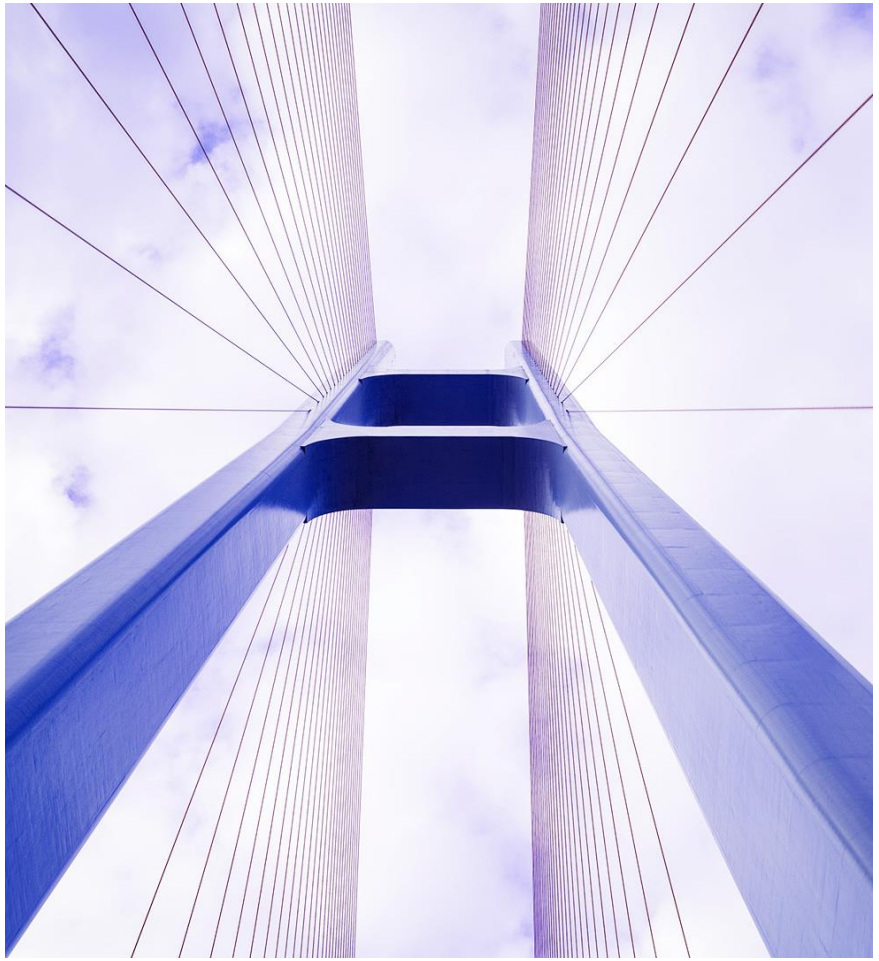
KPMG

EU AI Act und der Umgang mit KI

Herausforderung im Mittelstand

März 2025



Inhaltsverzeichnis

01

Einsatz von KI im Mittelstand

Bedeutung von Künstlicher Intelligenz für den Mittelstand

KI als Game-Changer

KI als Game-Changer für den Mittelstand

Künstliche Intelligenz optimiert Arbeitsprozesse und ermöglicht neue Arbeitsmodelle.

Weniger Aufwand, mehr Effizienz

Durch KI-gestützte Automatisierung werden Verwaltungsaufgaben schneller und präziser erledigt.

Automatisierte Textgenerierung hilft, Kundenanfragen effizient zu beantworten – mit menschlicher Kontrolle.

Kreativität statt Routinearbeit

KI übernimmt standardisierte Aufgaben, sodass Mitarbeiter mehr Freiraum für Innovationen haben.

Von der Vier-Tage- zur Drei-Tage-Woche

Prozessoptimierung mit KI ermöglicht den nächsten Schritt in die Zukunft der Arbeit.

Süddeutsche Zeitung 27. Februar 2024, 12:24 Uhr

In der Verwaltung des niederbayerischen Unternehmens gilt bereits die Vier-Tage-Woche. Bald sollen die Büromitarbeiter noch weniger arbeiten - auch dank künstlicher Intelligenz.

