Trusted AI – Digitale Innovation

KPMG Schweiz

Die generative KI-Landschaft entwickelt sich rasant und Unternehmen sehen sich mit einem unregulierten «Wilden Westen» konfrontiert. Hier kommt Trusted AI ins Spiel. Unser innovatives Servicepaket unterstützt Unternehmen bei der Einhaltung komplexer und rechtlich bindender Vorschriften. Unsere hochmodernen KI-Tools befähigen Unternehmen, geltende Vorschriften einzuhalten und ethische Standards zu wahren. So können die revolutionären Möglichkeiten der KI verantwortungsvoll genutzt werden.

Regulatorische Sichtweise auf KI

Risiken und Grundlagen

Die Regulierung der KI wird in erster Linie durch die Notwendigkeit bestimmt, bestehende Rechts- und Verwaltungsvorschriften einzuhalten. Hinzu kommt das Bedürfnis der Wirtschaft, in einer sich rasch entwickelnden KI-Landschaft Vertrauen zu schaffen, Risiken zu mindern und ein nachhaltiges Wachstum zu gewährleisten. Für die Schweiz ist das EU-KI-Gesetz von Bedeutung, da auch die FINMA die internationalen Entwicklungen und den Umgang mit dem Thema bei den überwachten Instituten verfolgt.

Externe Anforderungen und Vorschriften

Das KI-Gesetz der EU wird demnächst verabschiedet und ist ein wesentlicher Schritt zur Regulierung von KI-Technologien in der Europäischen Union. Klare Richtlinien und Regeln für die KI-Entwicklung zielen darauf ab, Bedenken in Bezug auf Ethik, Sicherheit und Grundrechte auszuräumen. In der EU und der Schweiz tätige Banken und Versicherungen müssen sich auf diese neuen rechtlichen und regulatorischen Rahmenbedingungen vorbereiten. Nur so können sie KI-Systeme verantwortungsvoll, vertrauenswürdig und nachvollziehbar einsetzen. Infolge des gestiegenen Marktdrucks ist das EU-KI-Gesetz ab Januar 2024 in Kraft getreten und sieht eine zweijährige Übergangsfrist für die Umsetzung vor.

Intrinsische Treiber

Um das Vertrauen ihrer Kunden und Stakeholder zu gewinnen und ein positives Markenimage aufzubauen, bemühen sich Unternehmen um verantwortungsvolle und vertrauenswürdige KI-Praktiken. Die Einhaltung von vertrauenswürdigen KI-Praktiken stellt sicher, dass KI-Systeme gesellschaftlichen Werten entsprechen und einen positiven Beitrag zum gesellschaftlichen und ökologischen Wohlergehen leisten. Damit erreichen Sie Nachhaltigkeit und langfristiges Wachstum.

Passives Abwarten ist riskant

Ethische KI-Grundsätze und die Vermeidung von Verzerrungen sind der beste Weg für Unternehmen, rechtliche und finanzielle Risiken zu vermeiden, die sich aus diskriminierenden oder schädlichen KI-Ergebnissen ergeben.

01 **Drohende Verletzung von Gesetzen und Vorschriften**
Bei Diskriminierung, Datenschutzverletzungen oder Regelverstössen durch KI-Systeme können den Unternehmen rechtliche und regulatorische Sanktionen drohen.

02 **Imageschaden**
Wenn künstliche Intelligenz nicht vertrauenswürdig ist, führt dies zu negativer Publicity. Dies untergräbt das Vertrauen der Kunden und schadet dem Ruf des Unternehmens.

03 **Verzerrungen und Diskriminierung**
Ein unkontrollierter Einsatz von KI kann zu Ungleichbehandlung und Diskriminierung bestimmter Gruppen führen. Öffentliche Proteste und Reputationsschäden können die Folge sein.

04 **Wirtschaftliche Verluste**
Nicht regulierte KI-Systeme können unvorhersehbare Folgen haben. Es drohen finanzielle Verluste, wenn Sicherheitsverletzungen die Kundenzufriedenheit und damit den Umsatz beeinträchtigen.

