SEST digital

KI-Modelle mit allgemeinem Verwendungszweck

Welche Regeln gelten für die Allroundtalente?

Larissa Mikolaschek
Head of Tech - Sest Digital

IHK Industrie- und Handelskammern in Bayern

Larissa Mikolaschek

Head of Tech Sest GmbH
Software Engineer, AI-Expertin ;)

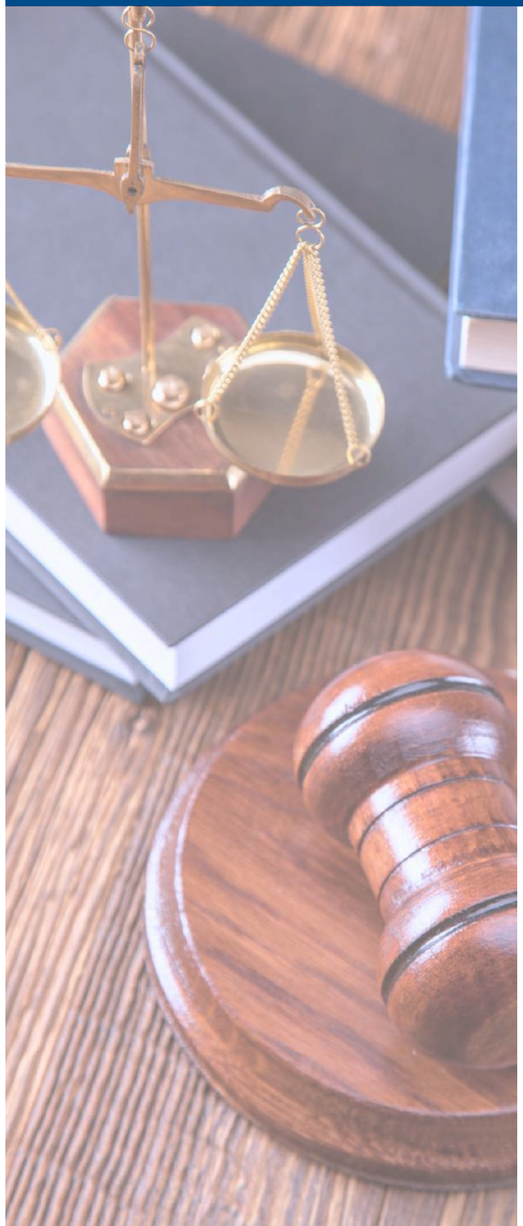
- **6+** Jahre Softwareentwicklung
- **10+** erfolgreiche (KI-) Softwareprojekte
- **100+** Trainings and Beratungen von Firmen im Bereich KI, Software und Strategie
- B.Sc. Mathematik, M.Sc.Informatik

Einführung AI-Act

- Erste umfassende Regulierung für KI weltweit
- Ziel: Risiken zu managen und Vertrauen in KI-Systeme zu schaffen.

- Seit 2. August 2024 in Kraft

- Zeitlich gestaffelte Anwendung der Regelungen:
  - **2.2.2025:** Verbot von KI-Systemen mit inakzeptablem Risiko
  - **2.8.2025:** Governance-Regeln und Verpflichtungen für General Purpose AI (GPAI) werden anwendbar
  - **2.8.2027:** Anwendung des gesamten EU AI Acts für alle Risikokategorien



