Juristische Grenzen und Möglichkeiten von künstlicher Intelligenz

Inhaltsverzeichnis

Was ist künstliche Intelligenz?

Was ist Künstliche Intelligenz (KI)?

- KI ist ein Zweig der Informatik, der darauf abzielt, Maschinen zu schaffen, die Aufgaben ausführen können, die normalerweise menschliches Denken erfordern.
- Beispiele für KI in der Alltagswelt: Sprachassistenten wie Alexa und Siri, Empfehlungsalgorithmen auf Netflix und Amazon, autonome Fahrzeuge usw.

Was ist maschinelles Lernen?

- Definition: "Maschinelles Lernen ist ein Ansatz zur Realisierung von KI und beinhaltet den Prozess, bei dem Maschinen auf der Grundlage von Daten und Algorithmen lernen und sich verbessern, ohne explizit programmiert zu werden."
- Beispiele für maschinelles Lernen in der Alltagswelt: Spam-Erkennung in E-Mails, Kreditkartentransaktionsüberwachung, personalisierte Werbung usw.

Warum sind KI und maschinelles Lernen wichtig?

- Sie ermöglichen Automatisierung und Effizienzsteigerung.
- Sie ermöglichen personalisierte und verbesserte Kundenerlebnisse.
- Sie treiben Innovationen in vielen Branchen voran, einschließlich Versicherungen.

Verbindung zu Sprachmodellen

- Sprachmodelle wie GPT-4 sind Anwendungen von KI und maschinellem Lernen.
- Sie nutzen maschinelles Lernen, um menschenähnlichen Text zu generieren und zu verstehen.

Inhaltsverzeichnis

Generative KI – Zwischen Hype und Hysterie

ZEIT ONLINE ifen, Limitationen kennen, Risiken managen

Künstliche Intelligenz

McKinsey-Studie sieht Milliardenpotenzial für ChatGPT & Co.

Künstliche Intelligenz

Eines der mächtigsten Instrumente der Menschheitsgeschichte

Eine Kolumne von Sascha Lobo

Nach nur wenigen Stunden führen Nutzer vor, wie weitreichend die Fähigkeiten der neuen Version von ChatGPT sind: Von in 60 Sekunden erstellten Atari-Games bis zu einer funktionierenden Website aus nur einem Foto.

SPIEGEL Netzwelt

Intelligente Tools in Büro und Atelier

Kollege KI – Jobkiller oder praktischer Helfer?

ChatGPT, Midjourney und Co. werden unsere Arbeitswelt umkrempeln. Doch wohin führt die KI-Revolution? Experten und Arbeitnehmer berichten über Chancen der neuen Tools – und ihre Gefahren.

Handelsblatt

EU beschließt umfangreichstes KI-Gesetz der Welt – das sind die wichtigsten Punkte

Brüssel hat die weltweit erste KI-Regulierung beschlossen. Worauf Industrie und Verbraucher sich jetzt einstellen müssen.

manager magazin

Warum 2024 bei KI in Deutschland zum „Jahr der Entscheidung" wird

ChatGPT, Gemini und diverse Copiloten – die Unternehmen experimentieren mit KI. Die neue Technologie entscheidet über persönliche Karrieren und die Wettbewerbsfähigkeit der Konzerne. Eine alarmierende Analyse zum Stand der KI in der deutschen Wirtschaft.

automotiveIT

Einsatz von KI-Chatbots

Warum Unternehmen vor ChatGPT zurückschrecken

Die meisten KI-Experten bewerten ChatGPT als großen Sprung, rechtlich ist die Technologie von OpenAI jedoch eine Grauzone, die Hürden für die Nutzung durch Unternehmen sind hoch. Das könnte sich durch europäische Versionen ändern.

Deutschlandfunk

Wie weit noch bis zur Superintelligenz?

Selbst Fachleute sind erstaunt über Fähigkeiten von KI, die in großen Sprachmodellen entstehen, ohne dass sie hineinprogrammiert wurden. Was passiert da gerade? Sind wir auf dem Weg in die maschinelle Superintelligenz – und muss uns das beunruhigen?