Definition von KI-Systemen

Künstliche Intelligenz ist komplex und vielschichtig. Dies hat zu verschiedenen Definitionen geführt. Nachfolgend gehen wir auf die zwei wichtigsten Definitionen aus dem EU-KI-Gesetz und der OECD ein. Beide definieren KI-Systeme unter Berücksichtigung ihrer gesellschaftlichen Auswirkungen, um Wege für eine vertrauenswürdige Entwicklung und Einführung von KI aufzuzeigen.

Definition von KI-Systemen

Wie werden KI-Systeme in der EU-Gesetzgebung beschrieben? Die derzeitige Definition lautet wie folgt, unterliegt jedoch potenziellen Änderungen.

Andere Rechtsordnungen definieren KI-Systeme aus unterschiedlichen Blickwinkeln.

Definition im EU-KI-Gesetz [1]

*[1] Ein KI-System ist ein maschinengestütztes System, das so konzipiert ist, dass es mit unterschiedlichem Grad an Autonomie arbeiten soll und nach der Einführung Anpassungsfähigkeit zeigen kann und explizite oder implizite Ziele aus den Eingaben, die es erhält, ableitet, und Ergebnisse wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erzeugen kann, die physische oder virtuelle Umgebungen beeinflussen können;»

Die Definition stammt aus dem letzten veröffentlichten Entwurf des EU-KI-Gesetzes vom 26. Januar 2024.

Es besteht eine gewisse Ähnlichkeit der Definition des EU-KI-Gesetzes mit der OECD-Definition (siehe unten).

Definition der OECD [3]

Das Direktorat für Wissenschaft, Technologie und Innovation (STI) der OECD untersucht auf verschiedene Weise die Auswirkungen der Informations- und Kommunikationstechnologien (IKT) auf nachhaltiges Wirtschaftswachstum und soziales Wohlergehen. Unter einem KI-System versteht die OECD «ein maschinenbasiertes System, das in der Lage ist, die Umwelt zu beeinflussen, indem es Empfehlungen, Vorhersagen oder andere Ergebnisse für eine bestimmte Reihe von Zielen produziert.

Es nutzt maschinelle und/oder menschliche Eingaben/Daten, um:

1) Umgebungen wahrzunehmen;
2) diese Wahrnehmungen in Modelle zu abstrahieren; und
3) die Modelle zu verwenden, um Optionen für Ergebnisse zu formulieren. KI-Systeme sind so konzipiert, dass sie mit unterschiedlichen Graden von Autonomie arbeiten.»

Andere Definitionen

ISO (International Organization for Standardization) und IEC (International Electrotechnical Commission) bilden das weltweite Normungssystem, wobei nationale Gremien und Fachausschüsse an der Erarbeitung internationaler Normen beteiligt sind. Dies fördert sowohl die Harmonisierung als auch die Innovation.

Nach der Norm ISO/IEC 22989:2022 3.1.4 (4) ist ein KI-System ein «technisches System, das Ergebnisse wie Inhalte, Prognosen, Empfehlungen oder Entscheidungen für eine bestimmte, vom Menschen definierte Zielsetzung erzeugt.»

Wofür steht vertrauenswürdige KI und warum brauchen wir sie?

Vertrauenswürdige KI steht für die ethische und verantwortungsvolle Entwicklung, Einführung und Nutzung von Technologien der künstlichen Intelligenz. Nach den von der Europäischen Kommission veröffentlichten ethischen Leitlinien muss vertrauenswürdige KI gesetzeskonform, ethisch einwandfrei und robust sein.

Verantwortungsvolle KI ist für Unternehmen des Finanzsektors wie Banken und Versicherungen, aber auch für Softwareanbieter und -händler unverzichtbar. Nur wenn sie sicherstellen, dass KI-Systeme fair, transparent und sicher sind, werden sie das Vertrauen ihrer Kunden und der breiten Öffentlichkeit gewinnen. Damit vermeiden Unternehmen Rechts- und Reputationsrisiken, fördern gesellschaftlich nützliche Innovationen und stellen sicher, dass KI ethischen Grundsätzen entspricht. Dies trägt zu einer nachhaltigen und positiven Entwicklung von Gesellschaft und Umwelt bei.