IHK Industrie- und Handelskammern in Bayern

SEST digital

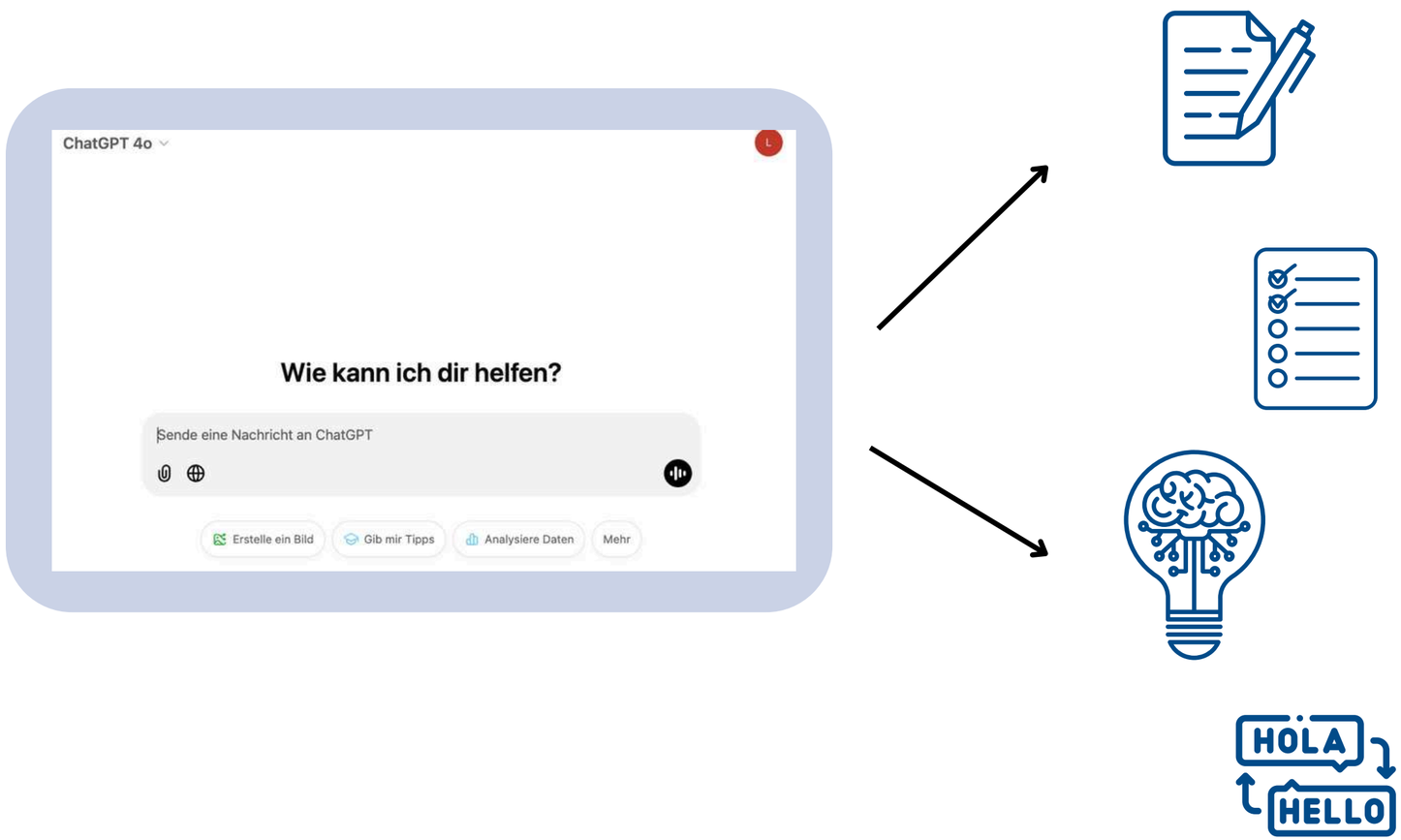
Was sind GPAI Modelle?

General Purpose AI-Modelle:

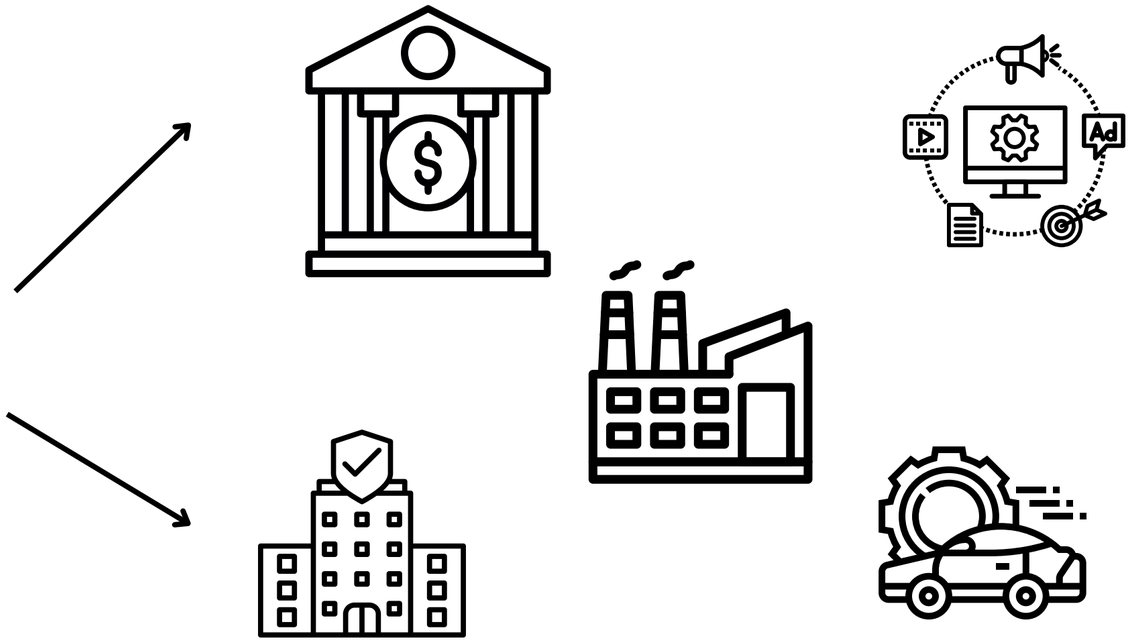
KI-Modelle, die eine erhebliche allgemeine Verwendbarkeit aufweisen, in der Lage sind, ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen, und in eine Vielzahl von nachgelagerten Systemen oder Anwendungen integriert werden können.

Art. 3 Nr. 63 KI-VO

Was sind GPAI Modelle?



