Die Anforderungen an das Qualitätsmanagement durch die KI-Verordnung

Prof. Dr. Thomas Söbbing*

Mit der Einführung der EU-KI-Verordnung (KI-VO) stellt sich auch die Frage, welche Anforderungen Unternehmen, die KI verwenden, im Bereich des Qualitätsmanagements erfüllen müssen. Die zentrale Norn hierfür ist Art. 17 KI-VO, die konkrete Anforderungen an das Qualitätsmanagement für Hochrisiko KI-Systeme enthält. Im Bereich des Qualitäts- und Risikomanagements existieren bereits etablierte internationale Normen, insbesondere die ISO 42001 als spezifische Norm für KI-Managementsysteme, die ISO 9001 als allgemeiner Standard für Qualitätsmanagementsysteme sowie die ISO 27001 für Informationssicherheitsmanagementsysteme. Der folgende Artikel geht der Frage nach, ob die Befolgung dieser Standards auch ausreichend ist, um die Anforderung nach Art. 17 KI-VO zu erfüllen.

I. Einleitung

1 Die rasante Entwicklung von Systemen der Künstlichen Intelligenz (KI) und deren zunehmender Einsatz in sicherheitskritischen und gesellschaftlich relevanten Bereichen stellt sowohl die Wirtschaft als auch die Gesetzgeber vor erhebliche Herausforderungen. Insbesondere sogenannte Hochrisiko-KI-Systeme, etwa in der medizinischen Diagnostik, in sicherheitsrelevanten Infrastrukturen oder im Bereich der Beschäftigung, können erhebliche Auswirkungen auf Leben und Rechte von Menschen haben. Vor diesem Hintergrund hat die Europäische Union mit der KI-Verordnung (KI-VO)[1] einen regulatorischen Rahmen geschaffen, der den sicheren und vertrauenswürdigen Einsatz solcher Systeme gewährleisten soll.

2 Ein zentrales Element dieser Verordnung bildet Art. 17 KI-VO, der die Anbieter hochriskanter KI-Systeme zur Einrichtung und Aufrechterhaltung eines Qualitäts- und Risikomanagementsystems verpflichtet. Ziel ist es, die kontinuierliche Compliance mit den rechtlichen Anforderungen sowie die effektive Risikominimierung über den gesamten Lebenszyklus der KI-Systeme hinweg sicherzustellen. Damit rückt die Frage in den Fokus, wie diese regulatorischen Anforderungen praktisch umgesetzt werden können.[2]

3 Im Bereich des Qualitäts- und Risikomanagements existieren bereits etablierte internationale Normen, ins-

besondere die ISO 42001[3] als spezifische Norm für KI-Managementsysteme, die ISO 9001 als allgemeiner Standard für Qualitätsmanagementsysteme sowie die ISO 27001 für Informationssicherheitsmanagementsysteme. Diese Normen bieten strukturierte Vorgehensweisen, um Managementsysteme zu planen, umzusetzen, zu überwachen und kontinuierlich zu verbessern. Dabei stellt sich die Frage, inwieweit diese Normen geeignet sind, die Anforderungen aus Art. 17 KI-VO zu erfüllen oder zumindest zu flankieren. Ziel dieses Beitrags ist es, die Anforderungen des Art. 17 KI-VO detailliert darzustellen, deren praktische Umsetzungsmöglichkeiten im Rahmen der genannten ISO-Normen zu analysieren und aus juristischer Sicht zu bewerten, ob eine Zertifizierung nach diesen Normen als Nachweis für die Erfüllung der gesetzlichen Pflichten ausreicht. Besonderes

Augenmerk wird dabei auf die Schnittstellen und möglichen Lücken („Gaps“) zwischen den regulatorischen Anforderungen und den Normvorgaben gelegt.

II. Die Anforderungen des Art. 17 KI-VO im Überblick

1. Zielsetzung und Systematik

4 Der europäische Gesetzgeber verfolgt mit Art. 17 KI-VO das Ziel, sicherzustellen, dass Anbieter hochriskanter KI-Systeme über geeignete interne Strukturen und Prozesse verfügen, um die Konformität ihrer Systeme während des gesamten Lebenszyklus zu gewährleisten.[4] Die Vorschrift stellt damit eine Konkretisierung des allgemeinen Konformitätsbewertungsregimes der KI-Verordnung dar und bildet eine Brücke zwischen dem produktspezifischen Risikomanagement und dem organisatorischen Qualitätsmanagement.[5] Während Art. 9 KI-VO das Risikomanagement auf der Ebene des einzelnen KI-Systems regelt, adressiert Art. 17 die dahinterliegende betriebliche Organisation und deren Fähigkeit, Risikomanagementprozesse effektiv zu steuern und zu dokumentieren. Zur Gewährleistung der Konformität der KI-Systeme mit den Anforderungen dieser Verordnung sollten Anbieter von Hochrisiko-KI-Systemen ein Qualitätsmanagementsystem einrichten, das als Teil ihrer internen Governance-Struktur fungiert. Dieses System sollte Verfahren zur Umsetzung der in dieser Verordnung vorgesehenen Anforderungen enthalten.[6]

5 Die Vorschrift verlangt somit die Einführung, Dokumentation und kontinuierliche Aufrechterhaltung eines Qualitätsmanagementsystems, das geeignet ist, sämtliche Anforderungen der KI-Verordnung – insbesondere in Bezug auf Risikominimierung, Transparenz, Datenqualität und menschliche Aufsicht – systematisch zu adressieren.[7] Damit nimmt Art. 17 eine zentrale Rolle bei der Operationalisierung der regulatorischen Vorgaben ein und hebt die Bedeutung eines strukturierten Managementsystems für die Compliance hervor.[8]

2. Pflicht zur Einführung eines Qualitäts- und Risikomanagementsystems

6 Art. 17 KI-VO verpflichtet Anbieter hochriskanter KI-Systeme zur Einführung, Dokumentation und Aufrechterhaltung eines Qualitäts- und Risikomanagementsystems. Diese Verpflichtung ist nicht optional, sondern zwingend ausgestaltet und stellt eine Grundvoraussetzung für die Inverkehrbringung sowie das Inbetriebhalten solcher Systeme dar.[9] Die Norm adressiert damit die organisatorische Sorgfaltspflicht der Anbieter und verlangt, dass nicht nur das Produkt selbst konform ist, sondern auch die zugrunde liegenden betrieblichen Strukturen geeignet sind, um eine dauerhafte Einhaltung der Verordnung sicherzustellen.[10]

7 Dabei ist zu beachten, dass die KI-Verordnung einen Lebenszyklusansatz verfolgt. Dies bedeutet, dass das Managementsystem alle Phasen des KI-Systems abdecken muss – von der Konzeption über die Entwicklung und Validierung bis hin zur Nutzung, Wartung und gegebenenfalls Außerbetriebnahme.[11] Die Implementierung eines solchen Systems erfordert eine systematische Planung, klare Verantwortlichkeiten, dokumentierte Prozesse und wirksame Kontrollmechanismen, vgl. Art. 17 II KI-VO.

