



KI-Governance in Pharmaunternehmen

Zwischen EU AI Act und GxP: So gelingt der regulatorische Spagat

Elisabeth Zinggrebe

Sehr geehrte Leser*innen,

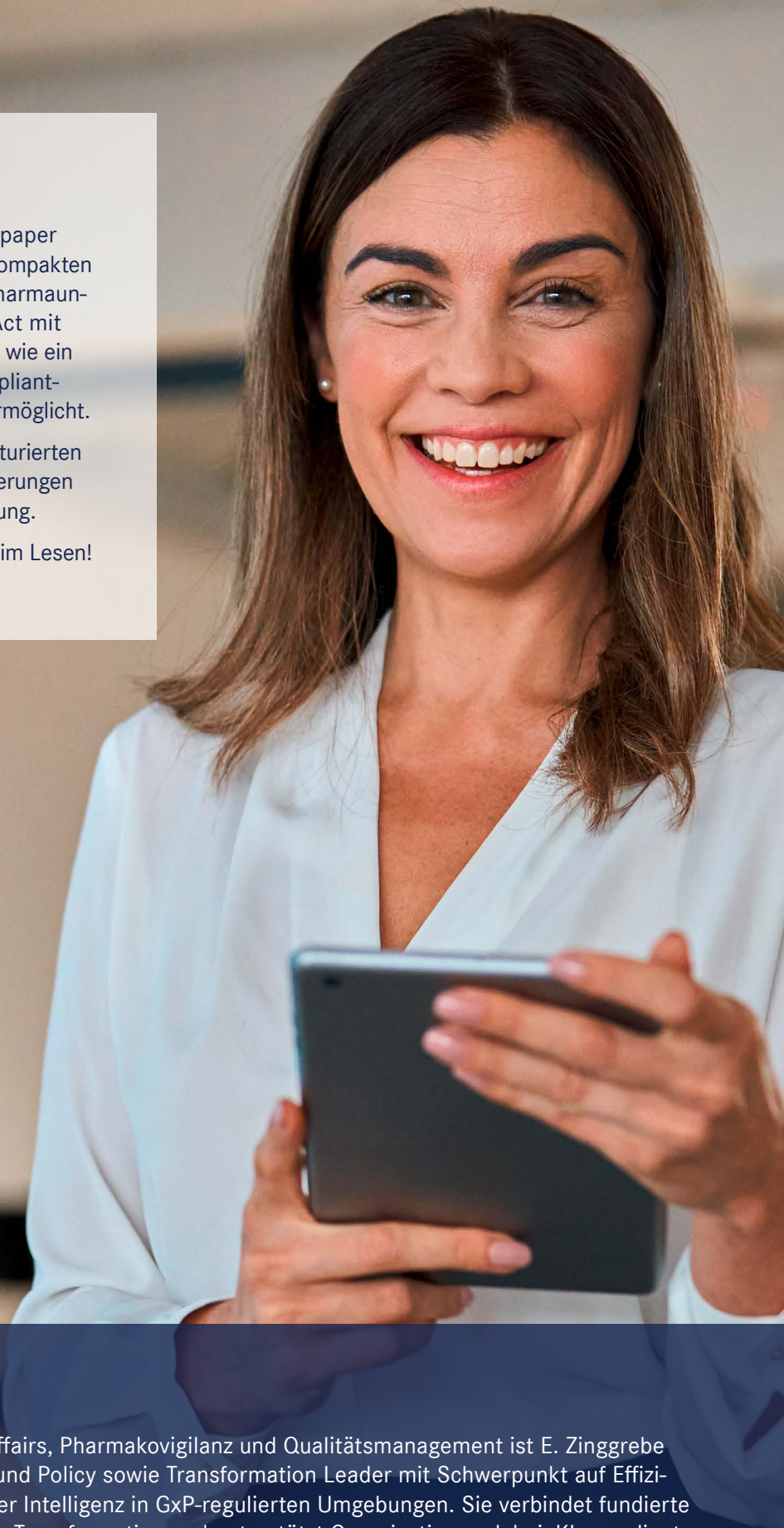
wir freuen uns, dass Sie sich für dieses Whitepaper interessieren. Nachfolgend erhalten Sie einen kompakten Überblick über das Thema KI-Governance in Pharmaunternehmen. Sie erfahren, wie sich der EU AI Act mit bestehenden GxP-Anforderungen verbindet und wie ein wirksames Governance-Rahmenwerk den compliant-konformen Einsatz von Künstlicher Intelligenz ermöglicht.

