Europaweite Regulierung von „Künstlicher Intelligenz" – Was Arztpraxen, Krankenhäuser und Pflegeeinrichtungen jetzt beachten müssen

von Thomas Althammer

Der europäische AI-Act (KI-Verordnung) ist eine der ersten Verordnungen weltweit, die Anwendungen, die auf Künstlicher Intelligenz (KI) oder genauer auf Machine Learning basieren, reguliert. KI gilt als Schlüsseltechnologie, die durch ihre disruptive Kraft die Arbeitswelt der allermeisten Branchen signifikant verändern wird. KI ist in der Lage, große Datenmengen schnell und umfangreich zu verarbeiten und zu analysieren – viel schneller, als der Mensch dies könnte – und soll so die Patientenversorgung verbessern, Krankheiten früher erkennen, das Personal des Gesundheits-, Sozial- und Pflegesektors entlasten und Kosten senken. Den Chancen stehen aber auch Risiken gegenüber, die die Europäische Union mit einer umfassenden Regulierung zu begrenzen sucht. Thomas Althammer, Geschäftsführer des Beratungsunternehmens Althammer & Kill, beleuchtet die Herausforderungen.

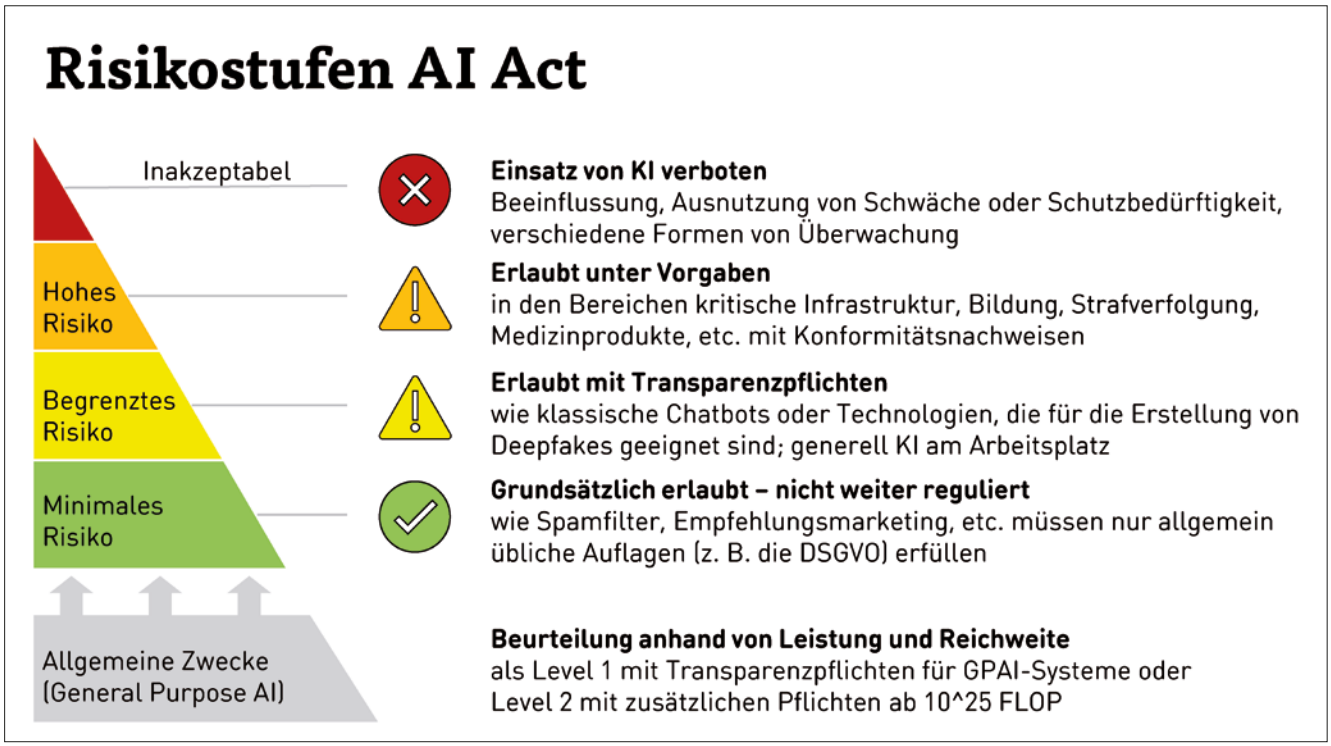


Abbildung 1: Risikoklassen für KI-Systeme nach Definition der europäischen KI-Verordnung (eigene Abbildung).

Wir leben in – aus technologischer Sicht – spannenden Zeiten. Die Entwicklungen der letzten 40 Jahre – insbesondere auf dem Feld der KI – sind bahnbrechend, bringen aber auch unerwünschte Nebenwirkungen mit sich. Wenn es um Desinformation und Manipulation durch Fake News und Deepfakes geht, fühlt man sich an orwellsche Zustände erinnert. Über sogenannte „Deepfakes" könnten Videos entstehen, in denen beispielsweise handelnden Personen Botschaften in den Mund gelegt werden, die so nie gesagt wurden. Fake News überfluten die sozialen Medien und machen Stimmung für oder gegen bestimmte Entscheidungen. Unterlegt werden können sie mit Bildmaterial, das eine KI erzeugt hat und das Realitäten vortäuscht, die es so nie gegeben hat.

