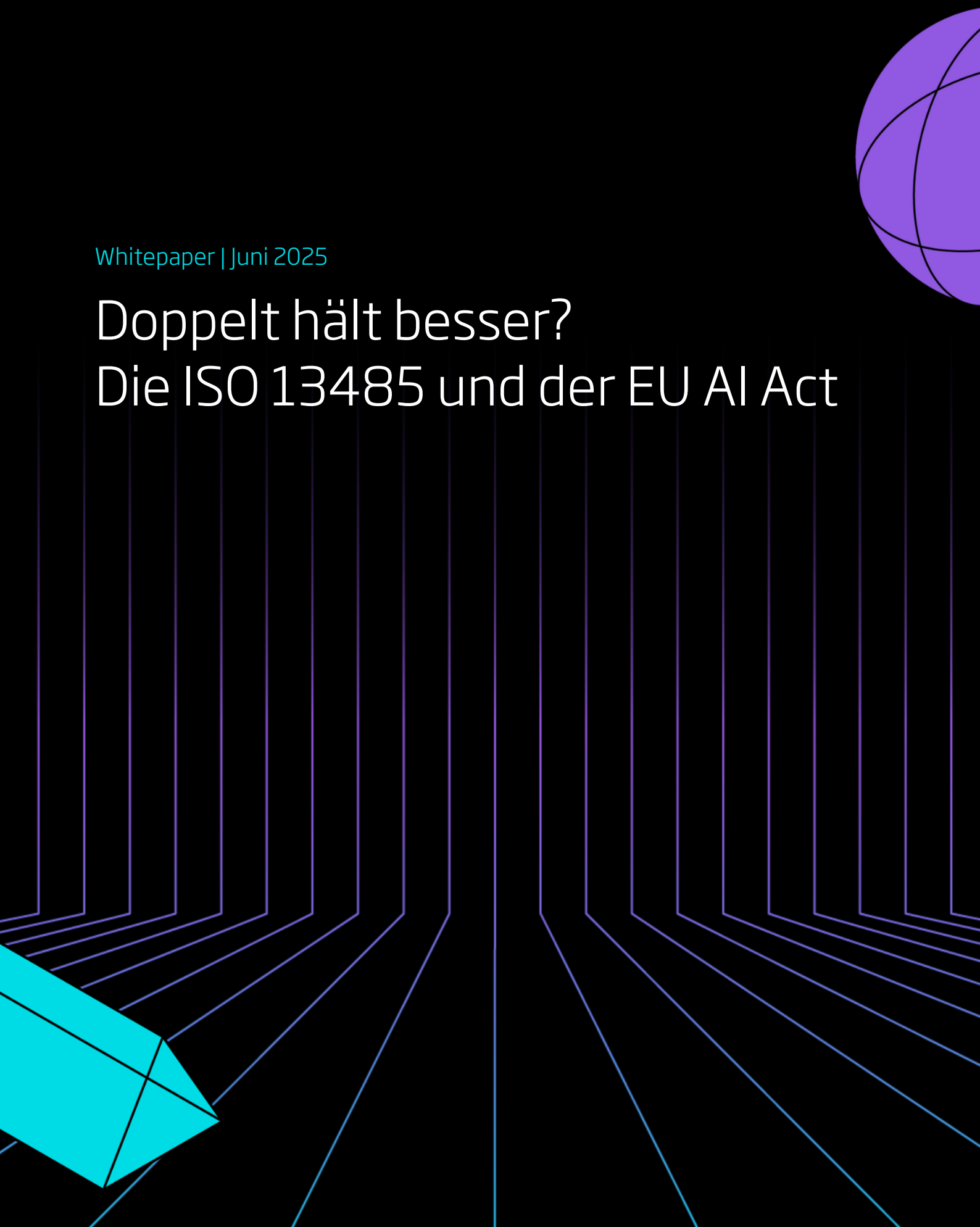
TÜV AI.LAB

Whitepaper | Juni 2025

Doppelt hält besser? Die ISO 13485 und der EU AI Act



Executive Summary

Künstliche Intelligenz hat längst Einzug in die Medizintechnik gehalten – ihr volles Marktpotenzial steht aber noch am Anfang. Ein zentraler Grund: Die regulatorischen Anforderungen an Hochrisiko-Anwendungen sind hoch. Neben den Pflichten der Medical Device Regulation (MDR) verlangt nun auch der europäische AI Act (EU 2024/1689) ein umfassendes Qualitätsmanagementsystem für Hochrisiko-KI-Systeme.