3. Mindestanforderungen an das Managementsystem

8 Art. 17 II KI-VO konkretisiert die Mindestinhalte des geforderten Managementsystems und nennt dabei explizit folgende Elemente:

- Festlegung einer Strategie zur Einhaltung der rechtlichen Anforderungen,
- Verfahren zur Risikobewertung und -minderung,
- Mechanismen zur Überwachung und Bewertung der Leistung des KI-Systems,
- Dokumentation aller relevanten Prozesse und Maßnahmen,
- Verfahren zur Aufrechterhaltung der Compliance über den gesamten Lebenszyklus.

9 Diese Anforderungen sind eng mit den Grundsätzen des Qualitätsmanagements verbunden, wie sie etwa in der ISO 9001 niedergelegt sind.[12] Insbesondere das Prinzip des „Plan-Do-Check-Act"-Zyklus (PDCA-Zyklus) spiegelt sich in der Systematik des Art. 17 KI-VO wider.[13] Es ist daher naheliegend, auf bestehende QM-Standards zurückzugreifen, um die Anforderungen der Verordnung in ein funktionierendes Managementsystem zu überführen.

10 Zugleich geht die KI-Verordnung über die klassischen Qualitätsmanagementaspekte hinaus. Beispielsweise verlangt sie im Bereich der KI-spezifischen Risiken besondere Maßnahmen zur Gewährleistung der Datenqualität, zur Minimierung von Bias[14] und zur Sicherstellung menschlicher Aufsicht, die in allgemeinen QM-Normen bislang nur randständig behandelt werden.[15]

III. Verhältnis zu anderen regulatorischen Pflichten (insbesondere zu Art. 9 KI-VO – Risikomanagement)

11 Ein zentrales Merkmal des Art. 17 KI-VO ist seine enge Verzahnung mit Art. 9 KI-VO. Während Art. 9 die konkrete Risikobewertung und -minderung für das jeweilige KI-System vorschreibt, stellt Art. 17 die organisatorischen Rahmenbedingungen bereit, um diese Anforderungen systematisch umzusetzen. Das Risikomanagementsystem nach Art. 9 ist damit ein Bestandteil des übergeordneten Qualitätsmanagementsystems im Sinne des Art. 17.[16]

12 Dies zeigt sich beispielsweise darin, dass Art. 17 ausdrücklich verlangt, Verfahren zur Durchführung und Dokumentation von Risikobewertungen vorzuhalten. Damit wird ein integrativer Ansatz verfolgt, der nicht nur auf ad hoc durchgeführte Risikoprüfungen setzt, sondern auf eine strukturierte und wiederholbare Einbettung des Risikomanagements in die Unternehmensprozesse.[17]

13 Eine Parallele hierzu besteht im Produktsicherheitsrecht, etwa im Medizinprodukterecht oder in der Maschinenrichtlinie, wo ebenfalls zwischen produktspezifischen Risikobewertungen und den Anforderungen an das Qualitätsmanagementsystem der Hersteller unterschieden wird.[18]

14 Die KI-Verordnung greift diese Logik auf und überträgt sie auf den Bereich der künstlichen Intelligenz, wobei der Fokus nicht nur auf physischen Gefahren, sondern auch auf algorithmischen Risiken liegt. Dazu zählen insbesondere Probleme wie Diskriminierung durch fehlerhafte Trainingsdaten, Intransparenz algorithmischer Entscheidungen (Black-Box-Problematik) sowie fehlende menschliche Kontrolle.[19]

15 Diese Besonderheiten machen es erforderlich, dass das Qualitätsmanagementsystem spezifische Maßnahmen zur Risikoerkennung und -minderung für KI-Systeme enthält, die über die allgemeinen Anforderungen herkömmlicher QM-Standards hinausgehen.

IV. ISO 42001:2023 – AI Management System

1. Struktur und Zielsetzung der Norm

16 Mit der Veröffentlichung der ISO 42001 im Dezember 2023 liegt erstmals ein international anerkannter Standard für ein Managementsystem vor, das speziell auf den Einsatz von Künstlicher Intelligenz ausgerichtet ist.[20] Die Norm versteht sich als Leitfaden für Organisationen, die KI-Systeme entwickeln, bereitstellen oder betreiben, und zielt darauf ab, ein systematisches Rahmenwerk zur Steuerung und Kontrolle von KI-bezogenen Risiken zu schaffen. Ihre Struktur orientiert sich an der sogenannten High Level Structure (HLS), die eine einheitliche Grundstruktur für Managementsystemnormen der ISO darstellt und bereits in der ISO 9001 sowie der ISO 27001 Anwendung findet.[21]

17 Das übergeordnete Ziel der ISO 42001 ist es, Organisationen dabei zu unterstützen, KI-Systeme verantwortungsvoll, sicher und gesetzeskonform zu betreiben. Hierzu definiert die Norm Anforderungen an die Implementierung eines AI Management Systems (AIMS), das alle relevanten

Aspekte des Lebenszyklus von KI-Systemen abdeckt, einschließlich Planung, Implementierung, Überwachung, Bewertung und Verbesserung.[22]

2. Anforderungen an Planung, Umsetzung, Monitoring und kontinuierliche Verbesserung

18 Die ISO 42001 verlangt von Organisationen die Festlegung einer KI-spezifischen Politik, die auf die Einhaltung gesetzlicher und regulatorischer Vorgaben so-