Dieses Whitepaper bietet Ihnen einen klar strukturierten Einblick in die zentralen regulatorischen Anforderungen und zeigt praxisnahe Ansätze für deren Umsetzung.

Wir wünschen Ihnen viele neue Erkenntnisse beim Lesen!

Über die Autorin Elisabeth Zinggrebe:

Mit über 20 Jahren Erfahrung in Regulatory Affairs, Pharmakovigilanz und Qualitätsmanagement ist E. Zinggrebe Global Head of Quality Management System und Policy sowie Transformation Leader mit Schwerpunkt auf Effizienzsteigerung und dem Einsatz von Künstlicher Intelligenz in GxP-regulierten Umgebungen. Sie verbindet fundierte regulatorische Expertise mit praxisorientierter Transformation und unterstützt Organisationen dabei, KI compliant, skalierbar und wertschaffend zu implementieren - von operativen Use Cases bis hin zur strategischen Weiterentwicklung globaler QMS-Strukturen. Als Speakerin und Vordenkerin im Bereich „AI in GxP“ übersetzt sie regulatorische Anforderungen in umsetzbare, auditfeste Lösungen und verbindet dabei Compliance, Qualität und Innovation.

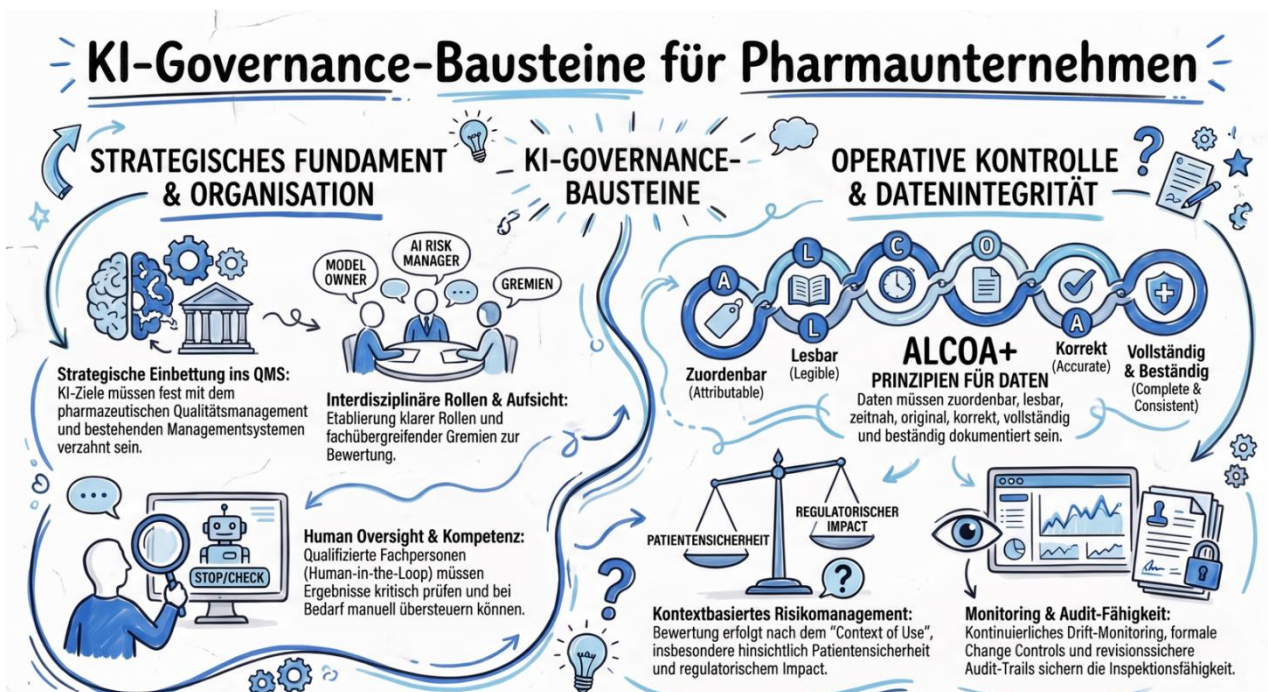


KI-Governance in Pharmaunternehmen

Einordnung

KI-Governance in Pharmaunternehmen beschreibt den organisatorischen und kontrollbezogenen Rahmen, mit dem KI-Systeme über ihren gesamten Lebenszyklus gesteuert werden. Gerade in diesem Umfeld verschärft sich der Governance-Bedarf, weil KI nicht nur Effizienzgewinne verspricht, sondern auch in Bereiche hineinwirken kann, die erhebliche Konsequenzen für Produktqualität, Zulassungsdokumentation, Patientensicherheit, Pharmakovigilanz und Inspektionsfähigkeit haben. Zu berücksichtigende Regularien, die im GxP-Umfeld greifen, stellen eine weitere besondere Herausforderung im Vergleich zu anderen Branchen dar. Deshalb verlangt dieser Sektor „Pharma & Healthcare“ eine besonders belastbare Verbindung von Innovationsfähigkeit, Risikoanalyse, Dokumentation und unabhängiger Aufsicht.

Bausteine der KI-Governance



Die Grafik wurde mit Unterstützung einer KI-basierten Anwendung erstellt.

Strategische Verankerung im regulierten Umfeld