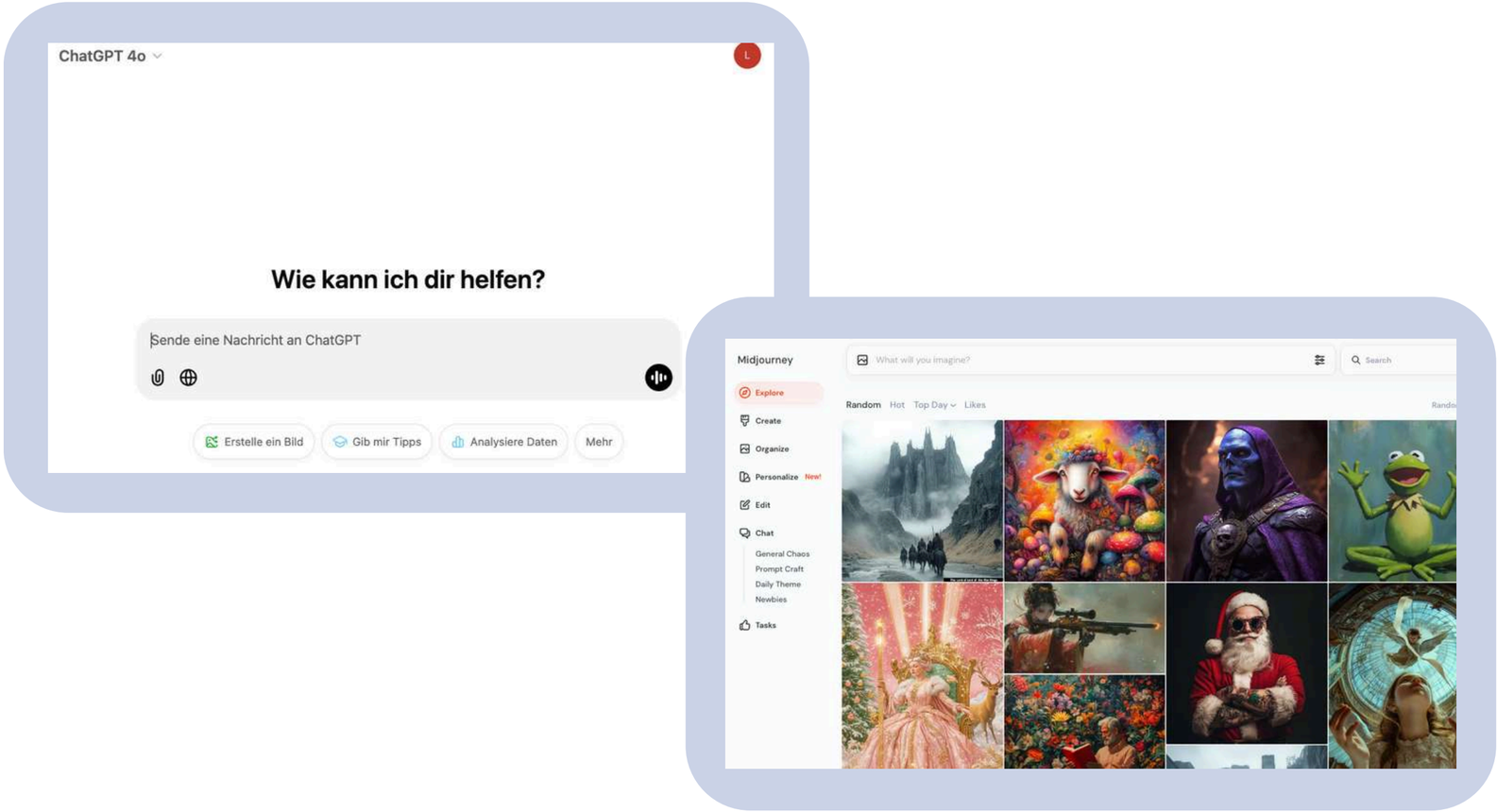
Was sind GPAI Modelle?



Was sind GPAI Modelle?

Bekannte Beispiele:

- ChatGPT
- Google Gemini
- Microsoft Copilot
- Midjourney, Stable Diffusion
- ...



Abgrenzung von GPAI zu anderen KI-Modellen

Abgrenzung von GPAI zu anderen KI-Modellen

Abgrenzung von GPAI zu anderen KI-Modellen

Abgrenzung von GPAI zu anderen KI-Modellen

Keine GPAI Systeme:

- Chatbot im Kundenservice
- Bilderkennung
- Predictive Maintenance
- Recommender-Systeme
- Fraud-Detection

IHK Industrie- und Handelskammern in Bayern

SEST digital

Chancen durch GPAI für Unternehmen

Produktivität

Automatisierung

Qualitätsgewinn

Analyse

Chancen durch GPAI für Unternehmen

Beispiel Personalisierung

- Maßgeschneiderte Marketingkampagnen auf Basis von Kunden Daten
- Individuelle Werbebotschaften & Content
- Höhere Conversion-Rates durch präzise Zielgruppenansprache