Dieses Whitepaper untersucht, inwieweit die ISO 13485 – als etablierte Norm für Medizinprodukte – die neuen Anforderungen des AI Act erfüllt. Dabei zeigt sich: Viele Vorgaben aus Artikel 17 AIA, etwa zur Entwicklung, Qualitätssicherung oder Behördenkommunikation, sind bereits umfassend adressiert. Doch gerade KI-spezifische Aspekte wie Datenmanagement oder KI-bezogenes Risikomanagement sind nicht per se abgedeckt.

Die gute Nachricht: Es bedarf keiner kompletten Neuentwicklung eines zweiten Qualitätsmanagementsystems (QMS). Stattdessen lassen sich bestehende ISO-13485-Systeme gezielt erweitern. Damit können Unternehmen regulatorische Anforderungen erfüllen, ohne doppelte Strukturen aufzubauen.

Das Whitepaper bietet eine praxisorientierte Orientierung für Hersteller, die sich im Spannungsfeld zwischen MDR und AI Act bewegen, und zeigt, wie ein evolutionär weiterentwickeltes QMS zur Brücke zwischen zwei Regularien werden kann.

QMS – A New Era?

KI-Systeme sind längst Bestandteil innovativer Medizinprodukte, und ihr Potenzial ist groß: Sie helfen Muster in Bilddaten zu erkennen, Diagnoseprozesse effizienter zu gestalten oder Therapieentscheidungen zu unterstützen. Für das regelmäßig überlastete medizinische Fachpersonal bietet das Unterstützung, Erleichterung und die Chance auf Effizienzgewinne sowie qualitative Konsistenz. Dennoch ist die Zahl der tatsächlich am Markt befindlichen KI-basierten Medizinprodukte in Europa bislang überschaubar - die breite Markteinführung steht noch am Anfang.

Eine der Schlüsselvoraussetzungen für die Zulassung nach Medizinprodukteverordnung (EU) 2017/745 (MDR) ist im Regelfall ein belastbares Qualitätsmanagementsystem (QMS). Für Medizinprodukte orientiert sich der Aufbau typischerweise an der ISO 13485[1]. Als harmonisierte Norm unterstützt sie Hersteller dabei, Prozesse und Aktivitäten zu etablieren, um den regulatorischen Anforderungen der MDR gerecht zu werden. Mit der kommenden Verordnung über Künstliche Intelligenz EU 2024/1689, dem europäischen AI Act, kommen jedoch zusätzliche Anforderungen an QM-Systeme für Anbieter von Hochrisiko-KI-Systemen hinzu.

Doch welche Anforderungen stellt der AI Act (AIA) konkret an QM-Systeme? Genügt ein QM-System, das nach ISO 13485 aufgestellt wurde, um die Anforderungen des AI Act abzudecken – oder muss ein zusätzliches QM-System etabliert werden? Diesen Fragen soll im Folgenden nachgegangen werden. Zunächst wird der Blick auf die konkreten Anforderungen an QM-Systeme nach AI Act geworfen, bevor eine vergleichende Analyse die ISO 13485 in Bezug zu den genannten Anforderungen stellt.

Dabei wird deutlich werden, dass die ISO 13485 den allgemeinen Anforderungen an QM-Systeme, wie sie im AI Act gefordert werden, weitgehend entspricht. Aufgrund ihres technologie-agnostischen Charakters verbleiben allerdings KI-spezifische Lücken, die gezielt adressiert werden müssen. Dies kann durch eine gezielte Erweiterung des QM-Systems nach ISO 13485 geschehen, sodass die Erstellung eines zusätzlichen QM-Systems nicht nötig ist. Somit ist regulatorische Konformität mit begrenztem Aufwand möglich.

