INSIGHTS

protiviti®
Global Business Consulting

EIN LEITFADEN FÜR FINANZINSTITUTE

Die Auswirkungen des EU Artificial Intelligence Act verstehen.

Von Carol M. Beaumier

Das EU-Gesetz über künstliche Intelligenz (KI), der EU AI Act, ist die bis dato wohl wichtigste und weitreichendste Verordnung zu KI, die von einer Jurisdiktion jemals erlassen wurde. Das Gesetz liefert einen integrierten Ansatz, der unter Berücksichtigung der Anwendungsmöglichkeiten von KI auch deren Risiken einbezieht – während gleichzeitig ein ethischer und verantwortungsvoller Umgang sichergestellt werden soll. Das Gesetz findet grenzübergreifend Anwendung und betrifft jedes Unternehmen in der EU, das KI-Dienste oder -Produkte zur Verfügung stellt oder diese nutzt. Ebenfalls eingeschlossen sind solche Unternehmen, die B2B KI-Dienste anbieten, die EU-Bürger*innen bereitgestellt oder von ihnen genutzt werden – unabhängig davon, wo sich der Hauptsitz des Unternehmens befindet. Daher ist es sowohl für EU-ansässige wie auch multinationale Finanzunternehmen Pflicht, die Anforderungen des Gesetzes zu verstehen.

Was sollten alle Unternehmen über den EU AI Act wissen?

Das Gesetz stützt sich auf wichtige Grundsätze, darunter Verhältnismäßigkeit basierend auf Risiken, Transparenz und Verantwortlichkeit, Fairness und Antidiskriminierung, Schadensvermeidung, Datenschutz und Datensicherheit, Sicherheit und Vertrauenswürdigkeit sowie die Notwendigkeit menschlicher Aufsicht.

Definition gemäß EU AI Act

KI-System

Ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können.

Das Gesetz verfolgt einen risikobasierten Ansatz zur Kategorisierung von KI-Systemen:

Inakzeptabel Systeme, die eine eindeutige Bedrohung für die Sicherheit, die Existenzgrundlage oder die Rechte von Menschen darstellen.

Hoch Systeme mit erheblichen Auswirkungen, die aufgrund ihrer potenziellen Folgen eine strenge Überwachung erfordern.

Begrenzt Systeme mit geringerer Auswirkung, die dennoch ein gewisses Maß an Transparenz erfordern, um sicherzustellen, dass Nutzer*innen wissen, dass sie mit einem KI-Dienst interagieren.

Minimal Systeme, die vernachlässigbare Risiken für die Rechte oder die Sicherheit der Nutzer*innen darstellen.

Risikolevel gemäß EU AI Act

Beispiele von KI-Systemen

- Social-Scoring-Systeme[1]
- Credit-Scoring-Systeme/Bonitätsanalysesystem
- Kundenservice-Chatbot
- E-Mail Spam-Filter

1) Social-Scoring-KI-Systeme nutzen Daten wie soziales Verhalten, Persönlichkeitsmerkmale und andere Daten, um Menschen zu bewerten und ihren Zugang zu Leistungen wie Bildung, Gesundheitsfürsorge und öffentlichen Verkehrsmitteln zu bestimmen. Menschen mit einer guten Bewertung erhalten Vorteile, während Menschen mit schlechten Bewertungen bestraft oder von Leistungen ausgeschlossen werden können.

Das Gesetz stützt sich auf die partnerschaftliche Zusammenarbeit der Anbieter und Anwender, um die Sicherheit und Vertrauenswürdigkeit von KI sicherzustellen. Anwender sind die Nutzenden eines Systems; Anbieter entwickeln KI-Systeme oder haben diese entwickelt und sie unter ihrem Namen auf den Markt gebracht – gegen Bezahlung oder auch kostenlos.

Alle KI-Systeme müssen einer Risikobewertung unterzogen und inventarisiert werden.