> Söbbing: Die Anforderungen an das Qualitätsmanagement durch die KI-Verordnung (RDi 2025, 337) 340

wie ethischer Grundsätze ausgerichtet ist. Dabei betont die Norm ausdrücklich die Notwendigkeit einer Risikoanalyse, die sowohl technische als auch ethische und soziale Aspekte umfasst.[23]

19 Konkret enthält die Norm Anforderungen an folgende Elemente:

- Definition der KI-bezogenen Ziele und Verpflichtungen,
- Risikoidentifikation und -bewertung hinsichtlich der Entwicklung und Anwendung von KI-Systemen,
- Festlegung angemessener Kontrollen und Maßnahmen zur Risikobehandlung,
- Durchführung interner Audits zur Überprüfung der Systemwirksamkeit,
- Management-Reviews zur systematischen Bewertung der Leistung des AIMS,
- Implementierung von Maßnahmen zur kontinuierlichen Verbesserung.

20 Der PDCA-Zyklus bildet dabei das methodische Rückgrat der Norm. Die Planung („Plan“) umfasst die Definition von Zielen und Prozessen, die Durchführung („Do“) bezieht sich auf die Umsetzung der geplanten Maßnahmen, die Überprüfung („Check“) erfolgt über Monitoring und interne Audits, und die Verbesserung („Act“) umfasst die Ableitung und Umsetzung von Optimierungsmaßnahmen aus den Ergebnissen der Überprüfung.[24]

21 Ein besonderer Fokus der ISO 42001 liegt auf der Berücksichtigung von sogenannten Impact Assessments, die eine Bewertung potenzieller Auswirkungen eines KI-Systems auf Betroffene, Gesellschaft und Umwelt vorsehen. Damit knüpft die Norm an international geführte Diskurse zur menschenzentrierten KI an und unterstützt Anbieter dabei, über die rein technische Perspektive hinausgehende Risiken zu adressieren.[25]

3. Konformitätspotenzial zu Art. 17 KI-VO

22 In Bezug auf die Anforderungen des Art. 17 KI-VO weist die ISO 42001 eine hohe Kompatibilität auf. Insbesondere die systematische Verankerung von Risikomanagementprozessen, die Dokumentationspflichten und die Pflicht zur kontinuierlichen Überprüfung und Verbesserung decken sich mit den Mindestanforderungen der Verordnung. Dies betrifft insbesondere die Anforderungen an:

- Lebenszyklusorientiertes Risikomanagement,
- Festlegung klarer Verantwortlichkeiten und Zuständigkeiten,
- Dokumentation und Nachvollziehbarkeit der Entscheidungsfindung,
- Monitoring und Anpassung bei veränderten Rahmenbedingungen.

23 Allerdings bleibt festzuhalten, dass auch die ISO 42001 kein unmittelbares regulatorisches Konformitätsversprechen in Bezug auf die KI-Verordnung abgibt. Die Norm stellt vielmehr ein flexibles Rahmenwerk zur Verfügung, das von den Anwendern entsprechend angepasst und

konkretisiert werden muss, um die spezifischen Anforderungen des europäischen Rechtsrahmens – etwa hinsichtlich Bias Detection, Transparenz und Human Oversight – vollständig abzubilden.[26]

24 Gleichwohl ist die ISO 42001 aufgrund ihres dezidierten KI-Fokus und ihrer systematischen Ausrichtung auf Risikomanagement und Compliance ein geeignetes Instrument, um die Anforderungen des Art. 17 KI-VO zumindest weitgehend operativ umzusetzen und zu flankieren. Eine vollständige Compliance-Prüfung erfordert jedoch in jedem Fall eine ergänzende rechtliche Bewertung und gegebenenfalls zusätzliche Maßnahmen außerhalb des Rahmens der Norm.

V. ISO 9001:2015 – Qualitätsmanagementsysteme

1. Grundlagen und Anwendungsbereich

25 Die ISO 9001:2015 stellt den weltweit am weitesten verbreiteten Standard für Qualitätsmanagementsysteme (QMS) dar. Ihr Ziel ist es, Organisationen bei der Fähigkeit zu unterstützen, konsistent Produkte und Dienstleistungen bereitzustellen, die den Anforderungen der Kunden sowie anwendbaren rechtlichen und regulatorischen Anforderungen entsprechen.[27] Die Norm folgt einem prozessorientierten Ansatz und basiert auf den Grundsätzen des Qualitätsmanagements, darunter Kundenorientierung, Führung, Engagement von Personen, prozessorientierter Ansatz, Verbesserung, faktengestützte Entscheidungsfindung sowie Beziehungsmanagement.[28]

26 Die Norm richtet sich nicht an spezifische Branchen oder Produkttypen, sondern ist branchenübergreifend anwendbar und flexibel ausgestaltbar. Ihre Hauptstärke liegt in der Standardisierung betrieblicher Abläufe und in der systematischen Verankerung von Qualitätssicherung über alle Prozesse hinweg.

2. Relevanz für die Qualitätsanforderungen aus Art. 17 KI-VO

27 Obwohl die ISO 9001 keinen spezifischen Bezug zu KI-Systemen oder algorithmischen Risiken enthält,

> Söbbing: Die Anforderungen an das Qualitätsmanagement durch die KI-Verordnung 341 (RDi 2025, 337)

bietet sie ein solides Grundgerüst für das Qualitätsmanagement, das auch für die Umsetzung von Art. 17 KI-VO genutzt werden kann. Besonders relevant sind dabei die folgenden Aspekte:

- die Definition des Anwendungsbereichs des Managementsystems (ISO 9001:2015, Abschnitt 4),
- die Verpflichtung zur Führung und zur Festlegung von Rollen, Verantwortlichkeiten und Befugnissen (Abschnitt 5),
- das Risikobasierte Denken im Rahmen der Planung (Abschnitt 6),
- die operative Steuerung und die Anforderung an dokumentierte Informationen (Abschnitt 8),
- sowie das Monitoring, die Bewertung und die kontinuierliche Verbesserung (Abschnitte 9 und 10).