[1] Bezug genommen wird auf die deutsche Fassung der EN ISO 13485:2016 Medizinprodukte – Qualitätsmanagementsysteme – Anforderungen für regulatorische Zwecke.

Anforderungen an QM-Systeme aus dem AI Act

Der AIA definiert in Art. 17 konkrete Anforderungen an QM-Systeme von KI-Anbietern. Deren Umsetzung soll im angemessenen Verhältnis zur Größe der jeweiligen Organisation stehen (Art. 17 Abs. 2 AIA) und kann in bereits bestehende QM-Systeme integriert werden (Art. 17 Abs. 3 AIA). Damit trägt der Gesetzgeber der unternehmensseitigen Forderung nach balancierten Aufwänden Rechnung.

Das QMS eines Anbieters von Hochrisiko-KI-Systemen muss gemäß Art. 17 Abs. 1 AIA zentrale Anforderungen systematisch abbilden. Zu den in diesem Absatz genannten Anforderungen zählt beispielsweise ein Konzept zur Einhaltung der regulatorischen Vorgaben, einschließlich Konformitätsbewertung und Änderungsmanagement. Darüber hinaus sind geeignete Verfahren für Entwurf, Entwicklung, Qualitätskontrolle und -sicherung nachzuweisen und die Entwicklungsphasen durch validierte Prüf-, Testverfahren abzusichern. Auch technische Spezifikationen und anwendbare Normen sind zu benennen und auf ihre Eignung zur Erfüllung der grundlegenden Anforderungen hin zu prüfen. Zentral ist darüber hinaus ein Risikomanagementsystem gemäß Art. 9 AIA, ein System zur Beobachtung nach dem Inverkehrbringen gemäß Art. 72 AIA sowie ein Verfahren zur Meldung schwerwiegender Vorfälle gemäß Art. 73 AIA. Eine detaillierte Darstellung der Anforderungen aus Art. 17 AIA ist im Anhang zu finden.

Artikel 17 AI Act trifft auf ISO 13485

Ein Abgleich der Anforderungen aus Art. 17 AIA mit jenen der ISO 13485 zeigt: Während einige Bereiche vollständig abgedeckt sind, bleiben andere nur unzureichend adressiert. Dieses Ergebnis ergibt sich hauptsächlich durch den technologie-agnostischen Charakter der ISO 13485, die KI-spezifische Themen nicht direkt abdeckt. Im Detail ergibt sich folgendes Bild:

Tabelle 1: Vergleich der Anforderungen an QMS zwischen Art. 17 (1) AIA und ISO 13485

AIA Referenz [2]	ISO 13485	Deckungsgrad [3]	Kurzbegründung
Art. 17 (1) (a)	**4.1.4** Regulatorische Anforderungen **5.6** Management-bewertung **7.3.9** Lenkung von Entwicklungs-änderungen	**Teilweise**	Die ISO 13485 verpflichtet zur Einhaltung regulatorischer Anforderungen und fordert deren Umsetzung im QMS. Eine strategisch dokumentierte Gesamtverantwortung für AI-Act-Konformität inklusive KI-spezifischer Richtlinien und Änderungsmanagementprozesse ist jedoch nicht vorgesehen.
Art. 17 (1) (b)	**7.1** Planung der Produktrealisierung	**Vollständig**	Die ISO 13485 fordert planvolle Produktrealisierung inklusive der notwendigen Verifizierungs- und Validierungsaktivitäten in dieser Phase und deckt damit Art. 17 (1) (b) ab.
Art. 17 (1) (c)	**7.3.1 – 7.3.7** Entwicklung	**Vollständig**	Die Norm spezifiziert Verfahren für die Entwicklungslenkung, qualifiziertes Personal sowie dokumentierte Qualitätskontrolle und -sicherung. Die Anforderungen an systematische Entwicklungs- und Produktionsprozesse sind damit abgedeckt.

[2] Eine detaillierte Darstellung der Anforderungen aus Art. 17 AIA ist im Anhang zu finden.
[3] Deckungsgrad-Legende: **Vollständig** – ISO 13485 deckt sich vollständig mit den Anforderungen des AI Act. **Teilweise** – Prozess vorhanden, aber deckt die Anforderungen nicht vollständig ab. **Lücke** – ISO 13485 deckt das Thema nicht oder nur marginal ab.

