Hochschule
Magdeburg • Stendal

Artificial Intelligence Act

AI ACT

synerKI

DATA SCIENCE · FINANCE · MANAGEMENT & HR · MARKETING & SALES · OPERATIONS ·

Der **AI ACT** soll die Nutzung und Entwicklung von **Künstlicher Intelligenz (KI)** in der Europäischen Union regulieren, um die Grundrechte der Menschen zu schützen.

KI4Altmark.h2.de

CHECK für Unternehmen zur Nutzung und Einführung von KI

Was Unternehmen jetzt tun sollten ...

☑ Kategorisierung der KI-Anwendung nach Risikostufen vornehmen in

Verbotene KI (biometrische Massenüberwachung, soziale Bewertungssysteme, manipulative Systeme)
Hochrisiko-KI (kritische Infrastruktur, biometrische Identifikation, Kreditvergabe, Personalwesen)
Begrenztes Risiko (Chatbots, automatisierte Empfehlungssysteme)
Minimales Risiko (Spiele, Spam-Filter)

☑ Regulatorische Anforderungen je nach Risikostufen treffen

Registrierung in der EU-Datenbank für Hochrisiko-KI
Risiko- und Auswirkungen bewerten für Hochrisiko-KI (Bias, Diskriminierung, Sicherheit)
Konformitätsbewertungsverfahren durchführen für Hochrisiko-KI
Menschliche Kontrolle und Überwachungsmechanismen sicherstellen für Hochrisiko-KI
Strenge Transparenz- und Dokumentationspflichten einhalten, gilt bereits ab begrenztem Risiko

☑ Transparenz und Nachvollziehbarkeit sicherstellen

Interne und externe Audits für KI-Systeme einplanen
KI-Ethik-Richtlinien für das Unternehmen erstellen
Dokumentation zur Modellentwicklung und -nutzung führen
Erklärbarkeit und Interpretierbarkeit der KI-Modelle sicherstellen

☑ Cybersicherheit und Resilienz berücksichtigen

Verantwortlichkeiten festlegen (KI-Compliance-Beauftragte)
Datenschutz und DSGVO-Anforderungen sicherstellen
Datenqualität und -sicherheit gemäß EU-Vorgaben gewährleisten
Sicherstellen, dass die KI-Modelle gegen Manipulation geschützt sind
Regelmäßige Sicherheits- und Penetrationstests durchführen
Notfallplan für KI-Fehlfunktionen oder Missbrauch erstellen

☑ Mitarbeiterschulungen & Change Management anstoßen

Sensibilisierung der Belegschaft für den verantwortungsvollen Umgang mit KI
Schulung zu ethischen und rechtlichen Herausforderungen der KI-Nutzung
Klärung der Schnittstellen zwischen Mensch und KI in Geschäftsprozessen

CHECK Was ist der Artificial Intelligence Act - kurz AI ACT ?

Der **AI Act (Artificial Intelligence Act)** ist eine Verordnung der Europäischen Union (EU), die als weltweit erstes umfassendes Regelwerk die Entwicklung und Nutzung von **Künstlicher Intelligenz (KI)** reguliert. Der AI Act folgt einem risikobasierten Ansatz: Je höher das Risiko eines KI-Systems für Sicherheit oder Grundrechte, desto strenger die Anforderungen. Unternehmen, die KI-Systeme entwickeln oder einsetzen, müssen prüfen, ob ihre Systeme in den Anwendungsbereich fallen und gegebenenfalls Anpassungen vornehmen.

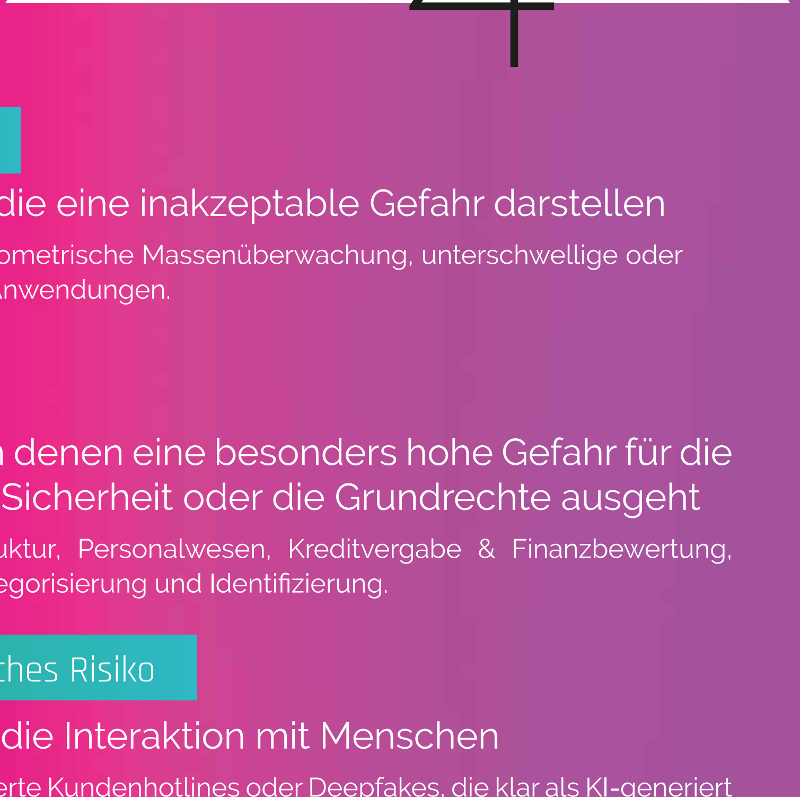
4 Die Kommission benennt für den angestrebten KI-Rechtsrahmen zentrale Ziele:

- **Gewährleistung, dass** die auf dem Unionsmarkt in Verkehr gebrachten und verwendeten **KI-Systeme sicher sind** und die **Grundrechte und Werte der Union wahren.**
- **Schaffung von Rechtssicherheit,** um Investitionen in KI und deren Innovativität zu fördern.
- **Stärkung von Governance und Durchsetzungsmechanismen** für geltendes Recht zur Wahrung der Grundrechte sowie der Sicherheitsanforderungen an KI-Systeme.
- **Erleichterung der Entwicklung eines Binnenmarktes** für rechtskonforme, sichere und vertrauenswürdige KI-Anwendungen sowie Verhinderung von Marktfragmentierung.

Was sind Risikoklassen?

Eine **Risikoklasse** beschreibt die **Einstufung eines KI-Systems** basierend auf seinem potenziellen Risiko für die Gesellschaft, Einzelpersonen oder grundlegende Rechte. Im **EU AI Act werden KI-Anwendungen nach ihrer Gefährdung** für Menschen und deren Rechte **in vier Risikoklassen unterteilt.**

Je höher die Risikoklasse, desto strenger sind die gesetzlichen Anforderungen an Sicherheit, Transparenz und Kontrolle.



Unzulässiges Risiko

KI-Systeme die eine inakzeptable Gefahr darstellen

Social Scoring, biometrische Massenüberwachung, unterschwellige oder manipulative KI-Anwendungen.

Hohes Risiko

Systeme von denen eine besonders hohe Gefahr für die Gesundheit, Sicherheit oder die Grundrechte ausgeht

Kritische Infrastruktur, Personalwesen, Kreditvergabe & Finanzbewertung, biometrische Kategorisierung und Identifizierung.

Mittleres & spezifisches Risiko

Systeme für die Interaktion mit Menschen

Chatbots, KI-basierte Kundenhotlines oder Deepfakes, die klar als KI-generiert gekennzeichnet werden müssen.

Geringes Risiko

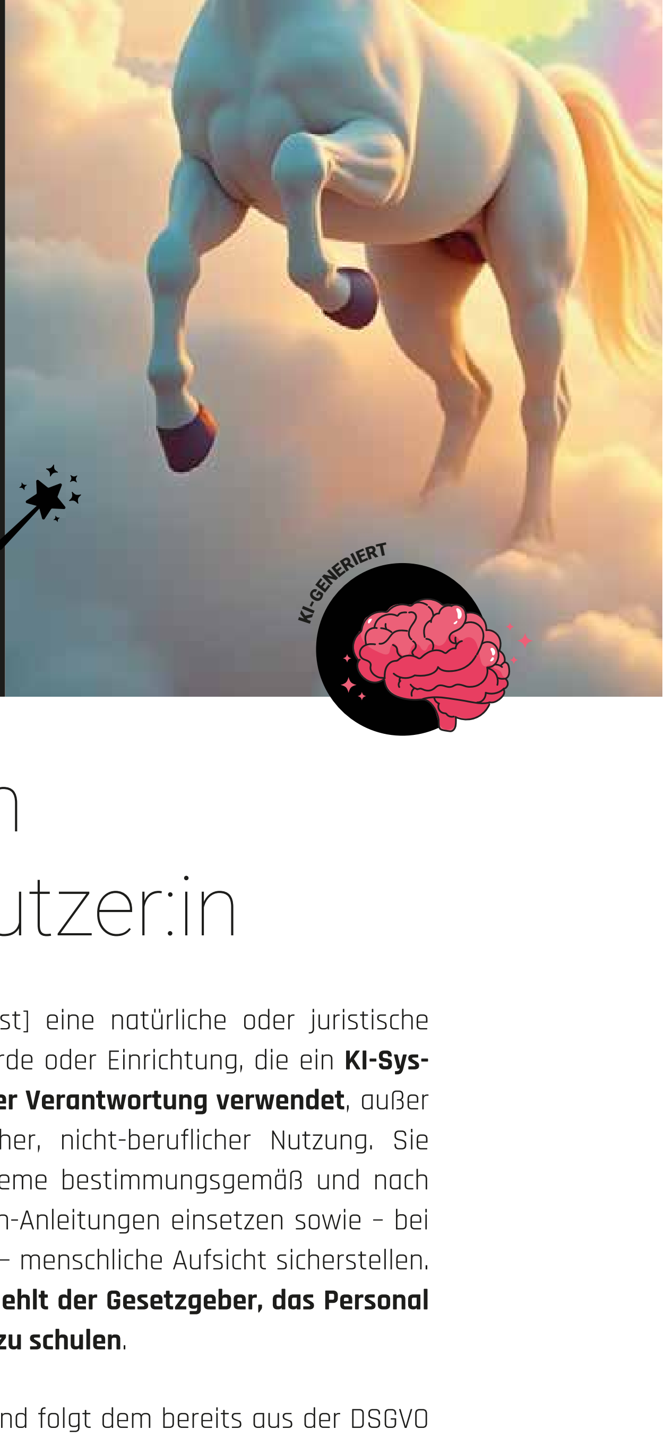
Systeme von denen keine expliziten Risiken ausgehen