28 Diese Elemente entsprechen in ihrer Zielrichtung weitgehend den strukturellen Anforderungen, wie sie Art. 17 KI-VO für das Qualitätsmanagement bei hochriskanten KI-Systemen fordert, auch wenn sie KI-spezifische Problemstellungen wie Bias Detection oder Transparenz nicht ausdrücklich adressieren.[29]

29 Besondere Bedeutung hat das in ISO 9001 verankerte Prinzip des risikobasierten Denkens, das verlangt, dass Organisationen Risiken und Chancen, die die Zielerreichung des Qualitätsmanagementsystems beeinflussen können, identifizieren und angemessene Maßnahmen

festlegen.[30] Diese Verpflichtung lässt sich als methodische Grundlage nutzen, um auch KI-spezifische Risiken in das Qualitätsmanagementsystem einzubetten.

3. Stärken und Grenzen der ISO 9001 im Kontext KI

30 Die wesentliche Stärke der ISO 9001 liegt in ihrer universellen Anwendbarkeit und in der etablierten Methodik zur Prozessgestaltung und -verbesserung. Dies erleichtert es, Prozesse zur Risikobewertung und -minderung sowie zur Dokumentation und Überwachung in ein bestehendes Managementsystem zu integrieren.

31 Jedoch zeigt sich zugleich, dass die ISO 9001 den spezifischen Anforderungen der KI-Verordnung, insbesondere hinsichtlich algorithmischer Risiken, datenethischer Fragestellungen und Bias Management, nicht vollumfänglich gerecht wird. Auch Aspekte wie Human Oversight, Nachvollziehbarkeit algorithmischer Entscheidungen oder Maßnahmen zur Sicherstellung der Trainingsdatenqualität sind in der Norm nicht explizit geregelt.[31]

32 Daher ist es für Anbieter hochriskanter KI-Systeme erforderlich, die ISO 9001 entweder um entsprechende KI-spezifische Leitlinien zu ergänzen oder diese mit Normen wie der ISO 42001 zu kombinieren, um die regulatorischen Anforderungen aus Art. 17 KI-VO umfassend abzudecken.

33 Die ISO 9001 kann dabei insbesondere die übergreifenden Managementstrukturen und das Qualitätsbewusstsein innerhalb der Organisation stärken und so ein Fundament für die Umsetzung der spezialisierten KI-bezogenen Anforderungen bilden. Sie ist somit ein wichtiges, aber nicht hinreichendes Element im Rahmen eines Compliance-konformen Qualitätsmanagementsystems nach KI-Verordnung.

VI. ISO 27001:2022 – Informationssicherheitsmanagement

1. Schutz von Informationssicherheit als Compliance-Faktor

34 Die ISO 27001:2022 bildet den internationalen Standard für Informationssicherheitsmanagementsysteme (ISMS) und stellt ein strukturiertes Rahmenwerk zur Verfügung, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sicherzustellen.[32] Sie adressiert damit zentrale Compliance-Anforderungen, die auch für hochriskante KI-Systeme von großer Bedeutung sind, insbesondere wenn diese auf sensible Daten angewiesen sind, etwa bei der Verarbeitung personenbezogener Daten, Gesundheitsinformationen oder bei sicherheitskritischen Anwendungen.

35 Das Managementsystem nach ISO 27001 basiert ebenfalls auf dem prozessorientierten Ansatz und folgt dem PDCA-Zyklus. Es enthält Anforderungen an die Risikobewertung und -behandlung, an die Etablierung von Sicherheitsrichtlinien, an das Asset Management sowie an den Schutz vor Bedrohungen durch interne und externe Akteure.[33] Die Norm fordert, dass Organisationen die relevanten Informationswerte identifizieren, Risiken bewerten und geeignete Maßnahmen zur Risikobehandlung umsetzen.

2. Bezug zu Art. 17 KI-VO im Hinblick auf Risikomanagement und Dokumentation

36 Der Bezug der ISO 27001 zu Art. 17 KI-VO ergibt sich vor allem aus zwei zentralen Schnittstellen: dem Risikomanagement und der Dokumentationspflicht. Beide Elemente sind für die Erfüllung der Anforderungen des Art. 17 KI-VO von erheblicher Relevanz. Insbesondere die Forderung der KI-Verordnung, ein Managementsystem einzuführen, das Risiken identifiziert, bewertet und angemessen adressiert, korrespondiert mit dem risikobasierten Ansatz der ISO 27001.

37 Die Norm verlangt detaillierte Verfahren zur Identifikation von Informationssicherheitsrisiken, zur Bestimmung der Eintrittswahrscheinlichkeit und Auswirkung dieser Risiken sowie zur Auswahl

geeigneter Risikominderungsmaßnahmen.[34] Diese Methodik lässt sich problemlos auch auf KI-spezifische Risiken übertragen, etwa im Hinblick auf Manipulationen von Trainingsdaten (Data Poisoning), Angriffe auf Modelle (Model Inversion, Adversarial Attacks) oder unautorisierte Zugriffe auf kritische Systemkomponenten.

38 Zudem stellt die ISO 27001 strenge Anforderungen an die Dokumentation sämtlicher sicherheitsrelevanter Prozesse. Diese Anforderung deckt sich mit der Pflicht zur vollständigen Prozessdokumentation, wie sie Art. 17 KI-VO für das Qualitäts- und Risikomanagement vorschreibt.[35] Gerade im Hinblick auf die Nachvollziehbarkeit von Entscheidungen und die Auditierbarkeit der Compliance kann dies ein entscheidender Beitrag zur Umsetzung der regulatorischen Anforderungen sein.

3. Ergänzungspotenzial zur ISO 42001 und ISO 9001

39 Die besondere Stärke der ISO 27001 im Vergleich zu den anderen beiden hier betrachteten Normen liegt in ihrem dezidierten Fokus auf Informationssicherheit. Während die ISO 9001 primär auf die Produkt- und Prozessqualität und die ISO 42001 auf KI-spezifische Managementprozesse zielen, ergänzt die ISO 27001 diese Perspektive um den Aspekt der Sicherheitsarchitektur.

