-VO.

47 *Paal* ZfDR 2024, 129 (145).

48 Melot de Beauregard/Lieder/Liersch/*v. Busekist/Federmann/Lochen*, Managerhaftung-HdB, 1. Aufl. 2022, § 13 Rn. 383 ff., Rn. 392; Institut der Wirtschaftsprüfer IDW EPS 980 nF 28.10.2021 Rn. 27, Tz. A28; Moosmayer/Lösler/*Heißner*, Corporate Compliance, 4. Aufl. 2024, § 46 Rn. 23.

49 *Lommatzsch/Albrecht* GWR 2025, 37 (39).

50 Godzierz/*Clodius*, Compliance Checklisten, 6. Aufl. 2025, § 4 Rn. 50 f.; Institut der Wirtschaftsprüfer IDW EPS 980 nF 28.10.2021 Rn. 27, Tz. A29.

51 Vgl. Art. 15 Abs. 1 KI-VO.

52 Leupold/Wiebe/Glossner/*Huber*, IT-R, 4. Aufl. 2021, Teil 9.4 Rn. 23; Reese BB 2024, 1515 (1519).