Hype OpenAI und ChatGPT

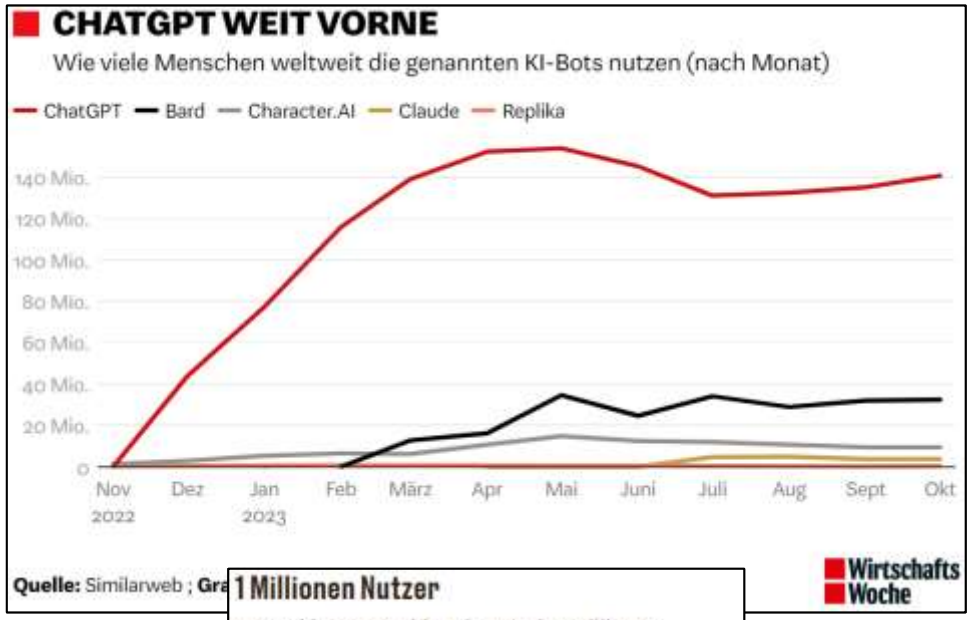
offizielles Logo / Produkt der Firma

OpenAI

gestartet November 2022

die Basisversion ist kostenfrei verfügbar

einfache Nutzung eines komplexen Modells

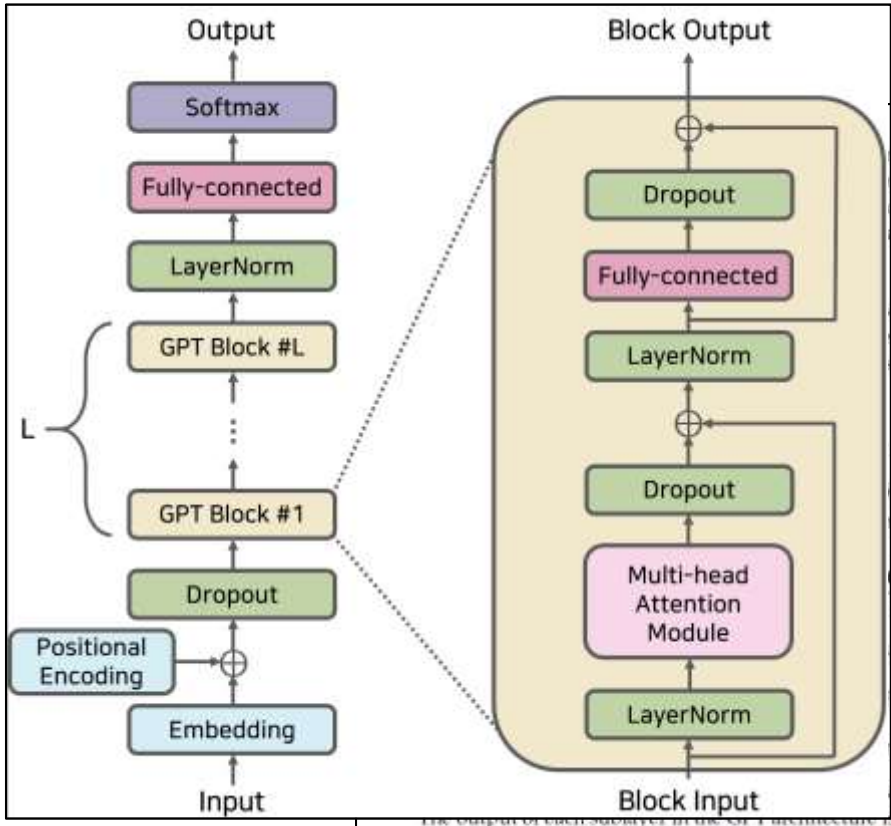


Ein Sprachmodell … kein Wissensmodell

Vorstellung

^- Deep Thought aus dem Film „Per Anhalter durch die Galaxis“

Realität



er model, is composed of L identical
mechanism and a position-wise feed-
the decoder part of the transformer,
d layer normalization are integrated

ented by $\mathbf{H}^{(l-1)}$ and $\mathbf{H}^{(l)}$, respec-
re n denotes the sequence length
elf-attention mechanism [26] can

$$\ldots, \text{Head}_K)\mathbf{W}^O, \quad (6)$$

$\mathbf{W}_k^V$), K is the number of attention
atrices. The attention mechanism

$$\left(\frac{\mathbf{Q}\mathbf{K}^\top}{\sqrt{d_k}}\right)\mathbf{V}, \quad (7)$$