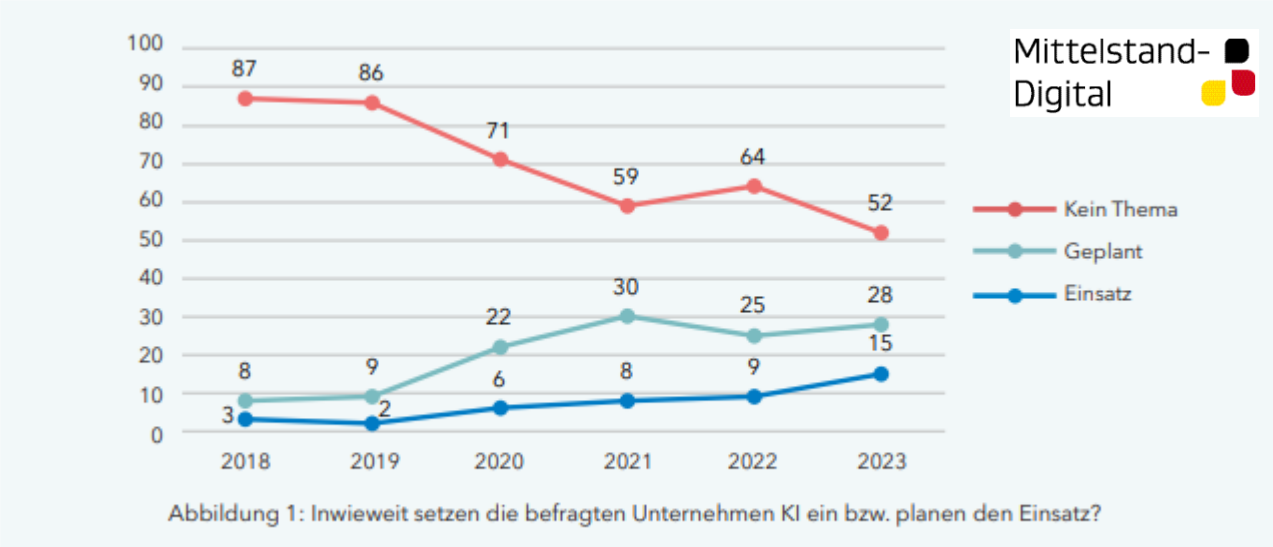
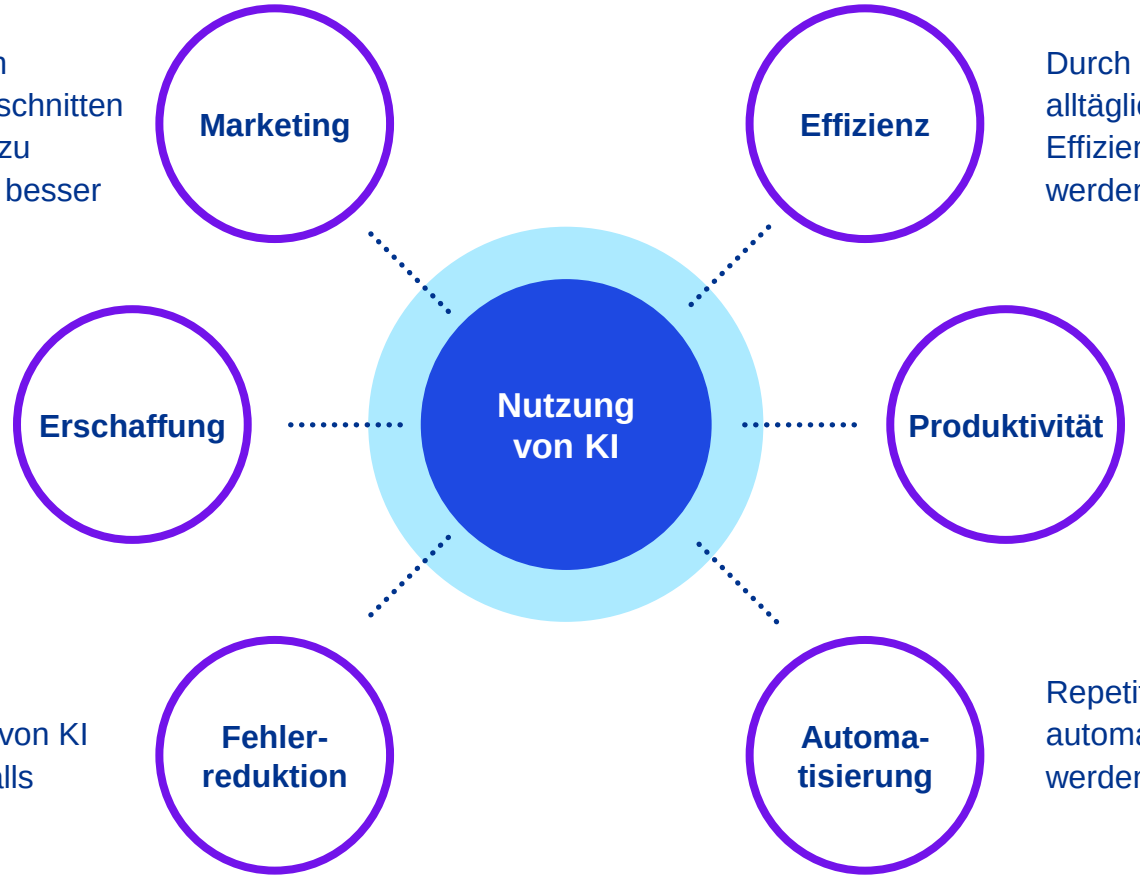