Anbieter stehen in der Verantwortung, sicherzustellen, dass die KI-Systeme den Regelungen des Gesetzes entsprechen, bevor sie auf den Markt gebracht oder in Betrieb genommen werden. Hochrisikosysteme, die den striktesten Regelungen unterliegen, müssen folglich eine Konformitätsbewertung durchlaufen, um zu gewährleisten, dass das System den Anforderungen des Gesetzes entspricht. Dazu zählen eine anhaltende, umfassende technische Dokumentation, die aufzeigt, dass das System gesetzeskonform ist, die Entwicklung und Pflege eines Risikomanagementsystems über den gesamten Lebenszyklus des KI-Systems hinweg, die Pflege von systemgenerierten Protokollen, um die Rückverfolgbarkeit der Funktionsweise des Systems sicherzustellen, die Wahrung von eindeutigen und exakten Informationen (einschließlich Systembeschränkungen) für Nutzer*innen, die Überwachung der Performance nach Systemeinführung sowie die Berichterstattung jeglicher Fehlfunktionen oder schwerwiegender Vorfälle und die Meldung dieser an die zuständigen Behörden. Außerdem sind Anbieter bestimmter Arten von Hochrisikosystemen dazu verpflichtet, diese in einer EU-Datenbank zu registrieren, bevor sie auf den Markt gebracht werden.

Für weiterführende Informationen zum Gesetz, lesen Sie „What Business Leaders Need to Know About the EU's AI Act".

Anwender sind in der Verantwortung, hochrisikoreiche KI-Systeme im Sinne ihres von den Anbietern vorgegebenen Einsatzzweckes zu nutzen und die Risiken mitigieren zu können, die sich durch Fehlfunktionen oder Missbrauch ergeben können. Dabei müssen sie sicherstellen, dass das System relevante, repräsentative und unverzerrte Daten nutzt und die Datennutzung den erforderlichen Datenschutzbestimmungen entspricht. Wo nötig ist sicherzustellen, dass menschliche Kontrolle Anwendung findet und dass jegliche Fehlfunktionen oder wesentliche Auffälligkeiten, welche die Gesundheit, Sicherheit oder Grundrechte gefährden könnten, überwacht und sofort gemeldet werden. Ein Anwender kann unter Umständen neu als Anbieter eingestuft werden, sofern er signifikante Änderungen an einem KI-System vornimmt, das bereits mit hohem Risiko klassifiziert worden ist oder wird.

KI-Anwendungen mit begrenztem Risiko müssen so entwickelt werden, dass Nutzer*innen wissen, dass sie mit einer Maschine interagieren und nicht mit einem Menschen.

KI-Systeme mit minimalem Risiko unterliegen keinen spezifischen Anforderungen gemäß des EU AI Acts, wenngleich erwartet wird, dass sie im Rahmen freiwilliger Verhaltenskodizes mit den grundsätzlichen Prinzipien für verantwortungsvolle KI übereinstimmen.

Das Gesetz trat am 1. August 2024 in Kraft, wobei die Bestimmungen schrittweise in den drei Folgejahren eingeführt werden. Die Regelungen zu Hochrisikosystemen treten am 2. August 2026 in Kraft. Die nationalen Behörden der EU erhalten im Sinne des EU AI Acts die Durchsetzungsbefugnisse und können für Konformitätsverstöße Geldbußen von bis zu 7 % des weltweiten Jahresumsatzes oder in Höhe von 35 Millionen Euro vorschreiben, je nachdem, welcher Wert höher ist.

Geldbußen für Konformitätsverstöße

bis zu

7%

des weltweiten Jahresumsatzes

in Höhe von

35

Millionen Euro

Wie wird der EU AI Act die Finanzdienstleistungsbranche beeinflussen?

(forbes.com)

Die transformativen Auswirkungen von KI auf Finanzdienstleistungen

In der sich rasant entwickelnden Finanzwelt sticht künstliche Intelligenz (KI) als eine transformative Kraft hervor, die die Landschaft der Finanzdienstleistungen neu formt.