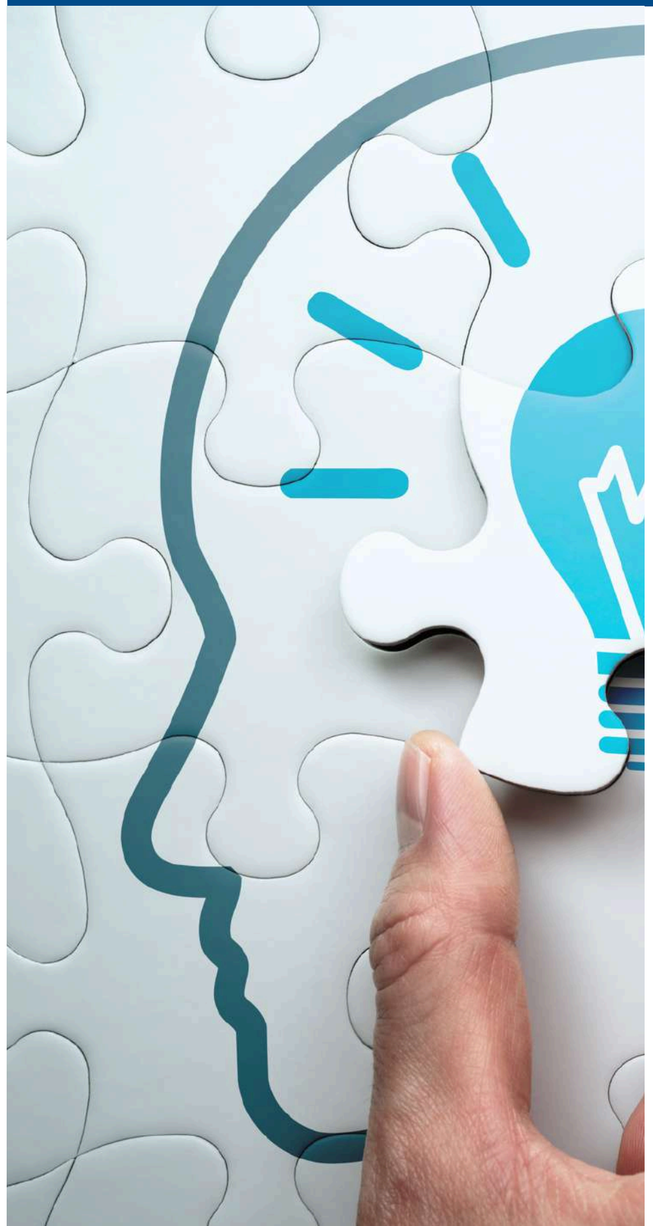
IHK Industrie- und Handelskammern in Bayern

SEST digital

Chancen durch GPAI für Unternehmen

Beispiel Wissensmanagement / FirmenGPT

- Nutzer:innen können mit Unternehmenswissen „chatten“
- Beschleunigtes Onboarding
- verhindern von “Brain-Drain”
- relevante Informationen in Echtzeit bereitstellen



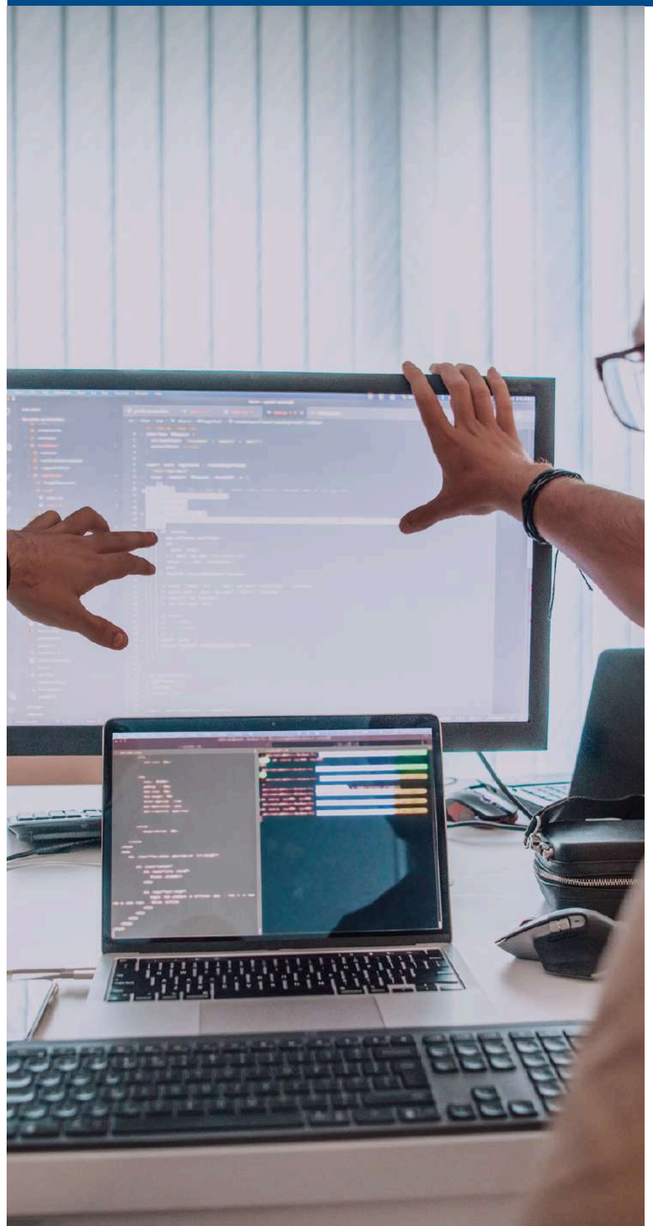
IHK Industrie- und Handelskammern in Bayern