Wie KPMG Sie unterstützen kann

Das Trusted AI-Angebot von KPMG umfasst ein Rahmenwerk, Kontrollen, Prozesse, Tools und Plattformen. Kunden können damit sicherstellen, dass KI-Systeme sicher und ethisch korrekt entwickelt und eingesetzt werden, und so den Geschäftswert deutlich steigern. Vertrauenswürdige KI stellt Unternehmen vor komplexe geschäftliche, regulatorische und technische Herausforderungen. Wir begleiten unsere Kunden dabei.

---

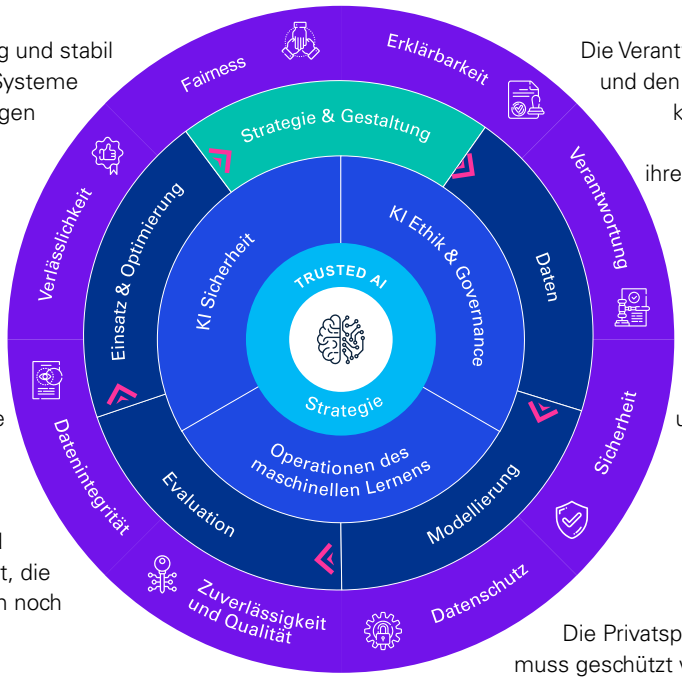
[1] EU-KI-Gesetz https://artificialintelligenceact.eu/the-act
[2] Definition des Ansatzes: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_2&format=PDF
[3] KI-Definition der OECD: https://www.oecd-ilibrary.org/docserver/2448f04b-en.pdf?expires=1689962519&id=id&accname=guest&checksum=65753939D1B3615FC89CF0A8EE506E4E
[4] ISO/IEC 22989:2022: https://webstore.iec.ch/publication/77839

Fairness
Der Begriff «Fairness» bedeutet, dass KI-Systeme unparteiische Prozesse und Ergebnisse liefern müssen, d. h. ohne Diskriminierung (z. B. aufgrund von Geschlecht, Rasse, Alter oder anderen Faktoren) von Einzelpersonen oder Gruppen.

Verlässlichkeit
KI-Systeme müssen zuverlässig und stabil sein. Dies bedeutet, dass die Systeme unter verschiedenen Bedingungen und Umständen konstant und genau funktionieren müssen.

Integrität
KI-Systeme müssen genau, konsistent und vertrauenswürdig sein. Daher dürfen während des gesamten Lebenszyklus keine falschen Informationen oder manipulierte Daten verwendet werden.

Zuverlässigkeit und Qualität
KI-Systeme müssen sicher und zuverlässig arbeiten. Das heisst, die Systeme dürfen weder Mensch noch Umwelt schaden.



Erklärbarkeit
KI-Systeme müssen in einer klaren, transparenten und nachvollziehbaren Weise funktionieren. Dies bedeutet, dass Entscheidungen und Prozesse der Systeme für Nutzer und Betroffene nachvollziehbar und erklärbar sind.