Der Ausgangspunkt ist die Verantwortung des Top-Managements. KI-Ziele müssen mit der Unternehmensstrategie, dem Qualitätsverständnis und der Risikotoleranz des Unternehmens abgestimmt werden, wobei die Anforderungen regulierter Umgebungen ausdrücklich berücksichtigt werden müssen. Eine unternehmensinterne KI-Richtlinie sollte im Pharmaumfeld eng mit bestehenden Managementsystemen verzahnt oder die besonderen Anforderungen in Bezug auf Umgang mit KI in diese integriert werden, insbesondere mit/ins pharmazeutische Qualitätsmanagement (QMS), Informationssicherheit, Datenschutz und etablierten risikobasierten Steuerungsmechanismen: KI-Governance darf sich nicht isoliert entwickeln, sondern sollte in vorhandene QMS- und Kontrollstrukturen eingebettet werden. Hinzu kommen klare Abbruchkriterien und ein Zero-Trust-orientiertes Verständnis. In hochsensiblen Prozessen darf einem KI-System nicht allein aufgrund eines guten Anscheins oder eines

namhaften Anbieters vertraut werden; Vertrauen muss durch dokumentierte Prüfung, Validierung und wiederholte Evidenz abgesichert werden.

Rollen, QMS und unabhängige Aufsicht

Pharmaunternehmen benötigen klar definierte Rollen entlang des gesamten KI-Lebenszyklus: Model Owner oder System Owner, Data Champions, AI Risk Manager und eine erweiterte Qualitätssicherung, die KI-gestützte Entscheidungen beaufsichtigt und Validierungsergebnisse formal freigibt werden etabliert. Besonders relevant ist die Einbindung interdisziplinärer Gremien. In regulierten Kontexten müssen Fachbereiche, Qualitätssicherung, Regulatorik, Recht, Datenschutz, IT und domänenspezifische Experten gemeinsam bewerten, ob ein KI-Anwendungsfall fachlich geeignet, regulatorisch vertretbar und organisatorisch beherrschbar ist. Wesentlich ist zudem die Trennung von Entwicklung, Validierung und Freigabe. Unabhängige Prüfungen, Audits und gegebenenfalls „Red-Teaming“ sind erforderlich, damit Governance nicht auf Selbstbewertung beruht, sondern belastbare Evidenz über Eignung, Grenzen und Restrisiken des Systems erzeugt.

