EU AI Act The imperative to build AI Governance



Mai 2024









Das EU-KI-Gesetz wird wahrscheinlich ab 2025 umgesetzt werden müssen und sieht drastische Strafen für die Nichteinhaltung vor

Zeitleiste

Voraussichtliches Inkrafttreten Sommer 2024

Verbotene KI-Systeme
6 Monate nach Inkrafttreten

Codes of Practice
9 Monate nach Inkrafttreten

Sanktionen treten in Kraft

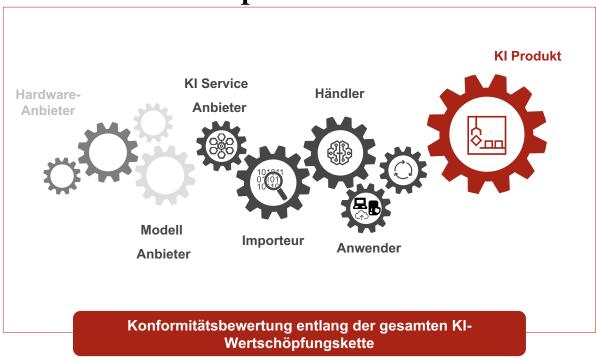
12 Monate nach Inkrafttreten

GPAI Verordnung12 Monate (24 Monate, wenn bereits auf dem Markt)

Alle anderen Aspekte des EU Al-Act (z.B. hohes Risiko)
24 Monate nach Inkrafttreten

Produktbasierte KI-Systeme mit hohem Risiko 36 Monate nach Inkrafttreten

Es ist an der Zeit, Ihre KI-Governance zu optimieren!



Die Geldbußen bei Nichteinhaltung der Vorschriften betragen bis zu 40 Mio. EUR oder 7% des Jahresumsatzes.



Die Auswirkungen des EU AI Acts hängen stark von den Use-Cases und der jeweiligen Rolle der Unternehmen ab

EU AI Act

1

Relevanz des EU Al Acts

KI Definition

Bewertung, ob es sich per Definition des EU AI Acts (OECD Definition für KI) um eine Künstliche Intelligenz handelt.

Verwendungszweck

Bestimmung des KI Verwendungszwecks zur Bewertung der EU AI Act Relevanz (Aktivitäten die bereits durch anderen Regularien abgedeckt sind (z.B. autonomes Fahren) sind nicht durch den AI Act reguliert).

 $(\mathbf{2})$

Risikoklassifizierung (wenn nicht verboten)

Hohes Risiko

KI-Systeme, die beispielsweise durch den Einsatz im HR Bereich, zur Bereitstellung von Fortbildungsmöglichkeiten oder in kritischen Infrastrukturen mit einem besonders hohen Risiko verbunden sind.

General Purpose Al/ GenAl

Häufig auf sehr viele Datenquellen und große Datenmengen trainiert, um eine Vielzahl von Aufgaben zu erfüllen. GenAl ist speziell für die Generierung von Inhalten wie Text, Bilder oder Audio gedacht.

Zusätzliche Transparenzanforderungen

Wenn ein KI-System zur Erzeugung von Text-, Audio- oder visuellen Inhalten genutzt wird oder für die Interaktion mit natürlichen Personen bestimmt ist, gelten zusätzliche Anforderungen.



Rollen innerhalb der KI Wertschöpfungskette

Anbieter

Entwickler des KI-Systems, die Einrichtung, die das KI-System auf den Markt bringt oder unter ihrem Namen Marke in Betrieb nimmt.

Bevollmächtigter

Natürliche oder juristische Person, die vom Anbieter dazu bevollmächtigt wurde, in seinem Namen die im EU AI Act festgelegten Pflichten zu erfüllen.

Nutzer

Natürliche oder juristische Person, einschließlich einer Behörde oder sonstigen Einrichtung, unter deren Aufsicht das System genutzt wird.

Händler

Natürliche oder juristische Person in der Lieferkette, die ein KI-System auf dem europäischen Markt bereitstellt und nicht Anbieter oder Importeur ist.