Art. 17 (1) (d)	**7.3.1 - 7.3.7** Entwicklung **7.5** Herstellung & Dienstleistung **8.1-8.2** Messung, Analyse und Verbesserung	**Vollständig**	Validierungs- und Verifizierungsaktivitäten zur Gewährleistung der notwendigen Sicherheit und Leistungsfähigkeit, basierend auf den funktionalen Anforderungen des Medizinprodukts, sind vollständig abgedeckt.
Art. 17 (1) (e)	**4.1.4** Regulatorische Anforderungen **7.3.3** Entwicklungseingaben	**Teilweise**	Die ISO 13485 verlangt die Berücksichtigung regulatorischer und funktionaler Anforderungen. Die Dokumentation von Daten und ihrer Governance, Aufzeichnungspflichten, menschlicher Aufsicht sowie Anforderungen an Genauigkeit, Robustheit und Cybersicherheit gemäß Kap. 3 Abschn. 2 AIA, sind jedoch nicht enthalten.
Art. 17 (1) (f)	-	**Lücke**	Die ISO 13485 adressiert Datenverwendung primär im Kontext von Entwicklungseingaben. Ein strukturiertes Datenmanagement mit Prozessen zur Datenerhebung, -bereinigung, -kennzeichnung und -einspeisung in KI-Modelle ist nicht vorgesehen.
Art. 17 (1) (g)	**7.1** Planung, inkl. Verweis auf ISO 14971	**Teilweise**	Die ISO 13485 fordert explizit die Integration von Risikomanagementprozessen und bezieht sich dabei auf die ISO 14971[4]. Vor allem für Software-Produkte wird diese bereits verwendet, enthält allerdings keine KI-spezifischen Risiken. Hersteller können sich nach MDR auf ein Risiko-Nutzen-Verhältnis beziehen, während nach AI Act zu größten Teilen nur das Risiko in Betracht gezogen wird.

[4] Wenn die ISO 13485 auf den Risiko-Management-Prozess Bezug nimmt, müssen diese Prozess im Einklang mit dem Risikoverständnisses der MDR stehen, d.h. das Risiko „so weit wie möglich und angemessen" zu verringern (vgl. ISO 13485, Anhang ZB).

Art. 17 (1) (h)	**8.2.1** Rückmeldungen **8.5** Verbesserung	**Teilweise**	Die ISO 13485 schreibt explizit einen Post-Market-Rahmen vor, der die Konformität des Produkts nach Inverkehrbringen gewährleisten soll. Allerdings tauchen die in Anhang VI Abs. 3 AIA genannten Elemente, die Teil der Überwachung nach Inverkehrbringung sein müssen, nicht explizit in der ISO 13485 auf und müssen ergänzt werden.
Art. 17 (1) (i)	**8.2.3** Behördenmeldung	**Vollständig**	Vorkommnisse, die die Sicherheit oder die Konformität des Produktes betreffen, müssen gemäß ISO 13485 an die zuständigen Behörden gemeldet werden. Die Anforderungen des AIA sind damit abgedeckt.
Art. 17 (1) (j)	**7.2.3** Externe Kommunikation	**Vollständig**	Die Norm sieht klare Kommunikationsprozesse mit Behörden, Benannten Stellen und Kunden vor. Der systematische Austausch ist zu dokumentieren und nachvollziehbar geregelt.
Art. 17 (1) (k)	**4.2.5** Lenkung von Aufzeichnungen	**Vollständig**	Dokumentationspflichten und Aufzeichnungskontrolle sind in der ISO 13485 umfassend geregelt. Revisionssicherheit und Nachvollziehbarkeit werden normativ verlangt und decken daher die Anforderungen des AIA ab.
Art. 17 (1) (l)	**6.1 - 6.4** Ressourcen **7.4** Einkauf	**Vollständig**	Personal, Infrastruktur, unterstützende Dienstleistungen, Arbeitsumgebung und Zulieferer sind von der ISO 13485 abgedeckt.
Art. 17 (1) (m)	**5.5** Verantwortung & Befugnisse	**Teilweise**	Rollen und Verantwortlichkeiten müssen von der Organisation benannt werden, sind allerdings nicht für KI-spezifische Anwendungen definiert.