Risiko- und Folgenmanagement in Pharma

Im Pharmabereich muss der Nutzungskontext eines KI-Systems besonders präzise definiert werden. Das Risiko ist nicht abstrakt, sondern nach Einfluss auf Entscheidungen und nach möglichen Konsequenzen für Patientensicherheit, Produktqualität oder regulatorische Auswirkungen zu bestimmen. Dadurch entsteht eine Differenzierung zwischen geringeren und höheren KI-Risiken innerhalb derselben Organisation. Wenn KI lediglich interne Texte formatiert, ist das Risiko anders zu bewerten als bei Anwendungen, die Abweichungen priorisieren, sicherheitsrelevante Signale unterstützen oder regulatorische Bewertungen beeinflussen. Ein pharmazeutisches Governance-Modell sollte deshalb klassische Risikomanagementansätze ausdrücklich um KI-spezifische Risiken erweitern, etwa Halluzinationen, Bias, nicht deterministische Ausgaben, Daten- oder Model Drift sowie neue Cyberbedrohungen. Etablierte Standards im regulierten Umfeld müssen für diese Risiken ergänzt und operationalisiert werden müssen.

Datenintegrität und Modell-Governance

Daten- und Modell-Governance haben in Pharma eine herausgehobene Bedeutung, weil Trainingsdaten, Testdaten, Prompts und KI-Ausgaben in qualitätsrelevanten Kontexten als kontrollbedürftige Aufzeichnungen behandelt werden müssen. Die Bedeutung von Datenintegrität, lückenloser Herkunftsdokumentation und reproduzierbaren Aufbereitungsschritten ist dabei deutlich hervorzuheben. Im regulierten Umfeld wurden hierfür die ALCOA++-Prinzipien als Maßstab angeführt. Daten müssen zuordenbar, lesbar, zeitnah, original, korrekt, vollständig und beständig sein, damit Entscheidungen auf belastbarer und auditierbarer Grundlage beruhen. Diese müssen in entsprechenden Anwendungsfällen auch zur Anwendung kommen. Ebenso essenziell sind Repräsentativität, Bias-Kontrolle, klare Trennung von Trainings-, Validierungs- und Testdaten sowie eine strikte Versionierung von Modellen und relevanten Skripten. Nur so lässt sich später nachvollziehen, welche Modellversion auf Basis welcher Daten zu welchem Ergebnis geführt hat.

Bei externen Modellen, Datensätzen oder Cloud-Diensten kommt die Lieferantensteuerung hinzu. Pharmaunternehmen behalten nach den vorliegenden Unterlagen die letzte Verantwortung für Validierung und sicheren Einsatz, weshalb Quality Agreements, technische Audits und die Prüfung von Datenschutz-, Lizenz- und Sicherheitsaspekten erforderlich sind.