Importeur

Person, die in der EU ansässig ist und das KI-System einer Person außerhalb der EU auf dem europäischen Markt in Verkehr bringt.



Einhaltung definierter Governance Vorgaben

Organisation

Organisatorische Anforderungen sind unternehmensweit zu etablieren und betreffen unmittelbar die 2nd Line of Defense. Darunter fällt z.B. die Befähigung der gesamten Organisation durch Awareness Programme, die Etablierung eines Code of Conduct sowie KI Risikomanagement Prozessen.

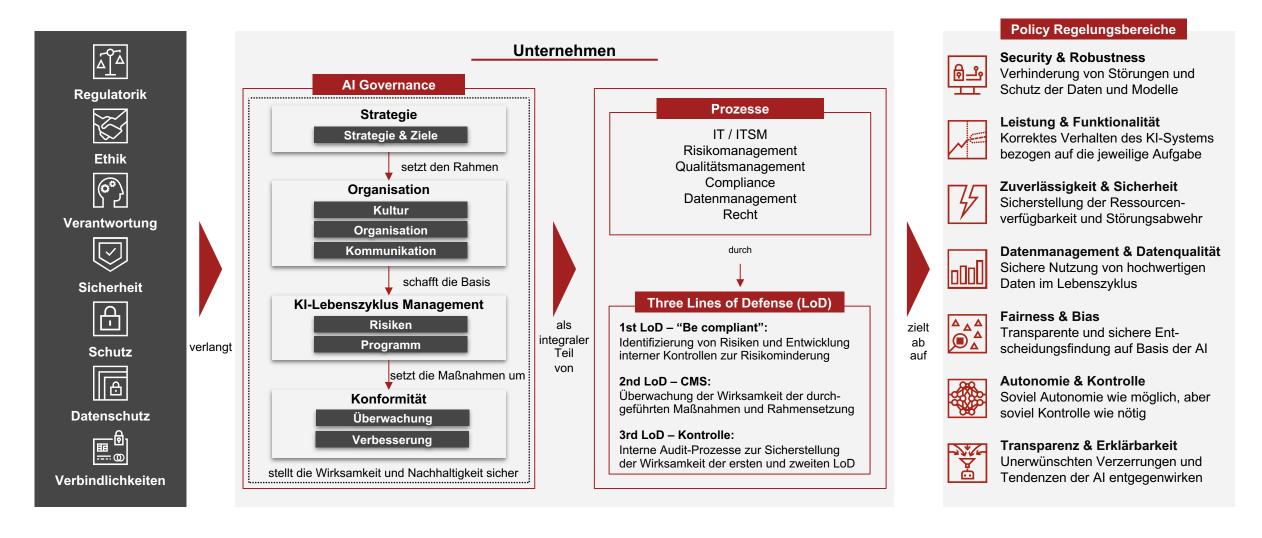
Lebenszyklus

Für jede Phase des KI-Lebenszyklus (auf Basis des aktuellen IT Lebenszyklus) sind eigene Prozesse notwendig. Dies beginnt mit der rechtssicheren Klassifikation der KI während der Ideenfindung und reicht bis zur Stilllegung des Systems. Diese Vorgaben sind insbesondere durch die 1st Line of Defense einzuhalten.