Verantwortlichkeit
Die Verantwortlichkeiten für die Entwicklung und den Einsatz von KI-Systemen müssen klar definiert sein. Dadurch können Systementwickler und -nutzer für ihre Handlungen und Entscheidungen in der Entwicklung und für die Ergebnisse verantwortlich gemacht werden.

Sicherheit
KI-Systeme müssen vor unbefugtem Zugriff, Missbrauch und Cyber-Bedrohungen geschützt werden. Das bedeutet, dass die Systeme sicher und robust gegen Bedrohungen von aussen und innen sein müssen.

Datenschutz
Die Privatsphäre der Nutzer von KI-Systemen muss geschützt werden. Die Systeme dürfen also keine persönlichen und sensiblen Daten abrufen, sammeln oder weitergeben.

Unsere acht Grundprinzipien für vertrauenswürdige KI im gesamten KI/ML-Lebenszyklus

Fairness
Die Modelle müssen unverzerrt und fair sein.

Erklärbarkeit
KI muss verständlich, dokumentiert und nachvollziehbar sein.

Verantwortung
Die Verantwortlichkeit muss durch geeignete Massnahmen während des gesamten Lebenszyklus sichergestellt werden.

Sicherheit
Das System muss vor unberechtigtem Zugriff, Verfälschung oder Angriffen geschützt sein.

Datenschutz
Dabei müssen sie die Bestimmungen zum Datenschutz und zur Verwendung von Verbraucherdaten einhalten.

Zuverlässigkeit und Qualität
Künstliche Intelligenz darf keine negativen Auswirkungen auf Menschen, Eigentum oder Umwelt haben.

Datenintegrität
Hochwertige Datenqualität, -kontrolle und -anreicherung schafft Vertrauen.

Verlässlichkeit
KI-Systeme müssen das gewünschte Mass an Präzision und Konsistenz aufweisen.

Was wir Ihnen bieten

Unsere Trusted AI Solution Suite unterstützt umfassend den gesamten KI-Lebenszyklus, von der Modellauswahl auf Basis spezifischer Anwendungsfälle bis hin zur Datenanalyse. Unsere Dienstleistungen umfassen auch die Bewertung von Daten im Hinblick auf Ethik, Verzerrungen, Nachhaltigkeit und Datenschutz. Dies gewährleistet eine verantwortungsvolle und transparente KI-Entwicklung. Besonderen Wert legen wir auch auf ein Risikomanagement, das den aufsichtsrechtlichen Standards entspricht. So bewegen Sie sich mit Zuversicht und unter Einhaltung der Vorschriften durch die sich wandelnde KI-Landschaft und vermeiden potenzielle Fallstricke.

AI Governance Health Check:
- Bewertung Ihrer KI-Konformität und Ihrer Modelle anhand der Standards im EU-KI-Gesetz
- Umsetzbarer Schritte zur Einhaltung von Vorschriften
- Modulare Dienstleistungen für individuelle Bedürfnisse
  – Bewertungen
  – technische Überprüfung von Modellen
  – Prüfsicherheit & Zertifizierung

Trusted AI Beurteilung von Modell und Algorithmus:
Evaluierung von KI-Modellen auf Erklärbarkeit, Verzerrung, Fairness und Genauigkeit.
- Verbesserte KI-Praktiken zur Modellverbesserung und Festlegung von Best Practices.
- Zusammenfassung der Ergebnisse und umsetzbare Empfehlungen.

KI-Governance-Rahmenwerk für Finanzinstitute:
- Risiken reduzieren durch ethische Nutzung von KI und Einhaltung von Vorschriften.
- Vertrauen schaffen, Entscheidungen verbessern, Wettbewerbsvorteile erzielen und die langfristige Nachhaltigkeit fördern.
- Umsetzung beschleunigen, bewährte Verfahren anwenden und unvoreingenommene Bewertungen gewährleisten.
- Ressourcen optimieren und organisatorische Veränderungen ermöglichen und zugleich Transparenz, Verantwortlichkeit und ethische Nutzung von KI fördern.