SESTdigital

Chancen durch GPAI für Unternehmen

Beispiel Produktentwicklung

- Einsatz von Bild-Modellen für Design-Ideen und Produktvisualisierungen
- Einsatz von Text-Modellen zur Ideenentwicklung und Konzepterstellung
- GPAI zur Analyse großer Datenmengen, z.B. Marktdaten

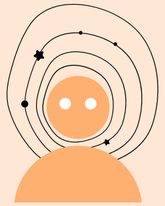


IHK Industrie- und Handelskammern in Bayern

SEST digital

Risiken von GPAI Modellen

Datenschutz

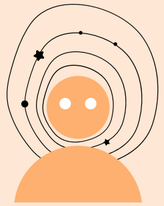


Halluzinationen, Fehler

Bias & Diskriminierung

Risiken von GPAI Modellen

Datenschutz



Halluzinationen, Fehler

Bias & Diskriminierung

Cyber-Security

Transparenz

Anbieter vs. Betreiber

Gemäß Art. 3 Nr. 4 KI-VO ist ein Betreiber:

„Eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein **KI-System in eigener Verantwortung verwendet**, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet“

- Einsatz von KI-Systemen für interne Zwecke
- Keine Weiterentwicklung
- Kein Anbieten des Modells als eigenes Produkt

Als Betreiber tragen Unternehmen Verantwortung dafür, das KI-System regelkonform zu nutzen, ohne die umfassenden Pflichten eines Anbieters zu übernehmen.

Anbieter vs. Betreiber

Gemäß Art. 3 Nr. 3 KI-VO ist ein Anbieter:

„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.“

- Unternehmen aktiv an Entwicklungbeteiligt
- z.B. KI-basierte SaaS Plattform
- Intgration bestehender KI-Modelle in eigene Produktion
- noch Klärungsbedarf
- Gefahr des schleichenden Übergangs von Betreiber zu Anbieter z.B. durch Fine-Tuning, RAG

=> Jede Anpassung eines KI-Systems muss sorgfältig geprüft werden

Anbieter vs. Betreiber

AI-Act richtet sich bzgl. GPAI an “Anbieter” von GPAI

- Der Schwerpunkt auf Unternehmen, die GPAI entwickeln oder „integrieren“ und sie auf dem europäischen Markt anbieten.

- Risiko, als Anbieter zu gelten, wenn bereits bestehende Modelle wie GPT-4 durch Änderung oder Anpassung der Datenquellen modifiziert werden

IHK Industrie- und Handelskammern in Bayern

SESTdigital

Risikoklassifizierung von GPAI nach EU AI-Act

abgestufte Risikoklassifizierung für GPAI-Modelle

Normale GPAI Modelle

Offen und frei lizenzierte GPAI-Modelle

GPAI-Modelle mit Systemischen Risiken

IHK Industrie- und Handelskammern in Bayern

SESTdigital

Risikoklassifizierung von GPAI nach EU AI-Act

abgestufte Risikoklassifizierung für GPAI-Modelle

Normale GPAI Modelle

- detaillierte technische Dokumentation des Modells
- Angaben zu den für das Training verwendeten Daten
- Einhaltung des Urheberrechts