Abbildung 1: Inwieweit setzen die befragten Unternehmen KI ein bzw. planen den Einsatz?

Quelle: Vgl. Bitkom (2023), S. 4.

Bedeutung von Künstlicher Intelligenz für den Mittelstand



Durch Datenanalyse kann Werbung individuell zugeschnitten werden, um neu Kunden zu akquirieren und Produkte besser zu vermarkten.

Durch die Unterstützung bei alltäglichen Aufgaben kann die Effizienz deutlich gesteigert werden.

Durch Generative KI können Inhalte erzeugt werden, die bisher nicht oder nur mit viel Aufwand erstellbar waren (z.B. Grafiken/ Code).

Da einfache Aufgaben von KI abgenommen werden können, haben Mitarbeiter mehr Zeit für relevante Themen.

Flüchtigkeitsfehler und Unstimmigkeiten können von KI erkannt und gegebenenfalls korrigiert werden.

Repetitive Tasks können automatisiert abgearbeitet werden.

02

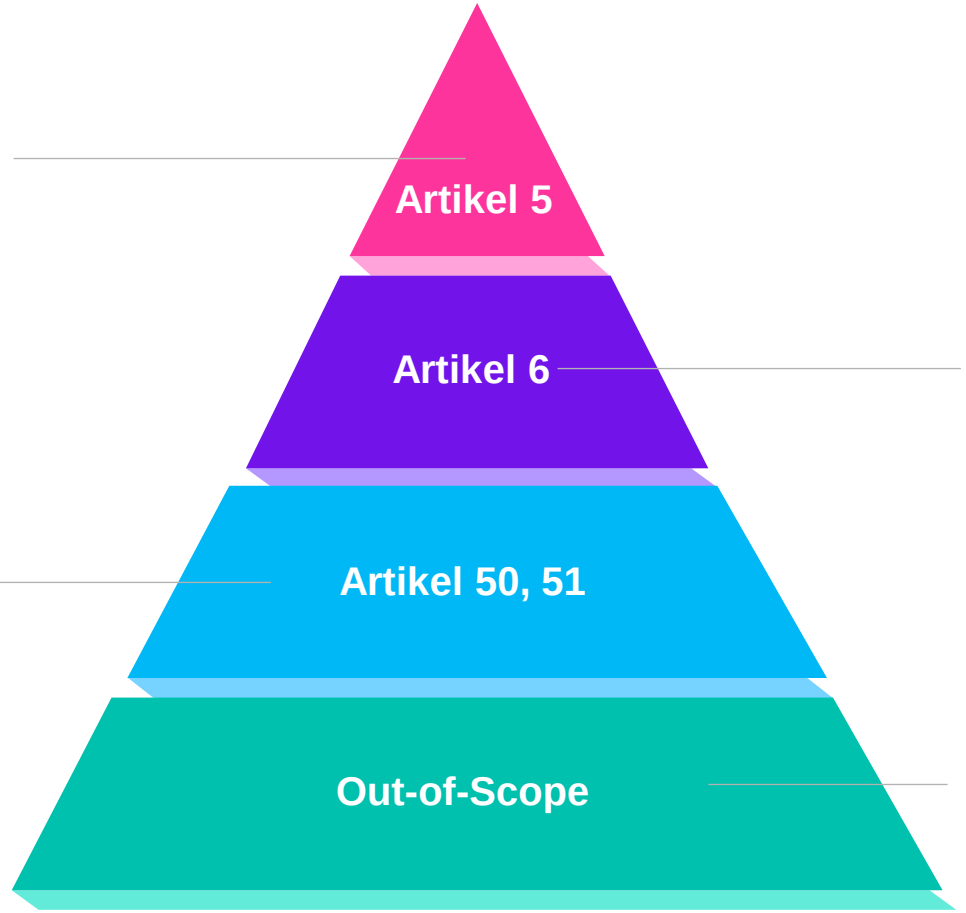
EU AI Act Anforderungen

Risikobasierte Regulierung von KI

Verbotene KI-Systeme

- Risikobewertung von Personen
- Ungezieltes Auslesen von Gesichtsbildern
- Biometrische Kategorisierung

(Massenmanipulation und Verletzung von Menschenrechten)



Hochrisiko KI-Systeme

- KI ist Sicherheitsbauteil oder Produkt selbst welches unter die Harmonisierungsvorschriften fällt

- Einsatz in KRITIS
- Allgemeine Berufliche Bildung
- Beschäftigung, Personalmanagement

KI-Systeme mit begrenztem Risiko

Transparenzverpflichtungen für KI-Systeme,

- Die mit natürlichen Personen interagieren
- Die synthetische Audio-, Bild, Text, Videoinhalte generieren
- General Purpose AI

Kein Risiko

- KI-Spam Filter
- Einsatz von KI in Videospielen.

Anforderungen High Risk (Artikel 9 – 25 EU AI Act)

Anforderungen an KI-System selbst

01

Risikomanagementsystem

Ermittlung, Abschätzung, Bewertung der Risiken
Ergreifen von gezielten Risikomanagementmaßnahmen

02

Data Governance