Systeme zur Erkennung von Betrug und Geldwäsche, Due-Diligence-Prüfungs- und Kundenbewertungssysteme, Credit-Scoring-Systeme, Algorithmus-basierte Handelssysteme, Entscheidungsfindung bei Anlageoptimierung und Vermögensverwaltung, Versicherungssysteme und Robo-Advisors: Das sind nur einige wenige Beispiele für von Finanzdienstleistern genutzten KI-Systemen, die in den Anwendungsbereich des EU AI Acts fallen. Zwar gilt das Gesetz im Allgemeinen für alle Branchen, aber die Auswirkungen für den Finanzdienstleistungssektor könnten größer sein als für andere, da Finanzunternehmen KI-Dienste inteniv nutzen und die Branche stark reguliert ist, weshalb multinationale Unternehmen oftmals verschiedene Konformitätsstrategien für unterschiedliche Märkte benötigen.

Eine der Herausforderungen, die auf Finanzunternehmen zukommen wird, ist die Nachweispflicht, dass sowohl neue als auch bestehende KI-Systeme die strengen Standards des Gesetzes erfüllen – unter anderem diejenigen mit Bezug auf Transparenz, Fairness, Verantwortung und Aufsicht. Die Zahl der KI-Systeme, die von Finanzinstituten genutzt wird, variiert signifikant und ist von Faktoren abhängig wie der Größe des Unternehmens, den geografischen Regionen, in denen es tätig ist, und der Phase seiner digitalen Transformation, in der es sich befindet. In größeren Finanzunternehmen kann die Anzahl der genutzten KI-Systeme in die Hunderte gehen. Finanzunternehmen, die KI-Systeme vor dem Inkrafttreten des Gesetzes entwickelt oder angewendet haben, müssen erneut evaluieren, ob diese Systeme die Bestimmungen des AI Acts erfüllen. Beispielsweise ist im Gesetz auch der Verbraucherschutz geregelt, was dazu führen kann, dass Finanzunternehmen bestehende Systeme dahingehend anpassen müssen. Weitere Schritte könnten dann ebenfalls sein, dass Kund*innen bezüglich der Auswirkungen von Hochrisikosystemen informiert werden müssen, etwa wie ihre Daten genutzt werden und wie Empfehlungen und Entscheidungen der KI-Systeme zustande kommen.

Das Gesetz gilt ebenfalls für den Gebrauch von KI-Systemen Dritter. Im Rahmen des Leitbilds gemeinsamer Verantwortung bedeutet das für ein von Finanzunternehmen genutztes KI-System Dritter, das in die Kategorie „hohes Risiko“ fällt, dass sowohl der Anbieter des KI-Systems (Dritter) als auch der Anwender (das Finanzunternehmen) jeweils spezifische Zuständigkeiten innehaben, um Compliance zu gewährleisten. Hat ein Finanzunternehmen ein KI-System von Dritten stark modifiziert oder personalisiert – was nicht unüblich ist – ist es unter Umständen vonnöten, weitere Konformitätsnachweise zu erbringen.

Handlungsaufforderung für Unternehmen

Im Rahmen der Umsetzung der oben aufgeführten strategischen KI-Kernprinzipien, gibt es eine Reihe von Schritten, die Finanzunternehmen jetzt umsetzen sollten, um die Konformität mit dem Gesetz zu gewährleisten. Dazu gehören unter anderem die folgenden:

- Durchführung einer Folgenabschätzung des Gesetzes und Zuordnung der Anforderungen zu bestehenden Richtlinien, Prozessen und Verantwortlichkeiten (z. B. Modellrisikomanagement, Daten, Risikomanagement für Dritte), wo es eventuelle Abhängigkeiten oder Überschneidungen geben kann.
- Schulungen der Mitarbeitenden in Bezug auf die ethische Nutzung von KI und die spezifischen Anforderungen des EU AI Acts.
- Identifizierung aller KI-Systeme (einschließlich solcher von Dritten), die in der EU eingesetzt werden und Einstufung in die verschiedenen Risikoklassen gemäß Gesetz.
- Überprüfung/Ergänzung der Dokumentation von KI-Systemen, um die Erfüllung der der gesetzlichen Anforderungen zu gewährleisten, angesichts der Rolle der Finanzinstitute sowohl aus Sicht der Anbieter als auch Anwender.
- Für Finanzunternehmen, die ihren Sitz nicht in der EU haben: Ermittlung der Unterschiede zwischen den Anforderungen für Finanzdienstleister in der EU und in den jeweiligen Heimatländern (sowie anderen Ländern, in denen sie operieren) und Entwicklung und Implementierung einer Strategie zur Einhaltung der Konformität mit allen Anforderungen, die in den KI-Richtlinien des Unternehmens dokumentiert werden sollten.
- Bewertung der von KI-Systemen genutzten Datensätze, um zu verstehen, wie sie beschafft werden, und sicherzustellen, dass sie korrekt, vollständig, fair und wertfrei sind und dass ihre Nutzung mit den entsprechenden Datenschutzbestimmungen konform ist.
- Ermittlung, welche Änderungen an operativen Abläufen vorgenommen werden müssen, z. B. bei Datenkontrollen oder an Systemprotokollen, um die fortlaufende Konformität mit dem Gesetz zu gewährleisten.
- Identifizierung des Bedarfs an zusätzlicher Kundenkommunikation und Entwicklung eines Kommunikationsplans.
- Prüfung, welche Konformitätsmaßnahmen sich in Bezug auf das Gesetz mit dem globalen KI-Programm des Unternehmens decken, das heißt: Kann das Unternehmen eine kohärente und einheitliche Anwendung von KI-Standards unternehmensweit nachweisen?

Befürworter*innen des EU AI Acts gehen davon aus, dass seine strikten Standards zu einem erhöhten Kundenvertrauen und zu Akzeptanz von KI-Systemen führen werden. Kritiker*innen behaupten, das Gesetz könne als Resultat der strikten Standards Innovation hemmen. Unbestritten ist momentan jedoch, dass alle Unternehmen, einschließlich Finanzdienstleister, die in der EU KI-Dienste zur Verfügung stellen oder diese nutzen, die Auflagen des Gesetzes erfüllen oder möglicherweise mit erheblichen Strafen für die Nichteinhaltung rechnen müssen.

Protiviti bietet Unterstützung und Beratung, um Ihnen zu erfolgreichen Ergebnissen zu verhelfen.

So kann Protiviti unterstützen

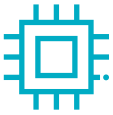
Ganz gleich, ob Ihr Unternehmen gerade erst damit beginnt, KI-Technologien zu nutzen, oder bereits weit fortgeschritten ist, hochentwickelte Anwendungsfälle auszuloten: Protiviti bietet Ihnen hierbei Unterstützung und Beratung an, um Ihnen entlang Ihrer individuellen KI-Transformation zu erfolgreichen Ergebnissen zu verhelfen, während wir gleichsam die Compliance mit dem EU AI Act sicherstellen. Wir unterstützen Sie bei:

Potentialanalysen zu KI

Protiviti unterstützt Sie bei der Identifizierung potenzieller Anwendungsbereiche, in denen KI den Betrieb, Produkte und Dienstleistungen verbessern kann, und entwirft gemeinsam mit Ihnen einen Implementierungsplan. Dazu gehören auch Überlegungen zur Definition des Unternehmenswertes, zur Datenzugänglichkeit, Betriebsmodellen, strategischer Ausrichtung und Governance.

Überwachung von KI

Protiviti unterstützt Sie bei der Messung von Effektivität und Auswirkungen von KI-Lösungen in Bezug auf den Betrieb und/oder Ihre Ziele. Dazu gehören die Festlegung relevanter Performance-Metriken, die Anpassung Ihres Risikomanagements an KI-Spezifika, die Durchführung gründlicher Tests und Validierung der KI-Modelle sowie die Einführung von Feedbackschleifen und kontinuierlicher Überwachung.



Implementierung von KI

Protiviti unterstützt Sie bei der erfolgreichen Entwicklung und Anwendung von KI-Lösungen, die besonders spezifische Unternehmensherausforderungen oder Chancen betreffen. Dazu gehören die Prüfung anfänglicher Hypothesen und technischer Herausforderungen, die Definition von eindeutigen Zielen für KI-Projekte, die Auswahl geeigneter KI-Methodologien und Zuteilung von Ressourcen, die Sicherstellung einer engen Zusammenarbeit zwischen allen relevanten Stakeholdern und die Entwicklung und Umsetzung einer starken Governance.