Transparenz, Erklärbarkeit und Inspektionsfähigkeit

Transparenz ist im pharmazeutischen Kontext nicht nur Vertrauensfaktor, sondern Voraussetzung für Inspektions- und Auditfähigkeit. Technische Dokumentationen, Model Cards oder System Cards, Inventare aller KI-Systeme sowie nachvollziehbare Betriebsanleitungen schaffen die Grundlage dafür, dass Einsatzgrenzen, Datenbasis, Leistungsparameter und bekannte Schwächen systematisch dargestellt werden können. Erklärbarkeit unterstützt die fachliche Bewertung durch qualifizierte Personen. Wenn KI-Ergebnisse sicherheitsrelevante, qualitätsrelevante oder regulatorische Bedeutung haben, müssen Fach- und Qualitätsexperten die Logik, Unsicherheiten und Grenzen der Ausgabe beurteilen können; hierfür werden in den Unterlagen sowohl interpretierbare Modelle als auch Explain-able-AI-Methoden als hilfreiche Ansätze beschrieben. Revisionssichere Audit-Trails sind unverzichtbar. Sie sollten Eingaben, Ausgaben, Modellstände, Zeitpunkte, menschliche Prüfschritte und Overrides so erfassen, dass Ursachenanalysen, retrospektive Bewertungen und Nachweise gegenüber Auditoren oder Behörden möglich bleiben.

Monitoring, Change Control und Decommissioning

Ein KI-System bleibt im Pharmabereich nur dann beherrschbar, wenn seine Leistung auch nach dem Rollout laufend überwacht wird. Kontinuierliches Monitoring, Drift-Erkennung und KPI-basierte Grenzwerte sind notwendige Elemente, um Leistungsabfälle, veränderte Datenmuster oder neue Verzerrungen frühzeitig zu erkennen. Besondere Bedeutung hat dabei das Änderungswesen. Retraining, Anpassungen von Parametern oder Veränderungen an Datenquellen sind im regulierten Umfeld nicht als beiläufige Optimierung zu behandeln, sondern als formale Systemänderungen mit dokumentierten Triggern, Change Control und risikobasierter Re-Validierung. Ebenso erforderlich sind ein strukturiertes Incident Management und ein kontrolliertes Decommissioning. Kritische Vorfälle müssen erkannt, analysiert, eskaliert und dokumentiert werden; bei nicht mehr beherrschbaren Risiken braucht es die Möglichkeit, das System sicher anzuhalten, auf manuelle Verfahren zurückzufallen oder eine frühere Version kontrolliert wiederherzustellen.

KI-Kompetenz und Human Oversight

Im pharmazeutischen Kontext ist menschliche Aufsicht kein formaler Zusatz, sondern ein zentrales Sicherheitsprinzip. Die verantwortliche Person muss fachlich kompetent sein, den Nutzungskontext verstehen und befugt sein, Ergebnisse der KI zurückzuweisen, zu korrigieren oder den Betrieb zu stoppen. Dafür genügt reine Tool-Schulung nicht. Erforderlich sind belastbare Kompetenzen in Prompting, kritischer Plausibilitätsprüfung, Erkennung von Halluzinationen, sicherem Umgang mit sensiblen Daten und Verständnis der regulatorischen Grenzen des jeweiligen Systems. Besonders relevant ist die Vermeidung von Automation Bias. Gerade in Umgebungen mit hoher Prozessdichte und starker Formalisierung besteht das Risiko, dass überzeugende KI-Ausgaben vorschnell übernommen werden; dem muss durch Schulungen, dokumentierte Prüfschritte, geeignete Eskalationsmechanismen und eine Kultur des begründeten Widerspruchs begegnet werden.

Governance-Bausteine für Pharmaunternehmen

Governance-Baustein	Pharmaspezifische Ausprägung
Strategische Verankerung	Einbettung in QMS, abgestimmte Risikotoleranz, klare No-Go-Kriterien
Rollen und Aufsicht	Model Owner, Data Champions, AI Risk Manager, erweiterte Qualitätssicherung, interdisziplinäre Gremien
Risiko- und Folgenmanagement	Bewertung nach Context of Use, Einfluss auf Entscheidungen, Patientensicherheit und regulatorischem Impact
Daten- und Modell-Governance	ALCOA++, Lineage, Testtrennung, Bias-Kontrolle, Versionierung, Lieferantenqualifizierung
Transparenz und Dokumentation	Model Cards, technische Dossiers, Audit-Trails, Inspektionsfähigkeit
Monitoring und Änderungen	Drift-Monitoring, Change Control, Re-Validierung, Fallbacks, Decommissioning
KI-Kompetenz und Aufsicht	Fachlich qualifizierter Human-in-the-Loop, Schutz vor Automation Bias, dokumentierte Overrides