Einrichtung von Data-Governance und Datenverwaltungsverfahren, die für Zweckbestimmung des KI-Systems geeignet sind

03

Technische Dokumentation und Transparenz

Allgemeine Beschreibung des KI-Systems, Erläuterung der Bestandteile und des Entwicklungsprozesses

Konzeption und Entwicklung des KI-Systems müssen den im Betrieb hinreichend transparent sein

Anforderungen an die Betreiber

01

Konformitätsbewertungsverfahren

Interne/Externe Prüfung zum Nachweis, dass alle Anforderungen erfüllt sind.

02

Informationspflicht

Bei Feststellung der Nichtkonformität müssen korrigierende Maßnahmen ergriffen und betroffene Personen informiert werden

03

Qualitätsmanagementsystem

Zur Systematischen Gewährleistung der Konformität

Anforderungen Low Risk (Artikel 50 – 55 EU AI Act)

Unter Low Risk fallen verschiedene Kategorien von Use Cases

Regelung von GPAI

Transparenzpflichten im Bezug auf Technische Dokumentation, Trainingsverfahren, Urheberrecht

Generierung von Inhalten mittels KI

Die Inhalte müssen im maschinenlesbaren Format als KI-Output gekennzeichnet werden. (Im Einklang mit Umsetzungskosten und Besonderheiten der Inhalte)

KI-Systeme mit direkter menschlicher Interaktion

Diese Systeme müssen die natürliche Person informieren, dass diese mit einem KI-System interagiert.

Deepfakes

Explizite Pflicht zur Kennzeichnung solcher Inhalte als manipuliert

Schrittweise Inkrafttreten des EU AI Acts

August 2024

Inkrafttreten des EU AI Acts
Noch sind keine der Anforderungen in Kraft getreten.

2. Februar 2025

Inkrafttreten von:

- Verbot bestimmter KI-Systeme
- Anforderungen zum Aufbau von KI-Kompetenz

2. August 2025

Regelungen für GPAI-Modelle treten in Kraft

2. August 2026

Inkrafttreten aller anderen Regelungen mit Ausnahme von Artikel 6 Abs. 1 EU AI Act (Hochrisikosysteme im Bezug auf Harmonisierungsvorschriften der EU)

2. August 2027

Inkrafttreten Artikel 6 Abs. 1 EU AI Act.