Dies sind die Schattenseiten einer Technologie, die eigentlich das Zeug dazu hat, viel Positives zu bewirken, Innovation voranzutreiben und die Digitalisierung auf ein neues Level zu heben. Sie sind auch der Grund dafür, dass die Europäische Union mit der KI-Verordnung eine umfassende und verbindliche Regulierung für KI weltweit auf den Weg gebracht hat, die für alle Mitgliedstaaten gilt. Sie legt verbindliche Anforderungen an Transparenz, Sicherheit, Grundrechtsschutz und Verantwortlichkeit fest, insbesondere für KI-Systeme mit hohem Risiko. Damit geht die KI-Verordnung weit über bisherige Selbstverpflichtungen, branchenspezifische Regelungen oder nationale Initiativen hinaus und schafft einen globalen Präzedenzfall für die Regulierung von KI – mit Auswirkungen auf alle Branchen, auch Gesundheit und Pflege.

Dabei ist KI nicht so neu, wie es scheint. Schon seit den 1950er Jahren wird daran geforscht. Aber erst das aktuelle Umfeld konnte ihr zum Durchbruch verhelfen:

- Rechenkapazität ist inzwischen fast unbegrenzt verfügbar.
- Riesige Mengen an Trainingsdaten stehen zur Verfügung.
- Der weltweite Fachkräftemangel sorgt für einen immensen Bedarf an Produktivitätssteigerungen durch Digitalisierung.
- Tech-Konzerne und Investoren sind bereit, große Summen in KI zu investieren.

KI wird nicht erst in ferner Zukunft für uns relevant. Sie hat längst Einzug in die allermeisten Praxen und Organisationen gehalten: Routenplaner, Textentwicklung, generative KI oder Robotik im OP-Saal.

KI in Gesundheit & Pflege: Best Practices

Wie KI-Anwendungen schon heute eingesetzt werden, zeigen diese Beispiele:

- Unter dem Namen **DAISY (Digitales Informations- und Alarmsystem)** plant das Uniklinikum Ostwestfalen-Lippe die Einführung eines Systems, welches den Beginn einer Sepsis – einer lebensbedrohlichen Erkrankung – bereits Stunden vor dem Auftreten klinischer Symptome vorhersagen kann.
- In der medizinischen Diagnostik sorgt Bilderkennung über KI schon in der Dermatologie, der Krebsmedizin oder Radiologie dafür, dass krankhafte Veränderungen schneller erkannt und behandelt werden können. Beispiele sind die **Hautscreening-App SkinScreener** oder das **Mammografie-Screening-System JiveX Enterprise PACS.**
- Das **Robotic-System Da Vinci** soll weltweit führend in der roboterassistierten Chirurgie sein. Es wird häufig in der Herzchirurgie, Urologie, Gynäkologie oder Orthopädie eingesetzt und sorgt für Präzision und minimalinvasive Eingriffe.
- Der **Empathie-Roboter Navel** leistet Erinnerungsarbeit bei Klienten (z. B. Tabletteneinnahmen, Unterhalten, Quizzen). Er spricht nicht nur Klienten und Betreuungspersonal proaktiv an, er kann sich auch Gesichter und Namen merken und knüpft an Gespräche vom Vortag an.

- Die **Pflegedokumentations-App „voize" v**erwandelt Sprache für die Pflegedokumentation in Text und beachtet dabei den Datenschutz. Die Sprache wird lokal auf dem Endgerät umgewandelt und anschließend über das Pflegedokumentationssystem verarbeitet.
- **Planerio oder Lösungen wie Connext-Vivendi** erstellen automatisch Dienstpläne. Der KI-gestützte Algorithmus berücksichtigt dabei Arbeitsplätze, Mitarbeiterwünsche, Urlaub, Qualifikation, arbeitsrechtliche Vorschriften, ungeplante Ausfälle und vieles mehr.

Transparenz und Nachvollziehbarkeit der Ergebnisse sind die zentralen Herausforderungen beim Umgang mit KI. Je mehr wir uns auf die vielfältigen Möglichkeiten und Vorteile von KI verlassen, desto wichtiger wird die Korrektheit und Qualität der produzierten Inhalte. Der saubere Umgang mit personenbezogenen Daten und die Einhaltung gesetzlicher Bestimmungen müssen auch beim Einsatz von KI gewährleistet sein.

Die EU-KI-Verordnung im Überblick

Umso wichtiger ist es, ein gutes Verständnis für die Funktionsweise, die Möglichkeiten, aber auch die Grenzen von KI zu entwickeln. Die europäische KI-Verordnung sieht vor, dass Unternehmen seit Februar 2025 für den Aufbau von KI-Kompetenzen bei ihren Mitarbeitenden sorgen müssen. Zudem gelten ab 2026 und 2027 je nach Risikostufe und Verarbeitungskontext weitergehende Compliance-Anforderungen (siehe Tabelle).

Besondere Auflagen gelten bei Nutzung von KI mit Gesundheitsdaten, am Arbeitsplatz und im Bildungsbereich.

Die KI-Verordnung reguliert Betreiber von KI-Systemen, die im EU-Binnenmarkt tätig sind. Ausgenommen sind militärische Anwendungen sowie reine Forschung und Entwicklung. Die Vorgaben der DSGVO werden durch die KI-Verordnung nicht ersetzt (Art. 2 Abs. 7 AI Act). Die DSGVO bzw. die Kirchengesetze zum Datenschutz bleiben bei einem Personenbezug von Daten im Kontext von KI parallel anwendbar! Dies hat Auswirkungen auf die Rechte von Betroffenen, z. B. im Zusammenhang mit Artikel 22 DSGVO (Automatisierte Entscheidungen im Einzelfall, einschließlich Profiling).

Wie in Abbildung 1 dargestellt, folgt die KI-Verordnung einem risikobasierten sowie menschenzentrierten Ansatz. Je höher das Risiko, desto strenger sind die Anforderungen an KI-Anwendungen. Es wird unterschieden zwischen verbotenen KI-Praktiken, Hochrisiko-KI-Systemen, KI-Systemen mit geringem Risiko und sogenannten „General Purpose"-KI-Systemen wie ChatGPT, die in unterschiedlichen Kontexten und für verschiedene Zwecke genutzt werden.

Pflichten für Betreiber von KI-Systemen und Fristen

Für Entwicklung und Einsatz von KI-Systemen sind u. a. bestimmte Compliance-Auflagen relevant, siehe Tabelle 1.