40 Im Zusammenspiel mit ISO 42001 und ISO 9001 kann die ISO 27001 insbesondere dazu beitragen, die Anforderungen der KI-Verordnung hinsichtlich Datenqualität und Datenintegrität umfassend abzusichern. Dies betrifft nicht nur den Schutz der Trainings- und Validierungsdaten, sondern auch die Sicherstellung der Verfügbarkeit und Unverfälschtheit der Modelle und Outputs während des Betriebs.[36]

41 Darüber hinaus bietet die ISO 27001 einen Katalog an organisatorischen und technischen Kontrollen (Annex A), die je nach Risikobewertung ausgewählt und implementiert werden können. Hierzu zählen unter anderem Zugangskontrollen, Verschlüsselung, Protokollierung, Incident Management und Maßnahmen zur Sicherstellung der Betriebskontinuität.[37] Diese Instrumente können im Rahmen eines integrierten Managementsystems auch zur Erfüllung der Anforderungen aus Art. 17 KI-VO herangezogen werden, insbesondere dort, wo der Schutz vor Manipulationen und Missbrauch von KI-Systemen gewährleistet sein muss.

42 Gleichwohl ist die ISO 27001, ebenso wie die anderen betrachteten Normen, kein vollständiger Ersatz für eine gezielte Umsetzung der KI-Verordnung. Sie bildet jedoch ein tragfähiges Fundament für die Absicherung des Informationsflusses innerhalb von KI-gestützten Prozessen und leistet einen wichtigen Beitrag zur Erfüllung der regulatorischen Anforderungen.

VII. Bewertung der Normenkombination für die Erfüllung von Art. 17 KI-VO

1. Synergien zwischen ISO 42001, ISO 9001 und ISO 27001

43 Die Kombination der ISO 42001, ISO 9001 und ISO 27001 bietet eine umfassende Grundlage zur Umsetzung der Anforderungen aus Art. 17 KI-VO. Während die ISO 9001 die allgemeine Prozessqualität sicherstellt und die ISO 27001 die Informationssicherheitsaspekte adressiert, ergänzt die ISO 42001 diese Perspektiven um KI-spezifische Fragestellungen wie Bias Management, Impact Assessments und human oversight.[38] Durch diese komplementären Schwerpunkte ergibt sich ein integratives Managementsystem, das sowohl die regulatorischen Vorgaben als auch ethische und technische Anforderungen systematisch abbilden kann.

44 Besonders hervorzuheben ist die Möglichkeit, die Risikomanagementmethodik der ISO 9001 und 27001 mit den speziellen Anforderungen der ISO 42001 zu verknüpfen. Dies ermöglicht es, klassische betriebliche Risiken, Informationssicherheitsrisiken und KI-spezifische Risiken im Rahmen eines einheitlichen Risikomanagementsystems zu erfassen und zu steuern.[39]

45 Darüber hinaus profitieren Organisationen von der gemeinsamen HLS-Struktur der drei Normen, die eine einfachere Integration der verschiedenen Managementsysteme erlaubt. Synergieeffekte können

etwa durch gemeinsame interne Audits, konsolidierte Management-Reviews oder integrierte Dokumentationssysteme erzielt werden.[40]

2. Lücken und spezifische Anforderungen der KI-Verordnung

46 Trotz der genannten Synergien verbleiben relevante Lücken zwischen den ISO-Normen und den spezifischen Anforderungen der KI-Verordnung. Insbesondere adressieren weder ISO 9001 noch ISO 27001 explizit die Anforderungen an Bias Detection, Erklärbarkeit („explainability") algorithmischer Entscheidungen oder

menschliche Aufsichtspflichten („human oversight") in der Tiefe, wie sie Art. 17 iVm Art. 9 und Art. 14 KI-VO verlangt.[41]

47 Auch die Anforderung an eine systematische Überprüfung der eingesetzten Datensätze auf Repräsentativität und Eignung (Art. 10 KI-VO) sowie die Verpflichtung zur Gewährleistung der Transparenz gegenüber den Nutzern (Art. 13 KI-VO) sind in den betrachteten Normen nur unzureichend abgebildet. Hier besteht Anpassungsbedarf innerhalb des Qualitäts- und Risikomanagementsystems, um die regulatorischen Anforderungen vollumfänglich umzusetzen.[42]

48 Zusätzlich bleibt zu beachten, dass die KI-Verordnung selbst keine Zertifizierungspflicht nach ISO-Normen vorsieht, sondern ausschließlich die tatsächliche Wirksamkeit der getroffenen Maßnahmen verlangt. Eine formale Zertifizierung kann daher nur Indizwirkung haben und ersetzt nicht die eigenständige Prüfung der Compliance durch die zuständigen Behörden, vgl. § 17 II KI-VO.

3. Rechtliche Bewertung: Reicht Zertifizierung zur Erfüllung der Verordnungspflichten aus?

49 Aus juristischer Perspektive stellt sich die Frage, ob die Einführung und Zertifizierung eines Managementsystems nach ISO 42001, 9001 und 27001 allein geeignet ist, den Anforderungen des Art. 17 KI-VO zu genügen. Dabei ist zu berücksichtigen, dass die Verordnung eine substanzielle Compliance-Pflicht fordert, deren Erfüllung an der tatsächlichen Wirksamkeit der Prozesse gemessen wird.[43] Eine Zertifizierung kann im Rahmen der Compliance-Verteidigung („compliance defense") eine erhebliche Indizwirkung entfalten, vermag aber nicht automatisch die Haftung auszuschließen.

50 Die Rechtsprechung zur Produktsicherheit und zur Compliance in anderen Rechtsbereichen legt nahe, dass Zertifizierungen als ein Element ordnungsgemäßer Organisation angesehen werden können, sofern sie durch wirksame interne Prozesse flankiert werden.[44] Auch die KI-Verordnung knüpft an diesen Maßstab an, indem sie neben der formalen Etablierung eines Qualitätsmanagementsystems die konkrete Risikominimierung sowie deren Überprüfung fordert.