03

IKS auf neuen Wegen

Internes Kontrollsystem (IKS) & Regulatorische Grundlagen

Aktiengesetz

§ 91 Abs. 2-3
§ 107 Abs. 3

Vorstände müssen ein Kontrollsystem einrichten, welches vom Aufsichtsrat überwacht wird.

Prüfungsstandards

ISA 315 rev.

IDW PS 860
Prüfung von IT-Systemen

IDW PS 861
Prüfung von KI-Systemen

Deutsche Corporate Governance Kodex

Grundsätze, Empfehlungen und Anregungen zur Leitung und Überwachung deutscher börsennotierter Gesellschaften

EU AI Act

Anwendungen mit hohem Risiko unterliegen besonderen rechtlichen Anforderungen

Der Gesetzgeber fordert zunehmend Unternehmen dazu auf, ihre Systeme zu überwachen.

Insbesondere mittelständische Unternehmen sind in der Verantwortung, sich durch interne Kontrollsysteme (IKS) abzusichern.

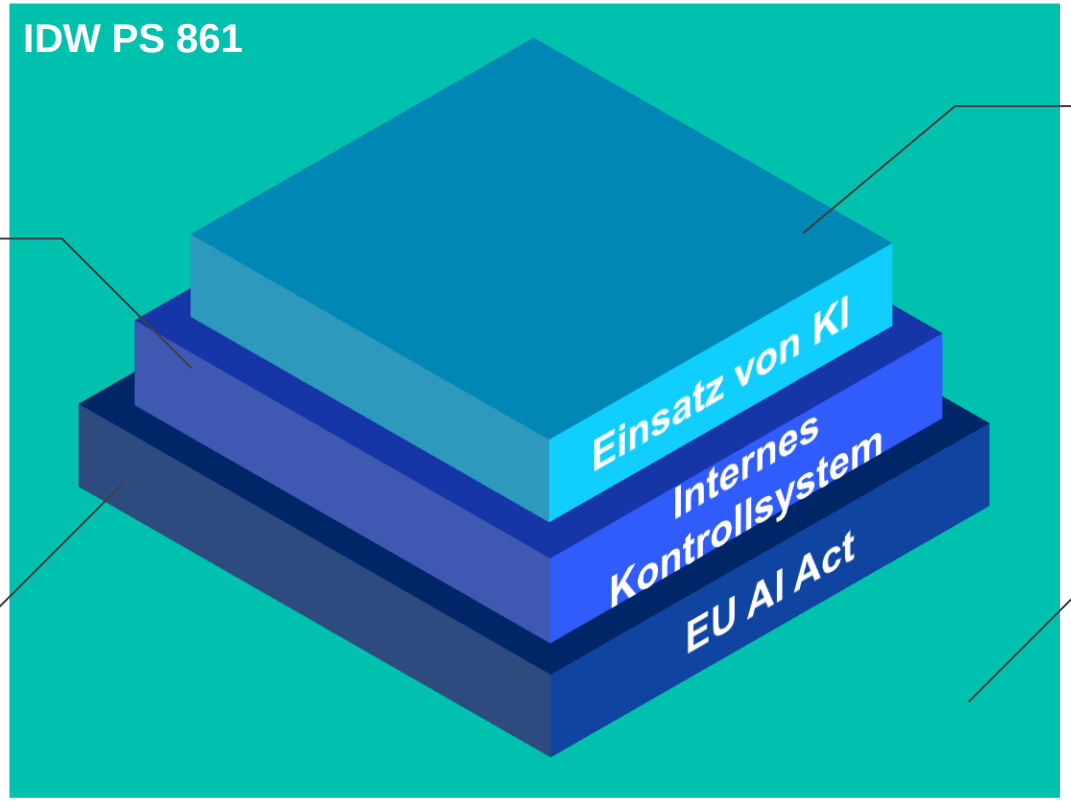
Anwendungsgebiete für den Einsatz von IKS:

- Sicherung der Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit (**Operativer Betrieb**)
- Ordnungsmäßigkeit und Verlässlichkeit der externen und internen Rechnungslegung (**Berichterstattung**)
- Einhaltung der für das Unternehmen maßgeblichen rechtlichen Vorschriften (**Compliance**)

Grundgerüst

Ein internes Kontrollsystem (IKS) ist notwendig, um den Einsatz der KI im Unternehmen zu überwachen.

Mit dem EU AI-Act wurde eine gesetzliche Grundlage geschaffen, nachdem sich Unternehmen, die KI einsetzten, richten müssen.