Absicherung Ihrer KI

Protiviti unterstützt Sie dabei, KI-Systeme und Daten vor potenziellen Bedrohungen zu schützen sowie bei der Sicherstellung einer ethischen und verantwortungsvollen Nutzung. Dazu gehört die Implementierung von robusten Cybersicherheitsmaßnahmen, um KI-Modelle zu sichern, das Adressieren von KI-Verzerrungen und Fairness-Bedenken und das Einhalten von ethischen Richtlinien und regulatorischen Anforderungen (z. B. Transparenz, Privatsphäre).

Protiviti unterstützt Sie nicht nur auf Ihrer KI-Reise, sondern stellt ebenso sicher, dass Sie dabei alle Aspekte und Anforderungen des EU AI Acts erfüllen.

Ansprechpartner

SEBASTIAN MAYER
Managing Director
+49 162 272 58 55
sebastian.mayer@protiviti.de
www.protiviti.de

KENTARO ELLERT
Associate Director
+49 160 910 512 87
kentaro.ellert@protiviti.de
www.protiviti.de

+49 69 963 768 100
contact@protiviti.de
www.protiviti.de

Die Autorin dankt Constantine Boyadjiev, Managing Director Protiviti New York, und Denis Lippolt, Director Protiviti Frankfurt, für ihre Mithilfe an diesem Artikel.

Über die Autorin

Carol Beaumier ist Senior Managing Director im Bereich Risiko und Compliance bei Protiviti und Leiterin der APAC Financial Services Practice des Unternehmens. Sie ist in Metro D.C. ansässig und verfügt über mehr als 30 Jahre Erfahrung mit einem breiten Spektrum im Bereich regulatorischer Angelegenheiten über zahlreiche Branchen hinweg. Bevor sie zu Protiviti kam, war Beaumier Partnerin für Regulatory Risk Services bei Arthur Andersen und Managing Director und Gründungspartnerin der The Secura Group, wo sie den Bereich Risikomanagement leitete. Vor ihrer Tätigkeit als Beraterin arbeitete Beaumier elf Jahre lang für das U.S. Office of the Comptroller of the Currency (OCC), wo sie als Prüferin mit Fokus auf multinationale und internationale Banken tätig war. Sie war als Mitglied des OCC Senior Management Teams und Kontaktperson für Rechnungsprüfung für externe und interne Angelegenheiten der Behörde ebenfalls Direktionsassistentin für die Rechnungsprüfung. Beaumier tritt häufig als Autorin und Referentin zu regulatorischen und anderen Risikothemen in Erscheinung.

Protiviti (www.protiviti.com) ist ein weltweit tätiges Beratungsunternehmen, das fundiertes Fachwissen, objektive Erkenntnisse, einen maßgeschneiderten Ansatz und beispiellose Zusammenarbeit bietet, um Führungskräfte selbstbewusst in die Zukunft blicken zu lassen. Protiviti und seine unabhängigen und regional ansässigen Mitgliedsfirmen unterstützen Kunden mit Beratungsleistungen und Managed Solutions in Bezug auf Finanzen, Technologien, Operatives, Digitales, HR, Risiko und Interne Revision – mithilfe eines Netzwerkes von mehr als 90 Niederlassungen in über 25 Ländern.

Protiviti wurde zum zehnten Mal in Folge in die Liste der Fortune 100 Best Companies to Work For® aufgenommen und hat mehr als 80 Prozent der Fortune 100 und fast 80 Prozent der Fortune 500 Unternehmen betreut. Protiviti arbeitet ebenfalls mit Regierungsbehörden sowie kleineren und wachsenden Unternehmen zusammen, einschließlich solchen, die den Börsengang planen. Protiviti ist darüber hinaus eine hundertprozentige Tochter der Robert Half Inc. (NYSE: RHI).

© 2025 Protiviti Inc. Ein Arbeitgeber, der Chancengleichheit für Männer/Frauen/Behinderte/Veteranen bietet.

Protiviti ist nicht als Wirtschaftsprüfungsgesellschaft zugelassen oder registriert und gibt keine Einschätzung zu Finanzberichten oder anderen Bestätigungsleistungen ab.

protiviti®
Global Business Consulting