Was im Einzelnen zu berücksichtigen ist, muss also in Hinblick auf den Zweck, die Zielrichtung und das Einsatzszenario für KI-Systeme im Lichte der europäischen Vorgaben individuell bewertet werden.

Seit dem 2. Februar 2025 muss die Nutzung verbotener KI-Systeme beendet sein. Ebenfalls zu diesem Stichtag müssen Praxen, Einrichtungen und Kliniken ihre Mitarbeitenden beim Umgang mit KI schulen.

Ab dem 2. August 2026 müssen alle übrigen Vorgaben der KI-Verordnung (z. B. Transparenzpflichten, Dokumentation) angewendet werden.

Mit Frist zum 2. August 2027 gelten spezifische Anforderungen für Hochrisiko-KI-Systeme verbindlich (z. B. Registrierung, Risikomanagement).

Die Verordnung sieht vor, dass bis zum 2. August 2030 ausnahmslos alle Anforderungen verbindlich gelten.

Risikoklasse	Beispiel Gesundheitswesen	Pflichten
1. Unannehmbares Risiko	Social Scoring, manipulative oder ausnutzende KI	Verbot des Inverkehrbringens und der Nutzung
2. Hohes Risiko	Diagnostik, Therapieempfehlungen, Bildanalyse	• Risikomanagementsystem • Daten-Governance und -qualität • Technische Dokumentation • Transparenzpflichten • Menschliche Aufsicht • Genauigkeit, Robustheit, Cybersicherheit • Registrierung in EU-Datenbank (für einige Systeme) • Konformitätsbewertung (ggf. durch benannte Stelle)
3. Begrenztes Risiko	Chatbots, administrative Systeme, KI am Arbeitsplatz	• Transparenzanforderungen, z. B.: – Offenlegung, dass Nutzer mit KI-System interagieren – Offenlegung synthetischer Inhalte (Deepfakes) – Offenlegung von Emotionserkennung oder biometrischer Kategorisierung
4. Minimales Risiko	Spamfilter, Virenschutz, Firewall, etc.	• Keine spezifischen regulatorischen Anforderungen • Freiwillige Codes of Conduct möglich

Tabelle 1: Compliance-Auflagen für die Entwicklung und den Einsatz von KI-Systemen

Haftungsrisiken durch KI-Verordnung und Produkthaftungsrichtlinie

Sollte Patientinnen und Patienten durch den Einsatz von KI-Systemen ein Schaden entstehen, liegt die Verantwortung beim Behandelnden – eine klassische Produkthaftung kennen die Gesetze (noch) nicht.

Wird KI als Medizinprodukt eingesetzt und entstehen daraus Schäden, z. B. weil der behandelnde Arzt die KI nicht richtig gebraucht oder falsche Daten eingegeben werden, dann gelten aktuell die bekannten rechtlichen Vorgaben zu Behandlungsfehlern. Das bedeutet, dass der Arzt für Behandlungen haftet, die nicht den allgemein anerkannten fachlichen Standards entsprechen, wenn dem Patienten daraus ein Schaden entsteht. Auch die KI-Verordnung sieht umfassende Pflichten bei der Nutzung von KI vor (siehe Tabelle 1). Die Nutzung von KI entbindet nicht von der Pflicht, Sorgfalt walten zu lassen und den Patienten über die Verwendung von KI und deren Risiken aufzuklären.

Darüber hinaus entstehen aus der neuen EU-Produkthaftungsrichtlinie[1], die im vergangenen Dezember in Kraft getreten ist, neue klägerfreundliche Anforderungen. Sie wird die Produkthaftungsrichtlinie der EU aus dem Jahr 1985 ersetzen. Bis dato erfasste die Produkthaftung Software nicht. Das wird sich jetzt ändern. Bei Schäden, die durch fehlerhafte KI-Systeme entstehen, kann dann der Hersteller, aber auch der Betreiber, (z. B. die Klinik) haftbar gemacht werden[2]. In Deutschland ist die Produkthaftungsrichtlinie derzeit noch nicht in nationales Recht umgesetzt – die Frist hierfür läuft bis Dezember 2026. Krankenhäuser, Praxen und Einrichtungen müssen mit einer erhöhten Transparenz- und Dokumentationspflicht rechnen, um im Schadensfall nachweisen zu können, dass sie Produkte ordnungsgemäß eingesetzt und überwacht haben[3].