Der Einsatz von KI im Unternehmen unterliegt je nach Kritikalität Regulatorien, welche eingehalten werden müssen.

Das Institut der Wirtschaftsprüfer hat mit dem PS 861 den Prüfungsstandard für die Verwendung von KI-Systemen eingeführt.

04

Prüfungsstandard als Hilfestellung

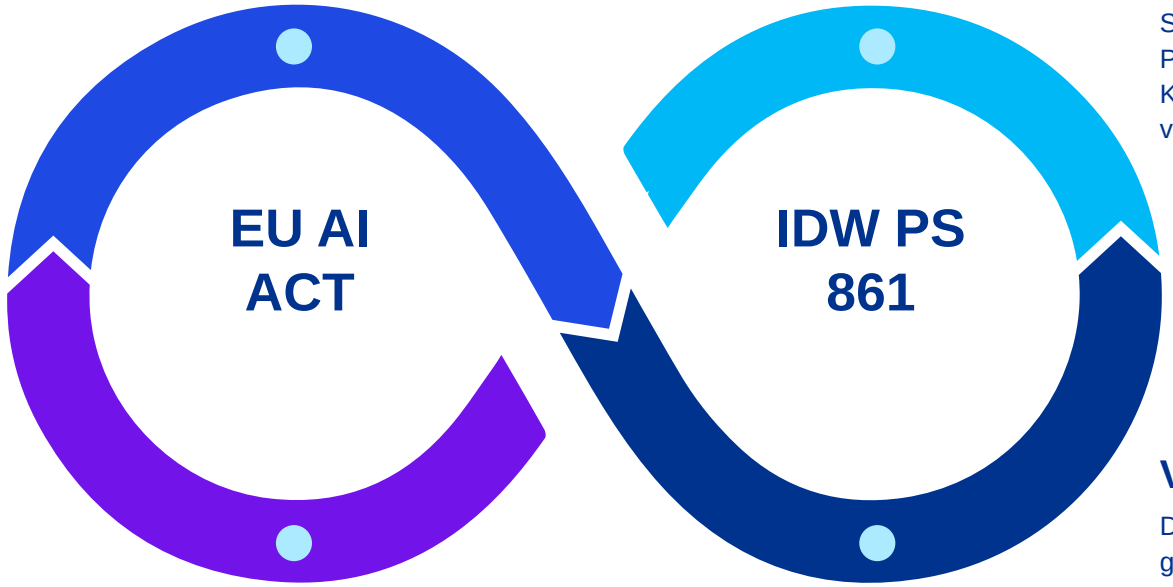
Zusammenspiel EU AI Act & PS 861

EU AI Act

Der “EU Artificial Intelligence Act” (kurz: „EU AI Act”) repräsentiert das weltweit erste umfassende Gesetz, welches auf die Regulierung von künstlicher Intelligenz (KI) abzielt.

IDW PS861

Während der EU AI Act die regulatorischen Anforderungen und Rahmenbedingungen für KI-Systeme festlegt, bietet der IDW-Prüfungsstandard: Prüfung von KI-Systemen (IDW PS 861) (03.2023) Kriterien zur Umsetzung einer einheitlichen Prüfung von KI-Systemen durch die Wirtschaftsprüfer.



IDW PS 861 Nutzen

Um dem steigenden Bedarf der Unternehmen nach standardisierten Prüfungen von KI-Systemen gerecht zu werden, kann die Wirtschaftsprüferbranche den IDW Prüfungsstandard IDW PS 861 nutzen.

Vereinbarkeit IDW PS 861

Der IDW 861 wurde bewusst offen und generisch gestaltet, um seine Vereinbarkeit mit verschiedenen Regelungen, einschließlich des EU AI Act, zu gewährleisten. Der Prüfungsstandard kann Anforderungen des AI Acts integrieren, die nicht bereits im PS 861 enthalten sind.

IDW PS 861 – Prüfungsbasis für KI

Abs. 3 Gegenstand, Ziel und Umfang der Prüfung

- Gegenstand der Prüfung ist die **Beschreibung des KI-Systems** einschließlich der in der Beschreibung enthaltenen Darstellungen der gesetzlichen Vertreter des Unternehmens, ob das beschriebene KI-System die Kriterien einhält
- Die Prüfung der Beschreibung des KI-Systems ist entweder in der Form einer **Angemessenheitsprüfung** oder einer **Wirksamkeitsprüfung** durchzuführen.