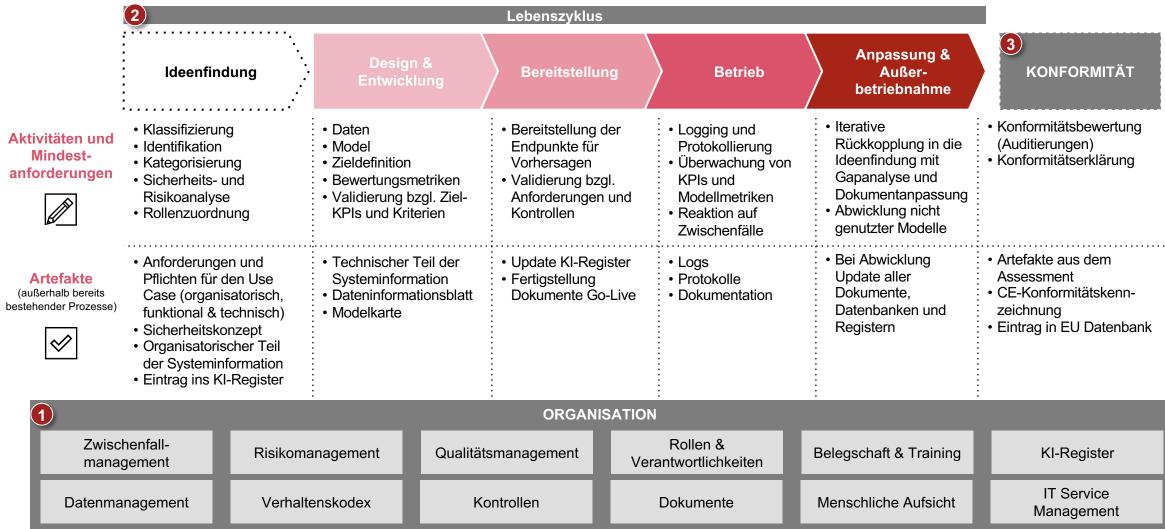
Überwachung/ Konformität

Konformitätsbewertungen gemäß EU AI Act müssen je nach Use-Case mit Hilfe externer Notified Bodies oder auf Basis interner Kontrollbewertungen (z.B. durch Internal Audit/ 3rd Line of Defense) durchgeführt werden. Dabei spielen die Einhaltung von Dokumentationsanforderungen und Kontrollen eine zentrale Rolle.

Das AI Governance Framework als integraler Bestandteil etablierter Prozesse zur Befähigung für einen verantwortungsvollen Umgang mit KI

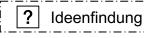


Unser integrierter KI-Lebenszyklus sorgt für eine strukturierte KI-Entwicklung vertrauenswürdiger KI auf Grundlage von Best Practice





Während des gesamten KI-Lebenszyklus wird sichergestellt, dass die KI-Lösung sicher, nachhaltig und skalierbar bereitgestellt wird





Design & Entwicklung



Deployment



Operation

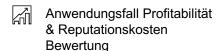


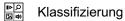
Anpassung & Ruhestand

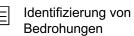
Umfasst alle Aktivitäten, die sich mit dem Sammeln, Speichern, Übertragen, Transformieren und Aufbereiten von Daten für das Training, die Validierung und das Testen eines KI-Systems befassen.

Umfasst alle Aktivitäten, die sich mit der Implementierung des Modells, der Auswahl der Leistungskennzahlen und der Überprüfung der Erklärbarkeit und des Bias befassen Beinhaltet alle Schritte, die notwendig sind, um das Modell anhand der Metriken zu validieren, die Fairnessund Bias-Metriken während des Betriebs zu messen und die Leistung zu erhalten. Umfasst alle Maßnahmen zur Wartung und Umschulung des KI-Systems sowie die Ausmusterung von Komponenten oder Systemen, die nicht mehr benötigt werden.

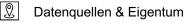
Erstellung des KI-Anwendungsfalls als integraler Bestandteil der Lebenszyklusprozesse



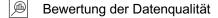




A Risikobewertung







Vorbereitung der Daten

Modell Architektur

Auswahl der Leistungsmetriken



Technische Dokumentation



Überprüfung der Robustheit



Bias und Fairness



Erklärbarkeit und Interpretierbarkeit



Leistungsmessung



Menschliche Interaktion



KI-System-Sicherheit



Protokollierung, Überwachung und Notfallmanagement



Umschulung



Software-Updates und Wartung









Thank you.

pwc.de/responsible-ai



Hendrik Reese
Responsible AI Lead, DE
hendrik.reese@pwc.com



© 2024 PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft.

All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, which is a member firm of PricewaterhouseCoopers International Limited (PwCIL). Each member firm of PwCIL is a separate and independent legal entity.