Schlussbetrachtung

KI-Governance in Pharmaunternehmen ist vor allem eine Frage der Beherrschbarkeit. Ein tragfähiger Einsatz von KI ist nur dann möglich, wenn Strategie, Qualitätsmanagement, Datenintegrität, Validierung, Monitoring und menschliche Verantwortung als integriertes Gesamtsystem ausgestaltet werden. Je stärker ein KI-System in qualitätsrelevante, sicherheitsrelevante oder regulatorisch sensible Entscheidungen eingreift, desto höher sind die Anforderungen an Nachweisführung, Unabhängigkeit der Prüfung und organisatorische Reife. Ein pharmazeutisches KI-Governance-Modell muss deshalb nicht nur Innovation ermöglichen, sondern vor allem sichere, nachvollziehbare und auditierbare Entscheidungen gewährleisten.

Glossar

ALCOA (++)-Prinzipien

Grundprinzipien der Datenintegrität. Daten müssen *Attributable* (zuordenbar), *Legible* (lesbar), *Contemporaneous* (zeitnah), *Original* (originalgetreu) und *Accurate* (korrekt) sein. In der erweiterten Auslegung (++) werden zusätzlich Vollständigkeit, Konsistenz, Beständigkeit und Verfügbarkeit berücksichtigt.

AI-System/KI-System

Maschinengestütztes System, das aus Eingaben Ergebnisse wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen ableitet und damit physische oder digitale Umgebungen beeinflussen kann.

Automation Bias

Neigung von Personen, automatisiert erzeugten Ergebnissen oder Empfehlungen übermäßig zu vertrauen und eigene kritische Prüfung zu reduzieren.

Bias

Systematische Verzerrung in Daten, Modellen oder KI-Ausgaben. Sie kann zu unfairen, fehlerhaften oder nicht repräsentativen Ergebnissen führen.

Context of Use

Konkret festgelegter Anwendungskontext eines KI-Systems. Er umfasst insbesondere Zweck, Nutzerkreis, Eingabedaten, Einsatzgrenzen, betroffene Prozesse sowie mögliche Auswirkungen der Ergebnisse.

Data Champion

Funktion oder Person, die die fachgerechte Nutzung, Qualität, Verfügbarkeit und Governance von Daten in einem Bereich unterstützt und vorantreibt.

Data Drift

Veränderung der Merkmale, Verteilungen oder Qualität von Eingangsdaten im Zeitverlauf. Dadurch kann die Leistung eines KI-Modells beeinträchtigt werden.

Decommissioning

Geordnete Außerbetriebnahme eines KI-Systems. Dazu gehören unter anderem die Entscheidung über das Ende der Nutzung, Sicherung relevanter Aufzeichnungen, Behandlung von Daten und Modellen sowie die Umstellung auf geeignete Ersatz- oder manuelle Prozesse.

Drift-Erkennung

Überwachung zur frühzeitigen Identifikation relevanter Veränderungen bei Daten, Modellverhalten oder Modellleistung.

Explainable AI (XAI)

Methoden und Ansätze zur Verbesserung der Erklärbarkeit von KI-Ergebnissen. Sie sollen qualifizierten Personen ermöglichen, Ergebnisse, Einflussfaktoren, Unsicherheiten und Grenzen eines Modells besser zu beurteilen.

Fallback

Vordefinierter Rückfallmechanismus für den Fall, dass ein KI-System ausfällt, unzuverlässige Ergebnisse liefert oder nicht weiter eingesetzt werden darf; beispielsweise ein manueller Prozess oder die kontrollierte Rückkehr zu einer früheren Systemversion.

Halluzination

Plausibel wirkende, aber sachlich unzutreffende, unbelegte oder erfundene Ausgabe eines KI-Systems, insbesondere eines generativen Sprachmodells.