Abs. 4.1 Kriterien für die Ausgestaltung des KI-Systems

4.1.1 Anforderungen an das KI-System:
Ethische und rechtliche Anforderungen für künstliche Intelligenz, Nachvollziehbarkeit, IT-Sicherheit und Leistungsfähigkeit.
4.1.2 Maßnahmen bezogen auf die Elemente des KI-Systems

Abs. 4.2 Verantwortung der gesetzlichen Vertreter

Die gesetzlichen Vertreter sind verantwortlich für die Auswahl, Implementierung und Dokumentation des KI-Systems sowie für die Erstellung einer fehlerfreien Beschreibung und notwendige interne Kontrollen.

Abs. 4.3 Beschreibung des KI-Systems

Die Beschreibung des KI-Systems muss Aussagen der gesetzlichen Vertreter zu den Maßnahmen und bestimmte Mindestinhalte umfassen.

Elemente aus EU AI Act und PS 861 und konkrete Maßnahmen

KI-Governance
KI-Compliance
KI-Monitoring

Artikel 8, 9 EU AI Act

Es müssen eine klare Strategie und Organisation für KI-Systeme etabliert werden, die ethische und gesetzliche Vorgaben berücksichtigen, sowie ein kontinuierliches Risikomanagementsystem implementiert werden, um die Einhaltung der Anforderungen sicherzustellen.

Daten

Artikel 10 EU AI Act

Es muss sichergestellt werden, dass die Datenqualität, -beschaffung und -nutzung ethischen, rechtlichen und regulatorischen Anforderungen entsprechen, und Maßnahmen zur Erkennung und Korrektur von Bias sowie zur Sicherstellung der Datensicherheit und Nachvollziehbarkeit implementiert werden.

KI-Algorithmus
KI-Modell

Artikel 11, 15 EU AI Act

Es müssen Verfahren zur Entwicklung und Anpassung von KI-Algorithmen und -Modellen etabliert werden, die ethische Werte wie menschliche Autonomie, Fairness und Nichtdiskriminierung berücksichtigen, sowie technische Maßnahmen zur Überwachung der Leistungsfähigkeit, Genauigkeit und Sicherheit implementiert werden.

KI-Anwendung

Artikel 13 EU AI Act

Es muss sichergestellt werden, dass die Hochrisiko-KI-Systeme transparent gestaltet und durch klare und umfassende Gebrauchsanweisungen begleitet werden, um den Anwendern die Interpretation der Systemausgaben und deren angemessene Nutzung zu ermöglichen.

IT-Infrastruktur

Artikel 12, 15 EU AI Act

Die IT-Infrastruktur muss sachgerecht gestaltet und durch ein umfassendes Sicherheitskonzept geschützt werden, das logische Zugriffskontrollen, Schutz vor Schadprogrammen, physische Sicherheitsmaßnahmen und Datensicherungsverfahren umfasst, um die Cybersicherheit der KI-Systeme zu gewährleisten.

Der Weg zur EU AI Act Konformität

Um nachzuweisen, dass die KI alle Anforderungen erfüllt, kann der Anbieter folgende zwei Verfahren anwenden:

Art. 43 Abs. 1 lit. a EU AI Act

Bewertungsverfahren auf Grundlage der internen Kontrolle

Anbieter überprüft über seine internen Kontrollen die Konformität

Art. 43 Abs. 1 lit. b EU AI Act

Bewertung des QMS und der technischen Dokumentation durch externe Prüfer

Externe Prüfer bewerten die Konformität anhand der Prüfungsgrundlagen und den Anforderungen

Ein Internes Kontrollsystem (IKS) unterstützt sowohl bei der Bewertung der Konformität als auch bei der Aufrechterhaltung und Prüfung dieser.

Einhaltung der EU AI-Act Anforderungen

Durch ein schwaches IKS besteht die Gefahr des Verstoßes gegen den AI-Act.

Kontakt

KPMG AG
Wirtschaftsprüfungsgesellschaft

Georg Eder
Wirtschaftsprüfer, Steuerberater
Senior Manager, Digital Process Compliance
T +49 151 619 813 64
geder@kpmg.com

kpmg.de/socialmedia

kpmg.de