51 Die alleinige Implementierung eines zertifizierten Managementsystems ohne tatsächliche Risikoanalyse und wirksame Maßnahmen zur Risikobeherrschung genügt daher nicht, um die Anforderungen der KI-Verordnung zu erfüllen. Entscheidend ist vielmehr die inhaltliche Ausgestaltung der Prozesse, deren Wirksamkeit und die Fähigkeit der Organisation, auf neue Risiken oder Veränderungen des Systems angemessen zu reagieren.[45]

52 Damit ergibt sich, dass eine Zertifizierung nach ISO 42001, ISO 9001 und ISO 27001 ein wichtiger Bestandteil einer Compliance-Strategie im Bereich KI sein kann, jedoch keine vollständige Entlastung von der Verantwortung für die Umsetzung der Verordnungspflichten bewirkt. Eine kritische Auseinandersetzung mit den spezifischen Anforderungen der KI-Verordnung und deren praktische Umsetzung bleibt unerlässlich.

VIII. CEN/CENELEC JTC21

53 Eine Konkretisierung der technischen und prozessualen Anforderungen an das QMS erfolgt jedoch nicht im Normtext selbst, sondern über die Rückbindung an harmonisierte Normen iSv Art. 40 KI-VO sowie über sogenannte gemeinsame Spezifikationen iSv Art. 41 KI-VO.

1. Erstellung harmonisierter Normen gem. Art. 40 KI-VO

54 Die Erstellung harmonisierter Normen ge. Art. 40 KI-VO obliegt den beiden europäischen Normungsorganisationen CEN (Comité Européen de Normalisation) und CENELEC (Comité Européen de Normalisation Électrotechnique), denen nationale Normungsinstitute wie DIN (Deutschland), AFNOR (Frankreich) oder BSI (UK, bis Brexit) als Mitglieder angehören.[46] Die Zuweisung der Zuständigkeit für die Ausarbeitung harmonisierter Normen im Sinne des Art. 40 KI-VO an die europäischen Normungsorganisationen CEN und CENELEC ergibt sich streng juristisch aus einem mehrstufigen Zusammenspiel von Primärrecht, sektorspezifischem Sekundärrecht sowie einschlägigen Durchführungsrechtsakten der Europäischen Kommission. Die Grundlage für die europäische Normung bildet Verordnung (EU) Nr. 1025/2012 über die europäische Normung, dabei definiert Art. 2 Nr. 1 definiert: „Europäische Norm" ist eine von einer der anerkannten europäischen Normungsorganisationen angenommene Norm: CEN, CENELEC oder ETSI.[47]

55 „Europäische Norm" ist eine von einer der anerkannten europäischen Normungsorganisationen angenommene Norm: CEN, CENELEC oder ETSI. Gem. Art. 10 I der Verordnung (EU) 1025/2012 kann die Kommission diesen Organisationen sog. Normungsaufträge (Standardisation Requests) erteilen, um „harmo-

nisierte Normen" für die Zwecke der Unionsharmonisierungsvorschriften zu entwickeln.[48]

56 Ein zentrales Gremium für die Entwicklung entsprechender Normen im Bereich künstlicher Intelligenz ist das Joint Technical Committee CEN/CLC JTC 21 mit dem formalen Titel:[49]

„*Artificial Intelligence – Horizontal aspects*"

57 Dieses Komitee wurde 2021 gegründet und ist ausdrücklich zuständig für die Entwicklung horizontaler Normen im KI-Bereich – also solcher, die branchenübergreifend anwendbar sind. Die Zielsetzung besteht darin, aufbauend auf den Arbeiten des internationalen ISO/IEC-Komitees JTC 1/SC 42 europäisch konsistente, an der KI-Verordnung ausgerichtete Normen zu entwickeln. Besonders relevant sind hier unter anderem:

- EN ISO/IEC 42001 (KI-Managementsysteme)
- EN ISO/IEC 23894 (Risikomanagement für KI-Systeme)
- EN ISO/IEC 5338 (AI lifecycle management)

58 Diese Normen dienen als Referenz für die Umsetzung der Anforderungen aus Art. 17 KI-VO, etwa hinsichtlich Dokumentationspflichten, Auditverfahren, Rollenverantwortlichkeit und Prozessen des Lebenszyklusmanagements.[50]

59 Die nationale Beteiligung an Normungsprozessen erfolgt dabei über Spiegelgremien, in denen Vertreter aus Wirtschaft, Wissenschaft und Verwaltung mitwirken (im Falle des JTC 21 über das DIN/DKE Gremium NA 043-04-41 AA). Durch diese Struktur wird die Beteiligung maßgeblicher Interessenträger institutionalisiert und zugleich sichergestellt, dass nationale Belange und spezifische technische Rahmenbedingungen aus deutscher Sicht wirksam in den europäischen Normungsprozess eingespeist werden.

2. Die Umsetzung der Anforderungen aus Art. 17 KI-VO durch ISO/IEC 42001, 23894 und 5338

60 Aktuell sind die Normen ISO/IEC 42001, ISO/IEC 23894 und ISO/IEC 5338 (noch) nicht als harmonisierte Normen im Sinne des Art. 40 KI-VO anerkannt.[51] Sie können daher de lege lata keine Konformitätsvermutung im Sinne von Art. 40 II KI-VO auslösen.[52] Dennoch stellt sich die Frage, ob ihre Anwendung gleichwohl inhaltlich geeignet ist, die Anforderungen aus Art. 17 KI-VO zu erfüllen.

a) EN ISO/IEC 42001 – Managementsysteme für Künstliche Intelligenz

61 Siehe hierzu die Ausführungen in Abschnitt IV.

b) EN ISO/IEC 23894 – Risikomanagement für KI-Systeme

62 Diese Norm ergänzt ISO 42001um ein spezifisches Rahmenwerk für Risikomanagement in KI-Systemen und ist als „vertical extension" der allgemeinen Risikomanagementnorm ISO 31000 zu verstehen.[53] Die ISO/IEC 23894 fordert u. a.:

- eine strukturierte Risikoidentifikation für KI-spezifische Risiken,
- Berücksichtigung von Bias, Erklärbarkeit und Transparenz,
- Dokumentation und Nachvollziehbarkeit von Risikoentscheidungen.

63 Damit erfüllt sie grundsätzlich die Anforderungen aus Art. 17 II Buchst. a, b und g KI-VO (Risikomanagementverfahren, Datenverarbeitung und Kontrolle, sowie Korrekturmaßnahmen) und konkretisiert das von Art. 9 KI-VO ebenfalls geforderte Risikomanagement.

c) EN ISO/IEC 5338 – AI-Lifecycle Management

64 Die jüngere ISO/IEC 5338[54] widmet sich dem vollständigen Lebenszyklusmanagement von KI-Systemen – von der Idee über Entwicklung und Einsatz bis zur Stilllegung. Sie legt systematisch fest:

- Phasenstruktur (Planung – Entwicklung – Bereitstellung – Betrieb – Einstellung),
- Rollen und Verantwortlichkeiten,
- Anforderungen an Schnittstellenmanagement, Überwachung und Validierung.