Human-in-the-Loop

Organisations- und Kontrollprinzip, bei dem eine qualifizierte Person KI-Ergebnisse prüft, bestätigt, korrigiert oder zurückweist und bei Bedarf den Prozess stoppen kann.

Human Oversight (menschliche Aufsicht)

Angemessene menschliche Kontrolle über ein KI-System und dessen Ergebnisse. Sie umfasst Fachkompetenz, Entscheidungsbefugnis, Prüfschritte, Interventionsmöglichkeiten und Eskalationswege.

Incident Management

Strukturierter Prozess zur Erkennung, Bewertung, Untersuchung, Dokumentation, Eskalation und Behebung von Vorfällen oder Abweichungen.

Lineage (Datenherkunft)

Nachvollziehbare Dokumentation der Herkunft, Verarbeitung, Transformation und Verwendung von Daten. Sie zeigt, aus welchen Quellen Daten stammen und wie sie in ein Modell oder Ergebnis eingeflossen sind.

Model Card

Standardisierte Dokumentation eines KI-Modells. Sie beschreibt typischerweise Zweck, Einsatzgrenzen, Trainings- und Testdaten, Leistungsmerkmale, bekannte Einschränkungen, Risiken und Verantwortlichkeiten.

Model Drift

Veränderung des Zusammenhangs zwischen Eingabedaten und erwarteten Ergebnissen eines KI-Modells im Zeitverlauf. Dadurch kann ein ursprünglich geeignetes Modell an Leistungsfähigkeit oder Zuverlässigkeit verlieren.

Model Owner

Benannte verantwortliche Rolle für ein KI-Modell. Zu ihren Aufgaben gehören typischerweise die Sicherstellung des zulässigen Einsatzes, die Pflege der Dokumentation, die Überwachung der Leistung und die Veranlassung notwendiger Maßnahmen.

Nicht-deterministische Ausgabe

Ausgabe eines Systems, die bei identischen oder sehr ähnlichen Eingaben nicht zwingend jedes Mal gleich ausfällt. Dies ist insbesondere bei generativen KI-Modellen relevant.

Override

Bewusste Übersteuerung oder Zurückweisung eines KI-Ergebnisses durch eine befugte Person. Overrides sollten in kritischen Anwendungsfällen nachvollziehbar dokumentiert werden.

Red-Teaming

Strukturierte, kritische Prüfung eines KI-Systems aus einer Angriffs- oder Gegenperspektive. Ziel ist, Schwachstellen, Fehlanwendungen, Sicherheitsrisiken und unerwünschte Ergebnisse frühzeitig aufzudecken.

Zero Trust

Sicherheitsprinzip, nach dem keinem Nutzer, System oder Dienst standardmäßig vertraut wird. Zugriffe und Berechtigungen werden fortlaufend überprüft und auf das erforderliche Maß begrenzt.

Passende Weiterbildungen finden Sie hier:

Seminare zu Pharma & Healthcare

Wir bieten Ihnen maßgeschneiderte Weiterbildungsoptionen für die gesamte Healthcare-Branche. Wir konzipieren unsere Weiterbildungen gründlich recherchiert und nach didaktischen Gesichtspunkten. Wir garantieren fachlich hochwertige Weiterbildung für Ihren Erfolg – unsere ISO-Zertifizierungen nach 9001 und 21001 unterstreichen dies. [Jetzt informieren.](#)

e-Learning – Klicken und Lernen

Das FORUM Institut bietet mit hochwertigen e-Learning-Programmen eine flexible Weiterbildungsform. Entscheiden Sie selbst, wann und wo Sie lernen. [Jetzt gratis testen.](#)

Inhouse-Seminare – Maßgeschneiderte Lösungen

Alle unsere Seminare eignen sich auch hervorragend als [Inhouse-Training](#). [Jetzt individuelles Angebot anfordern.](#)