Spam-Filter, Videospiele - AI Act sieht die Verpflichtung für Anbieter:innen und Nutzer:innen vor, beim Personal ein ausreichendes Maß an KI-Kompetenz („AI Literacy") herzustellen.

KENNZEICHNUNGSPFLICHT

- **Interaktionen mit einem KI-System müssen gekennzeichnet werden!** Es sei denn, es ist „offensichtlich", dass eine Interaktion mit einer Maschine stattfindet. Ob eine „offensichtliche" Interaktion mit einer Maschine stattfindet, wird dabei am Maßstab einer durchschnittlichen betroffenen Person gemessen.
- **Deepfakes** (Fotos, Video, Audio) müssen **eindeutig gekennzeichnet werden.**
- **KI-generierte Texte,** die zur öffentlichen Information über Angelegenheiten von öffentlichem Interesse dienen, **müssen klar als künstlich erzeugt oder manipuliert gekennzeichnet werden**.
- **KI-generierter Text** muss von den Nutzenden der KI-Anwendung **nicht gekennzeichnet werden**, **wenn** die **KI-generierten Inhalte einer menschlichen Überprüfung oder redaktionellen Kontrolle unterzogen wurden** und eine natürliche oder juristische Person die redaktionelle Verantwortung für die Veröffentlichung der Inhalte trägt.

MEHR INFOS



Unterscheidung in Anbieter:in und Nutzer:in

„Anbieter:in" [ist] eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein **KI-System oder** ein **KI-Modell** mit allgemeinem Verwendungszweck **entwickelt oder entwickeln lässt** und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich.

„Nutzer:in" [ist] eine natürliche oder juristische Person, Behörde oder Einrichtung, die ein **KI-System in eigener Verantwortung verwendet**, außer bei persönlicher, nicht-beruflicher Nutzung. Sie müssen Systeme bestimmungsgemäß und nach Anbieter:innen-Anleitungen einsetzen sowie – bei Hochrisiko-KI – menschliche Aufsicht sicherstellen. Zudem **empfiehlt der Gesetzgeber, das Personal ausreichend zu schulen**.

Der **AI Act** hat somit einen **extraterritorialen Anwendungsbereich** und folgt dem bereits aus der DSGVO bekannten **Marktortprinzip**, um eine **Umgehung des EU-Rechts zu verhindern.**

QUELLE Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) > http://data.europa.eu/eli/reg/2024/1689/oj

KONTAKT

FOLLOW synerKI!

PROF. DR.-ING.
FABIAN BEHRENDT
Projektleitung
fabian.behrendt@h2.de
03931 2187 3831

NADINE KALTSCHMIDT
Projektkoordination
nadine.kaltschmidt@h2.de
03931 2187 4860

FRANCES RUCH
Forschungskommunikation
frances.ruch@h2.de
0391 886 4710

KI4Altmark.h2.de

SACHSEN-ANHALT

Finanziert von der
Europäischen Union

Impressum

EFRE-Forschungsprojekt „synerKI"
synergetische KI-Lösungen für ganzheitliche Prozessoptimierung in Finance, HR & Management, Operations, Markting & Sales

c/o Hochschule Magdeburg-Stendal
Osterburger Str. 25 | 39576 Stendal

Redaktion & Gestaltung
Frances Ruch &
Nadine Kaltschmidt

Webseite