65 Die Norm bietet damit eine strukturierte operationalisierbare Auslegung von Art. 17 II Buchst. a, e und f KI-VO, indem sie organisatorische Prozesse und Zuständigkeiten über den gesamten Lebenszyklus definiert.[55]

66 Auch wenn diese Norm (noch) nicht als harmonisierte Norm gilt, ist sie zur Erfüllung der Dokumentations- und Nachweispflichten aus Art. 17 iVm Art. 11 KI-VO einer technischen Dokumentation geeignet.

IX. Resümee

67 Die Analyse der Anforderungen des Art. 17 KI-VO und deren mögliche Umsetzung über die Normen

ISO 42001, ISO 9001 und ISO 27001 zeigt deutlich, dass ein integriertes Managementsystem einen wesentlichen Beitrag zur Einhaltung der regulatorischen Pflichten leisten kann. Dabei fungieren die genannten ISO-Standards als strukturgebende Instrumente, die es ermöglichen, Risikomanagement, Qualitätsmanagement und Informationssicherheit systematisch zu organisieren und zu dokumentieren.

68 Besonders die ISO 42001 bietet mit ihrem KI-spezifischen Fokus ein praxisnahes Rahmenwerk, um die besonderen Anforderungen der KI-Verordnung – etwa hinsichtlich Bias Management, Transparenz und human oversight – zu operationalisieren. In Kombination mit den prozessorientierten Strukturen der ISO 9001 sowie den Sicherheitsarchitekturen der ISO 27001 ergibt sich ein robustes Fundament für ein Compliance-gerechtes Management hochriskanter KI-Systeme.

69 Gleichwohl verbleiben Regelungslücken, die durch die Normen allein nicht geschlossen werden können. Die KI-Verordnung setzt über die strukturellen Anforderungen hinaus auch inhaltliche Maßstäbe, etwa hinsichtlich der Qualität und Eignung von Trainingsdaten, der Gewährleistung menschlicher Kontrolle oder der Vermeidung systematischer Diskriminierung. Diese Aspekte erfordern eine vertiefte Auseinandersetzung, die über das hinausgeht, was die betrachteten ISO-Normen unmittelbar leisten können. Die bloße Existenz eines zertifizierten Managementsystems genügt nicht, um die Compliance sicherzustellen. Vielmehr ist die tatsächliche Wirksamkeit der getroffenen Maßnahmen und deren kontinuierliche Überprüfung ausschlaggebend.

70 Vor diesem Hintergrund erscheint es sinnvoll, ergänzend zu den bestehenden ISO-Normen branchenspezifische Leitlinien und sektorspezifische Standards zu entwickeln, die die regulatorischen Vorgaben der KI-Verordnung konkretisieren und in die betriebliche Praxis im Sinne AI-Governance überführen. Auch eine Weiterentwicklung der ISO 42001 in Richtung einer engeren Anlehnung an die Anforderungen der KI-Verordnung könnte zur weiteren Harmonisierung beitragen.

71 Zukünftig wird sich zudem die Frage stellen, ob europäische oder nationale Behörden die Zertifizierung nach ISO 42001, ISO 9001 oder ISO 27001 als Teil der Konformitätsbewertung im Sinne der KI-Verordnung offiziell anerkennen werden. Eine solche Entwicklung könnte sowohl die Rechtssicherheit für Anbieter erhöhen als auch die behördliche Kontrolle erleichtern.

72 Art. 17 KI-VO entfaltet seine praktische Wirksamkeit auch im Zusammenspiel mit den Art. 40 und 41 KI-VO und der darauf aufbauenden europäischen Normungsstruktur. Die technischen Detailanforderungen an das QMS von Anbietern Hochrisiko-KI-Systemen werden dabei im Wesentlichen vom CEN/CLC JTC 21 formuliert und durch das DIN in deutsches Normenrecht überführt. Die hieraus resultierenden Normen (zB DIN EN ISO/IEC 42001) stellen faktisch den maßgeblichen Prüfungsmaßstab für regulatorische Konformität dar. Unternehmen, die sich an diesen Normen orientieren, können sich auf eine rechtlich anerkannte Konformitätsvermutung stützen.

73 Dies verdeutlicht die Untrennbarkeit rechtlicher und technischer Regulierung im Bereich der KI-Governance: Der Gesetzgeber gibt mit Art. 17 KI-VO die Leitplanken vor – die technische Ausgestaltung erfolgt durch europäische und nationale Normungsgremien, deren Arbeit für Rechtsanwender faktisch bindend ist.

74 Abschließend lässt sich festhalten, dass die Verknüpfung von Qualitätsmanagement, Risikomanagement und Informationssicherheit im Lichte der KI-Verordnung ein zentraler Bestandteil einer effektiven Compliance-Strategie sein muss. Die Nutzung der bestehenden ISO-Standards bietet hierfür ein bewährtes Instrumentarium, das jedoch einer kritischen Prüfung und Anpassung an die spezifischen Anforderungen der KI-Verordnung bedarf. Nur so kann gewährleistet werden, dass KI-Systeme nicht nur formal, sondern auch materiell den Anforderungen an Sicherheit, Vertrauenswürdigkeit und Rechtskonformität genügen.

---

* Der Autor, LL. M. (HHU), hat eine Professur für Zivilrecht mit dem Recht der Digitalen Wirtschaft an der Hochschule Kaiserslautern. Alle Internetquellen wurden zuletzt am 17.6.2025 aufgerufen.

1 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 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.

2 Wendt/Wendt Das neue Recht der künstlichen Intelligenz, 1. Aufl. 2024, § 6 Rn. 6 f.

3

Autor: ISO Technical Committee JTC 1/SC 42, abrufbar unter https://www.iso.org/news/ref2865.html.