Aktuell diskutiert die EU auch über eine Studie zum Entwurf einer Richtlinie über KI-Haftung, die Teil der KI-Verordnung ist. Wird die Richtlinie über KI-Haftung verabschiedet, wird sie zusammen mit der Produkthaftungsrichtlinie ein zivilrechtliches Haftungssystem bilden, das Hersteller und Anbieter von KI-Systemen und -Software vollumfänglich zur Verantwortung zieht, resümieren die Juristen von TaylorWessing[4].

Wie kann der richtige Umgang mit KI gelingen?

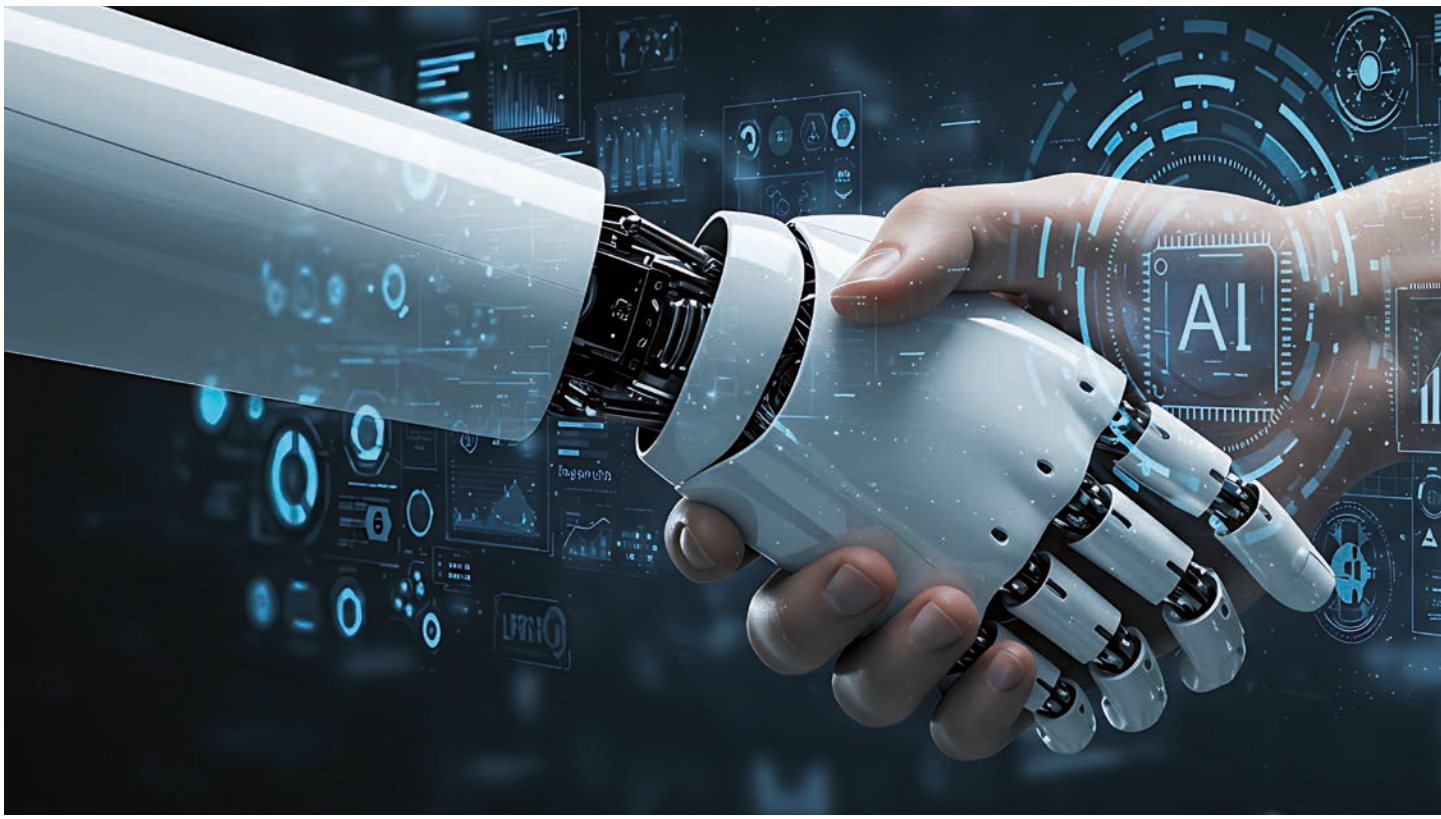
Praxen, Einrichtungen und Kliniken müssen sich entscheiden, ob sie KI über „learning by doing" einführen oder über wissenschaftlich-theoretische Ansätze mit umfassender Beratung. Viele werden erst einmal abwarten und die weitere Entwicklung beobachten. Wir raten unseren Kunden, die Einführung in drei Phasen strategisch zu planen, ethische Fragestellungen einzubeziehen und alle regulatorischen und organisatorischen Anforderungen auf den Weg zu bringen. Alsdann können erste kleine Pilotprojekte gestartet und im Prozess das Personal geschult werden. Sobald Einrichtungen KI-gestützte Anwendungen einführen, sind sie „Betreiber" im Kontext der KI-Verordnung und „Verantwortliche" im Sinne der Datenschutzgesetze. Wer also einen Chatbot im Unternehmen einführt oder die Kontierung in der Buchhaltung KI-gestützt durchführen lässt, ist „Verantwortlicher" im Sinne der Datenschutzgesetze.