Fazit: Zwischen Synergie und Zusatzaufwand – wohin geht die Reise?

Der AI Act fordert als zentralen Nachweis zur Einhaltung der regulatorischen Anforderungen ein Qualitätsmanagementsystem. Dabei zeigt sich, dass die ISO 13485 als zentrale QM-Norm für Medizinprodukte eine hohe strukturelle Anschlussfähigkeit gegenüber den Anforderungen des AI Act aufweist.

Die Analyse zeigt allerdings auch, dass die ISO 13485 mit Blick auf KI-spezifische Eigenschaften Lücken aufweist. Dies erklärt sich aus dem technologie-agnostischen, aber sektorspezifischen Charakter der MDR, die für Medizinprodukten der Klassen I bis III gilt und sowohl Software- als auch physische Medizinprodukte abdeckt. Dieser Charakter übersetzt sich in die ISO 13485, die auf die gleichen Produktgruppen angewendet werden kann. Der AI Act bildet mit seinem technologie-spezifischen, aber sektorübergreifenden Ansatz das komplementäre Gegenstück zur MDR[5]. Die genannten Lücken zwischen ISO 13485 und AI Act sind daher erwartbar und zugleich spezifisch.

Für Hersteller, die bereits ein ISO 13485-konformes QM-System betreiben, bedeutet dies, dass der AI Act keine Abkehr von bestehenden QM-Systemen erfordert, sondern gezielte Weiterentwicklungen notwendig sind. Diese Weiterentwicklungen beziehen sich insbesondere auf Aspekte, in denen sich KI-Systeme grundlegend von klassischen, regelbasierten Softwareprodukten – sei es als Standalone-Systeme, sei es als Sicherheitskomponenten in physischen Produkten – unterscheiden.

So fordert die ISO 13485 beispielsweise eine planvolle Produktentwicklung und die Lenkung von Änderungen, differenziert dabei aber nicht, ob es sich um KI-basierte oder klassische Systeme handelt. Änderungen an einem KI-System – etwa durch erneutes Training mit aktualisierten Datensätzen – unterliegen anderen Dynamiken und Risiken als Änderungen an einer traditionellen Softwarekomponente und erfordern daher eine Erweiterung um KI-spezifische Steuerungsmechanismen. Ein weiteres Beispiel ist das Datenmanagement: Während die ISO 13485 Anforderungen an die Validierung von Entwicklungseingaben stellt, fehlen klare Vorgaben für Prozesse wie Datenannotation, -bereinigung oder Kontrolle der Nichtdiskriminierung, was allesamt entscheidende Faktoren für die Leistungsfähigkeit und Sicherheit KI-basierter Systeme sind.

Eine Möglichkeit, bestehende QM-Systeme zu erweitern, kann in Zukunft erwartet werden, sobald die harmonisierten Normen für den europäischen Raum, die explizit zur Umsetzung der KI-Verordnung erstellt werden, vorliegen. In diesem Kontext sind insbesondere JT021024 EN AI Risk Management und JT021039

[5] Während KI-Technologien hier als ein Begriff aufgefasst werden, sind diese Technologien in der Praxis natürlich äußerst divers und bringen ihre jeweils spezifischen Anforderungen mit.

EN Quality Management System for EU AI Act Regulatory Purposes zu nennen. Diese befinden sich jedoch noch in einem frühen Stadium und werden in finaler Version laut offiziellem Zeitplan erst Mitte 2026 erwartet.

Eine Möglichkeit, die KI-spezifischen Lücken zwischen AI Act und ISO 13485 bereits heute schon zu schließen, ist die Anwendung der ISO 42001. Die ISO 42001 wurde als Managementsystem-Norm speziell für KI-Anwendungen (KIMS) verfasst und bezieht sich daher konkret auf KI-relevante Anwendungsfälle. Hier lassen sich spezifische Anforderungen, wie beispielsweise KI-Rollen, KI-Risiken oder erste Hilfestellungen zur Umsetzung KI-spezifischer Steuerungsmaßnahmen entnehmen.