Nutzen

Die Wahl eines Dienstleisters ist nicht nur eine Entscheidung. Sie ist Ausdruck Ihres Engagements für Spitzenleistungen, Ethik und Vertrauenswürdigkeit. Wir sind mit den Werten vertraut, die Ihre Branche ausmachen – Integrität, Vertrauen, Stabilität, Kundenorientierung und Innovation. Unsere Trusted AI Solution Suite ist mehr als nur eine Lösung, sie ist die Verkörperung dieser Werte.

Passives Abwarten ist riskant

01 Verbesserte Transparenz und Vertrauen
Durch Transparenz in der Entscheidungsfindung stärkt Trusted AI das Vertrauen Ihrer Kunden und Stakeholder.

02 Reduzierung von Verzerrungen und Diskriminierung
Für faire und gerechte Ergebnisse minimiert Trusted AI die Verzerrungen und Diskriminierungen in KI-Algorithmen.

03 Verbesserte Entscheidungsfindung
Zuverlässige KI-Systeme führen zu fundierteren Entscheidungen und verbesserter betrieblicher Effizienz.

04 Einhaltung rechtlicher und ethischer Regeln
Trusted AI befähigt Finanzinstitute, regulatorische Anforderungen und ethische Standards einzuhalten.

05 Wettbewerbsvorteil
Unternehmen, die Trusted AI priorisieren, sind für diejenigen Kunden, Arbeitnehmer und Investoren attraktiv, die Wert auf ethische und vertrauenswürdige Praktiken legen.

Mit uns als Partner an Ihrer Seite verwirklichen Sie Ihre Visionen. Unsere Experten unterstützen Sie bei der Entwicklung, Bereitstellung und Bewertung von KI-Systemen, die vertrauenswürdig, ethisch einwandfrei und fair sind. Dadurch stärken Sie Ihre Mitarbeitenden und Ihr Unternehmen und schaffen gleichzeitig einen Mehrwert für Ihre Kunden und die Gesellschaft. Unser Engagement für zuverlässige, ethische und vertrauenswürdige Finanzpraktiken deckt sich nahtlos mit Ihren Zielen. Wir freuen uns darauf, Sie mit unserem Fachwissen zu unterstützen und Ihre Vision Wirklichkeit werden zu lassen.

Kontakte

KPMG AG
Badenerstrasse 172
Postfach
CH-8036 Zürich

kpmg.ch

Thierry Kellerhals
Director, Digital Innovation
Financial Services

+41 58 249 44 84
tkellerhals@kpmg.com

Fabian Meier
Director, Risk Management
Financial Services

+41 79 669 06 36
fabianmeier@kpmg.com

Die hierin enthaltenen Informationen sind allgemeiner Natur und beziehen sich daher nicht auf die Umstände einzelner Personen oder Rechtsträger. Obwohl wir uns bemühen, genaue und aktuelle Informationen zu liefern, besteht keine Gewähr dafür, dass diese die Situation zum Zeitpunkt der Herausgabe oder eine künftige Situation akkurat widerspiegeln. Die genannten Informationen sollten nicht ohne eingehende Abklärungen und professionelle Beratung als Entscheidungs- oder Handlungsgrundlage dienen. Bei Prüfkunden bestimmen regulatorische Vorgaben zur Unabhängigkeit des Prüfers den Umfang einer Zusammenarbeit. Sollten Sie mehr darüber erfahren wollen, wie KPMG AG personenbezogene Daten bearbeitet, lesen Sie bitte unsere Datenschutzerklärung, welche Sie auf unserer Homepage **www.kpmg.ch** finden.

© 2025 KPMG AG, eine Schweizer Aktiengesellschaft, ist eine Gruppengesellschaft der KPMG Holding LLP, die Mitglied der globalen KPMG-Organisation unabhängiger Firmen ist, die mit KPMG International Limited, einer Gesellschaft mit beschränkter Haftung englischen Rechts, verbunden sind. Alle Rechte vorbehalten.