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202402853

[2] https://health.ec.europa.eu/ehealth-digital-health-and-care/artificial-intelligence-healthcare_de

[3] www.johner-institut.de/blog/regulatory-affairs/produkthaftung/

[4] www.taylorwessing.com/de/insights-and-events/insights/2025/01/die-neue-eu-produkthaftungsrichtlinie



Die eigentlichen Anbieter und Hersteller der Systeme sind im Rahmen der bestehenden Datenschutzgesetze (bisher) nur teilweise im Fokus von Regulierung.

Zur Einbindung von Dienstleistern kennt die DSGVO Verträge zur Auftragsverarbeitung und Verarbeitung in gemeinsamer Verantwortung. Diese ist dann anzunehmen, wenn der Auftraggeber nicht allein über Mittel und Zweck der Verarbeitung entscheidet, was häufig für KI-basierte Systeme gelten dürfte. Wenn der KI-Anbieter aufgrund des Nutzungsverhaltens der Kunden sein System weiter verbessern und optimieren möchte, ist das ein eigener Zweck und der KI-Anbieter wird selbst zu einer verantwortlichen Stelle. All dies und viele weitere Aspekte müssen bedacht werden und finden Eingang in unser 3-Phasen-System:

Phase 1: Der KI-Readiness-Check

Sind Organisationen bereit für den Einsatz von KI? Die richtige Einschätzung der vorliegenden Daten und Prozesse ist essenziell, um für einen verantwortungsvollen Einsatz zu sorgen, insbesondere im Gesundheits- und Sozialwesen. Dazu gehören Analysen des Datenschutzes, der IT-Sicherheit (gerade im Hinblick auf die zunehmende Cyberkriminalität) und eine Prüfung der Kompetenzen im Haus. Das Praxis-Know-how externer Berater kann diese Prozesse schneller zum Abschluss bringen.