Insgesamt zeigt sich, dass die ISO 13485 strukturell anschlussfähig an die QMS-Anforderungen des AI Act ist. Damit wird der AI Act seinem Anspruch, Doppelarbeit zu vermeiden, gerecht und die Erweiterung bestehender QM-Systeme beschränkt sich für Hersteller auf die Abdeckung KI-spezifischer Anforderungen. Die Einrichtung eine komplett neuen QM-Systems ist nicht nötig.

Anhang

Tabelle 2: Anforderungen des AIA an QMS nach Artikel 17 (1)

Art. 17 (1)	Anforderung
(a)	Ein Konzept zur Einhaltung der Regulierungsvorschriften, was die Einhaltung der Konformitätsbewertungsverfahren und der Verfahren für das Management von Änderungen an dem Hochrisiko-KI-System miteinschließt.
(b)	Techniken, Verfahren und systematische Maßnahmen für den Entwurf, die Entwurfskontrolle und die Entwurfsprüfung des Hochrisiko-KI-Systems.
(c)	Techniken, Verfahren und systematische Maßnahmen für die Entwicklung, Qualitätskontrolle und Qualitätssicherung des Hochrisiko-KI-Systems.
(d)	Untersuchungs-, Test- und Validierungsverfahren, die vor, während und nach der Entwicklung des Hochrisiko-KI-Systems durchzuführen sind, und die Häufigkeit der Durchführung.
(e)	Die technischen Spezifikationen und Normen, die anzuwenden sind, um die in Abschnitt 2 genannten Anforderungen zu erfüllen.
(f)	Systeme und Verfahren für das Datenmanagement, einschließlich Datengewinnung, Datenerhebung, Datenanalyse, Datenkennzeichnung, Datenspeicherung, Datenfilterung, Datenauswertung, Datenaggregation, Vorratsdatenspeicherung und sonstiger Vorgänge in Bezug auf die Daten, die im Vorfeld und für die Zwecke des Inverkehrbringens oder der Inbetriebnahme von Hochrisiko-KI-Systemen durchgeführt werden.
(g)	Das in Art. 9 AIA genannte Risikomanagementsystem.
(h)	Die Einrichtung, Anwendung und Aufrechterhaltung eines Systems zur Beobachtung nach dem Inverkehrbringen gemäß Art. 72.
(i)	Verfahren zur Meldung eines schwerwiegenden Vorfalls gemäß Art. 73 AIA.

(j)	Die Handhabung der Kommunikation mit zuständigen nationalen Behörden, anderen einschlägigen Behörden, auch Behörden, die den Zugang zu Daten gewähren oder erleichtern, notifizierten Stellen, anderen Akteuren, Kund:innen oder sonstigen interessierten Kreisen.
(k)	Systeme und Verfahren für die Aufzeichnung sämtlicher einschlägigen Dokumentation und Informationen.
(l)	Ressourcenmanagement, einschließlich Maßnahmen im Hinblick auf die Versorgungssicherheit.
(m)	Einen Rechenschaftsrahmen, der die Verantwortlichkeiten der Leitung und des sonstigen Personals in Bezug auf alle in diesem Absatz aufgeführten Aspekte regelt.

TÜV AI.Lab GmbH
Max-Urich-Str. 3
13355 Berlin
Deutschland
www.tuev-lab.ai
www.tuev-risk-navigator.ai

info@tuev-lab.ai

Das TÜV AI.Lab wurde 2023 als eigenständiges Joint Venture der TÜV-Unternehmen TÜV SÜD, TÜV Rheinland, TÜV NORD, TÜV Hessen und TÜV Thüringen gegründet. Das TÜV AI.Lab hat zum Ziel, die regulatorischen Anforderungen an KI in die Praxis zu übersetzen und Europa zum Hotspot für sichere und vertrauenswürdige KI zu machen. Hierfür entwickelt es quantifizierbare Konformitätskriterien und geeignete Prüfmethoden für KI. Zudem unterstützt das AI.Lab aktiv die Entwicklung von Standards und Normen für KI-Systeme.