IHK Industrie- und Handelskammern in Bayern

SESTdigital

Risikoklassifizierung von GPAI nach EU AI-Act

abgestufte Risikoklassifizierung für GPAI-Modelle

⚠ ⚠

Offen und frei lizenzierte GPAI-Modelle

- Basis-Verpflichtungen
- keine detaillierten Dokumentationsstandards

IHK Industrie- und Handelskammern in Bayern

SESTdigital

GPAI mit systemischem Risiko

Ein KI-Modell für allgemeine Zwecke wird als **KI-Modell für allgemeine Zwecke mit Systemrisiko** eingestuft, wenn es eine der folgenden Bedingungen erfüllt:

(a) Sie verfügt über **hohe Wirkungskapazitäten**, die auf der Grundlage geeigneter technischer Instrumente und Methoden, einschließlich Indikatoren und Benchmarks, bewertet werden;

(b) auf der Grundlage einer Entscheidung der Kommission von Amts wegen oder aufgrund einer qualifizierten Warnmeldung des wissenschaftlichen Gremiums unter Berücksichtigung der in Anhang XIII genannten Kriterien Fähigkeiten oder Auswirkungen hat, die den unter Buchstabe a genannten gleichwertig sind.

KI-VO Art. 51

GPAI mit systemischem Risiko

- GPAI-Modelle mit einer **„hohen Wirkungsmöglichkeit“**. Wirkungsmöglichkeit ist hoch, wenn die Fähigkeiten des Modells den Fähigkeiten der fortschrittlichsten GPAI-Modelle entsprechen oder diese übertreffen

- Benchmark: systemisches Risiko, wenn „die kumulierte Menge der für sein Training verwendeten Berechnungen, gemessen in Gleitkommaoperationen, mehr als 10^25 beträgt“ (Floating Point Operations per Second (**FLOPs**) - Metrik zur Bewertung der Rechenleistung eines KI-Modells

IHK Industrie- und Handelskammern in Bayern

SESTdigital

Risikoklassifizierung von GPAI nach EU AI-Act

abgestufte Risikoklassifizierung für GPAI-Modelle

GPAI-Modelle mit Systemischen Risiken

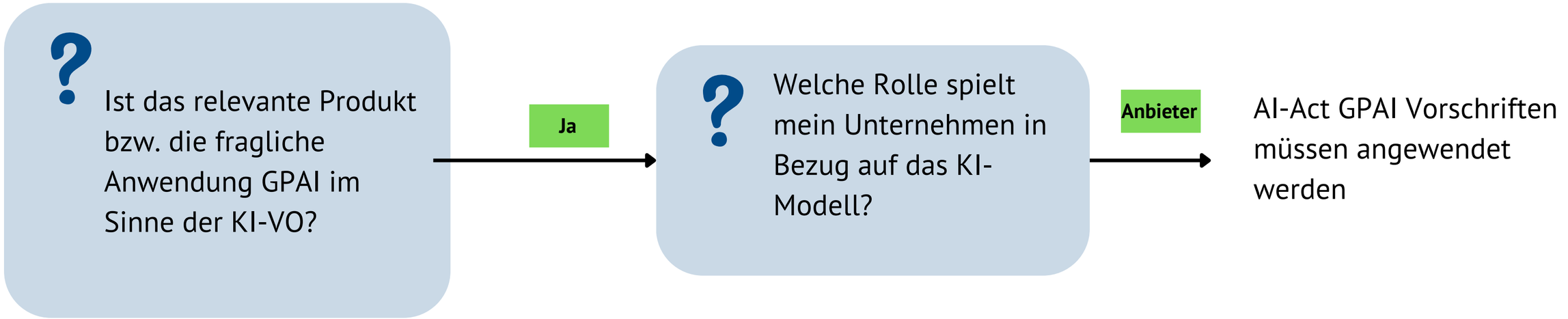
- Basis-Verpflichtungen
- Cybersecurity Anforderungen
- Incident Reporting
- Risk Mitigation (Risikominimierung)
- Performance of Model Evaluations