4 Art. 17 I KI-VO; BeckOK KI-Recht/Henke, 2. Ed. 1.5.2025, KI-VO Art. 17 Rn. 3.

5 Wendt/Wendt Das neue Recht der künstlichen Intelligenz, 1. Aufl. 2024, § 6 Rn. 6 f.

6 KI-VO ErwGr. 48 – Zweck des Qualitätsmanagementsystems.

7 KI-VO ErwGr. 48 – Zweck des Qualitätsmanagementsystems.

8 Martini/Wendehorst/Eisenberger, 1. Aufl. 2024, KI-VO Art. 16 Rn. 21.

9 Art. 17 I KI-VO; BeckOK KI-Recht/ Henke, 2. Ed. 1.5.2025, KI-VO Art. 17 Rn. 3.

10 KI-VO ErwGr. 48 – Zweck des Qualitätsmanagementsystems.

11 BeckOK KI-Recht/ Henke, 2. Ed. 1.5.2025, KI-VO Art. 17 Rn. 4.

12 ISO 9001:2015, Abschnitt 4 ff.

13 Der „Plan-Do-Check-Act"-Zyklus (PDCA-Zyklus) ist ein iteratives Managementmodell zur kontinuierlichen Verbesserung von Prozessen und Systemen, insbesondere im Rahmen von Qualitätsmanagementsystemen. Er ist zentraler Bestandteil vieler Normen, insbesondere der ISO 9001, ISO 14001 und auch der ISO/IEC 42001:2023, abrufbar unter https://www.iso.org/standard/62085.html.

14 Die Verzerrung oder auch das Bias oder systematischer Fehler einer Schätzfunktion ist in der Schätztheorie, einem Teilgebiet der mathematischen Statistik, diejenige Kennzahl oder Eigenschaft einer Schätzfunktion, welche die systematische Über- oder Unterschätzung der Schätzfunktion quantifiziert, vgl. Georgii Stochastik, 2009, S. 207.

15 BeckOK KI-Recht/Henke, 2. Ed. 1.5.2025, KI-VO Art. 17 Rn. 5

16 Wendt/Wendt Das neue Recht der künstlichen Intelligenz, 1. Aufl. 2024, § 6 Rn. 6 f.

17 Art. 17 II Buchst. b KI-VO.

18 Vgl. zB § 30 MPG aF, Art. 10 MDR (EU) 2017/745.

19 BeckOK KI-Recht/Henke, 2. Ed. 1.5.2025, KI-VO Art. 17 Rn. 5.

20 ISO 42001:2023, Introduction.

21 ISO 42001:2023, Introduction; vgl. auch ISO 9001:2015 und ISO 27001:2022, Einleitung.

22 ISO/IEC 42001:2023, Managementsysteme für künstliche Intelligenz.Verweist mehrfach auf den PDCA-Zyklus als konzeptionelle Grundlage, abrufbar unter https://www.iso.org/standard/81230.html.

23 ISO 42001:2023, Abschnitt 4 ff.

24 ISO 42001:2023, Abschnitt 4 ff.; zum PDCA-Zyklus vgl. auch ISO 9001:2015, Anhang A.

25 ISO 42001:2023, Abschnitt 6.1.3.

26 BeckOK KI-Recht/Henke, 2. Ed. 1.5.2025. KI-VO Art. 17 Rn. 6

27 ISO 9001:2015, Introduction.

28 ISO 9001:2015, Anhang B.

29 BeckOK KI-Recht/Henke, 2. Ed. 1.5.2025, KI-VO Art. 17 Rn. 7.

30 ISO 9001:2015, Abschnitt 6.1.

31 ISO 9001:2015, Abschnitt 6.1; BeckOK KI-Recht/Henke, 2. Ed. 1.5.2025, KI-VO Art. 17 Rn. 7.

32 ISO 27001:2022, Introduction.

33 ISO 27001:2022, Abschnitt 6 ff.

34 ISO 27001:2022, Abschnitt 6 ff.

35 Art. 17 II Buchst. b KI-VO.

36 BeckOK KI-Recht/Henke, 2. Ed. 1.5.2025, KI-VO Art. 17 Rn. 8.

37 ISO 27001:2022, Annex A.

38 ISO 42001:2023, Abschnitt 6 ff.

39 ISO 9001:2015, Abschnitt 6; ISO 27001:2022, Abschnitt 6.

40 Vgl. ISO 9001:2015, Annex SL.

41 BeckOK KI-Recht/Henke, 2. Ed. 1.5.2025, KI-VO Art. 17 Rn. 9.

42

BeckOK KI-Recht/Henke, 2. Ed. 1.5.2025, KI-VO Art. 17 Rn. 9; vgl. auch Art. 10 und Art. 13 KI-VO.

43 Art. 17 II KI-VO.

44 Vgl. BGH NJW 2008, 3770.

45 BeckOK KI-Recht/Henke, 2. Ed. 1.5.2025, KI-VO Art. 17 Rn. 10.

46 BeckOK KI-Recht/Kilian, 1. Ed. 1.1.2025, KI-VO Art. 40 Rn. 12-15.

47 Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 über die europäische Normung, ABl. L 316 vom 14.11.2012, S. 12–33, insbesondere Art. 2 Nr. 1 und Nr. 6 iVm Anhang I.

48 BeckOK KI-Recht/Kilian, 1. Ed. 1.1.2025, KI-VO Art. 40 Rn. 12-15.

49 CEN/CLC JTC 21, Artificial Intelligence – Horizontal aspects, Mandat und Arbeitsprogramme, Stand: Mai 2025, abrufbar unter: https://standards.cencenelec.eu.

50 BeckOK KI-Recht/Henke, 2. Ed. 1.5.2025, KI-VO Art. 17 Rn. 20.

51 KI-VO ErwGr. 77-78 zur Rolle von Normung und QM-Systemen.

52 BeckOK KI-Recht/Kilian, 1. Ed. 1.1.2025, KI-VO Art. 40 Rn. 12-15.

53 Vgl. ISO TC 262 / JTC 1/SC 42 (AI) – Risikomanagement für KI.

54 aktueller Status: Draft international standard (DIS, seit 2024).

55 BeckOK KI-Recht/Henke, 2. Ed. 1.5.2025, KI-VO Art. 17 Rn. 15 ff.