Phase 2: KI-Projekt-Assessment

Im KI-Assessment werden für konkrete Anwendungsfälle wie ChatGPT und Microsoft Copilot oder etwa den Einsatz von Sensorik und Robotik frühzeitig die Potenziale analysiert, gegen die Risiken abgewogen und die Voraussetzungen für eine erfolgreiche Implementierung zusammengefasst. Anhand eines Maßnahmenplans kann so bereits frühzeitig auf die rechtskonforme Implementierung geachtet werden.

Phase 3: KI-Risikomanagement

Verschiedene KI-Lösungen sollten hinsichtlich Funktionalität, Skalierbarkeit und Kompatibilität mit vorhandenen Systemen evaluiert werden. Welche Daten nutzt die KI, wie kommt sie zu Ergebnissen, welche Kontrollmechanismen gibt es, wer sorgt für IT-Sicherheit und Einhaltung der Unternehmens-Compliance? Diese Fragen müssen in der Risikoanalyse geklärt und im Kontext der geltenden Rechtsvorschriften adressiert werden, z. B. mit Grundrechte- und Datenschutz-Folgenabschätzungen.

Die Entwicklung und Implementierung von KI-Funktionen muss sich an wechselnde Umgebungsbedingungen anpassen und der hohen Entwicklungsgeschwindigkeit Rechnung tragen. Es ist übrigens ein Irrglaube, dass der Einsatz von KI im Gesundheits- und Sozialwesen nicht mit den Grundsätzen des Datenschutzes zu vereinbaren sei. Durch Nutzung von Technologien wie Retrieval-Augmented-Generation ist der verantwortungsvolle Einsatz von KI in Verbindung mit personenbezogenen Daten möglich. Halluzinationen können begrenzt und die Verwendung bestehender Datenquellen in den Einrichtungen unter Beachtung der Vorgaben der Datenschutzgesetze integriert werden.

Mit Augenmaß agieren

Die Einführung von KI-Systemen ist für Praxen, Einrichtungen und Kliniken eine komplexe Herausforderung. Durch ihre disruptive Kraft werden maschinelles Lernen und neuronale Netze unseren Arbeitsalltag künftig branchenübergreifend verändern. Dass technologische Entwicklungen und regulatorische Maßnahmen zu einer umfassenden Überwachung oder Kontrolle führen, wie Orwell in seinen Werken schreibt, geht zu weit. Richtig ist aber, dass wir uns mit dem Umgang mit KI auseinandersetzen müssen, um Chancen und Risiken der Technologie bestmöglich auszubalancieren. Der Gesundheits- und Pflegesektor muss einen ausgewogenen Ansatz finden, um an Innovation und Fortschritt zu partizipieren, ohne die ethischen Grundsätze und die Verantwortung für Patienten und Klienten aus den Augen zu verlieren.

Praxistipp:

Das Whitepaper „Der Weg zu einer pragmatischen KI-Richtlinie" von Althammer & Kill bietet Informationen zu einem Baustein einer umfassenden IT-Strategie im Hinblick auf KI. Die Handreichung informiert über den Einsatz von KI-Systemen und KI-Methoden – sei es die Nutzung durch Mitarbeitende, die Integration in Produkte oder bei der Eigenentwicklung – und stellt detailliert die Bereiche vor, mit denen sich Organisationen auseinandersetzen müssen.

Das Whitepaper steht auf der Homepage zum kostenlosen Download bereit.

www.althammer-kill.de/themen/ki-richtlinie-whitepaper

Thomas Althammer

ist Geschäftsführer des 40-köpfigen Beratungsunternehmens Althammer & Kill GmbH & Co. KG, das an der Schnittstelle von Recht und Technik aktiv ist, z. B. mit der Stellung externer Datenschutzbeauftragter und externer Informationssicherheitsbeauftragter sowie Beratungsangeboten im Umfeld von KI und Compliance. Thomas Althammer ist Lehrbeauftragter an der Katholischen Universität Eichstätt-Ingolstadt und der Hochschule Hannover sowie Co-Leiter der Fachgruppe IT-Compliance bei FINSOZ e. V.