IHK Industrie- und Handelskammern in Bayern

SESTdigital

Kontrolle & Governance von GPAI Modellen

Folgende Fragen müssen im Unternehmen beantwortet werden:

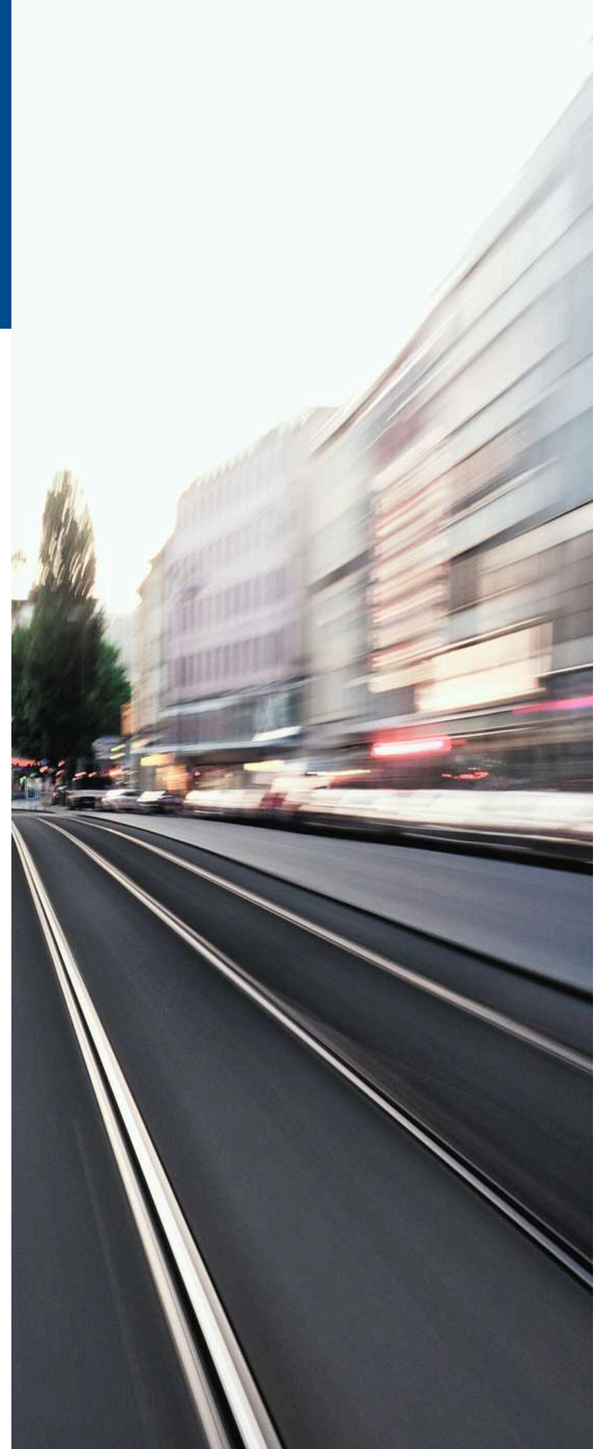


IHK Industrie- und Handelskammern in Bayern

SESTdigital

Was müssen Unternehmen tun?

- Verständnis über eingesetzte KI-Lösungen gewinnen
- AI-Management-System implementieren
- Klare Rollen & Verantwortlichkeiten schaffen
- Weiterbildung & Aufklärung im Unternehmen



Vielen Dank!

Fragen?

Larissa Mikolaschek
Head of Tech
l.mikolaschek@sest.gmbh

E-Mail
hello@sest.gmbh

Web
sest.gmbh

Location
Sest GmbH
Markplatz 7
82031 Grünwald