e matrices, respectively, and d_k is

a two-layer neural network with

$$_2 + \mathbf{b}_2, \quad (8)$$

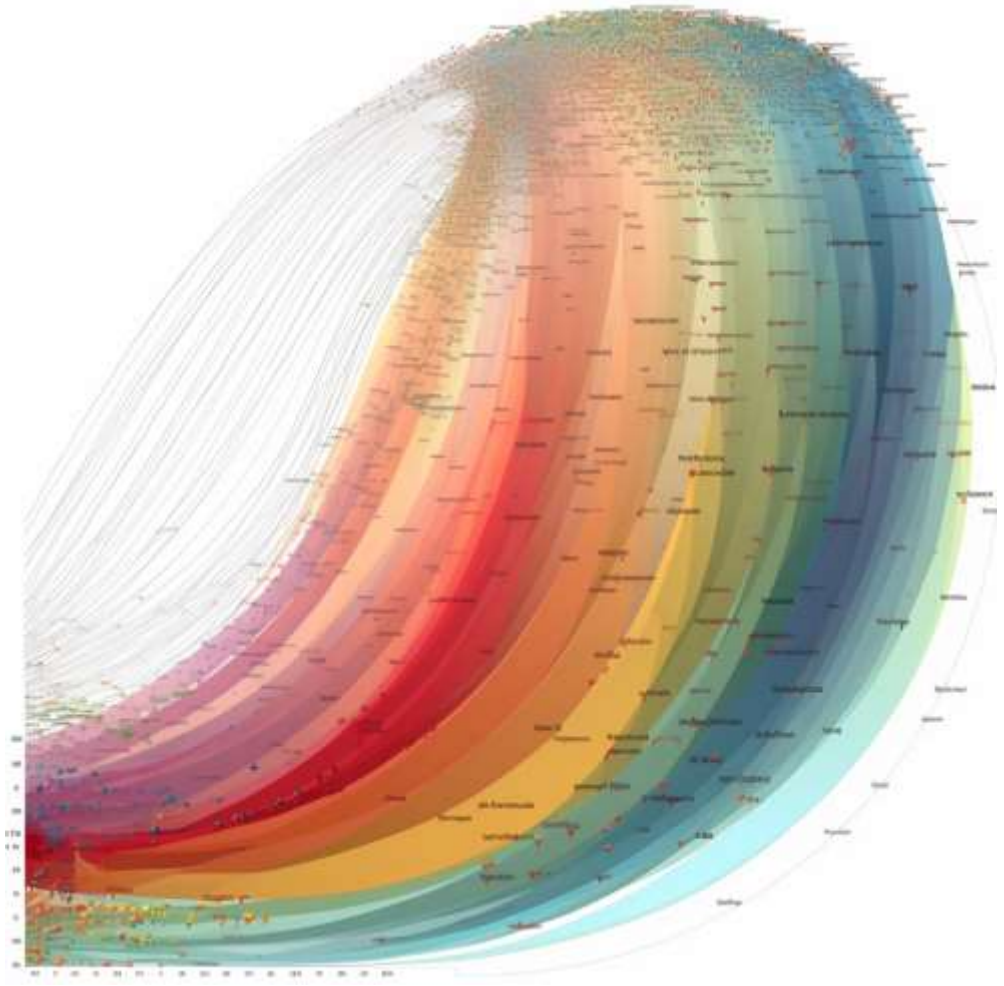
and bias vectors.

combined with its input through
residual connections and is subsequently normalized [33]:

$$\mathbf{H}^{(l)} = \text{LayerNorm}\left(\mathbf{H}^{(l-1)} + \text{SubLayer}(\mathbf{H}^{(l-1)})\right), \quad (9)$$

Was sind Sprachmodelle

- Ein Sprachmodell ist eine KI, die die menschliche Sprache auf der Basis von Textdaten erlernt.
- Es weist Wahrscheinlichkeiten zu, um das nächste Wort in einer Textsequenz vorherzusagen.
- Sprachmodelle werden in Anwendungen wie Textvervollständigung, Übersetzung und Spracherkennung verwendet.



Entwicklung von Sprachmodellen

- Anfänge der Sprachmodelle
  Die Entwicklung der Sprachmodelle begann mit regelbasierten Systemen, die auf handgeschriebenen Regeln basierten.
- Später kamen statistische Sprachmodelle, die auf der Berechnung von Wortwahrscheinlichkeiten basierten.
- Diese Modelle hatten jedoch viele Einschränkungen, insbesondere bei der Handhabung von Kontext und komplexer Sprache.

- Aufkommen von Deep Learning
  Mit dem Aufkommen von Deep Learning begannen Forscher, neuronale Netzwerke für Sprachmodelle zu verwenden.
- Diese Modelle waren in der Lage, komplexere Muster und Kontext in der Sprache zu erkennen.

- Beispiele sind RNNs (Recurrent Neural Networks) und LSTM (Long Short-Term Memory) Modelle.

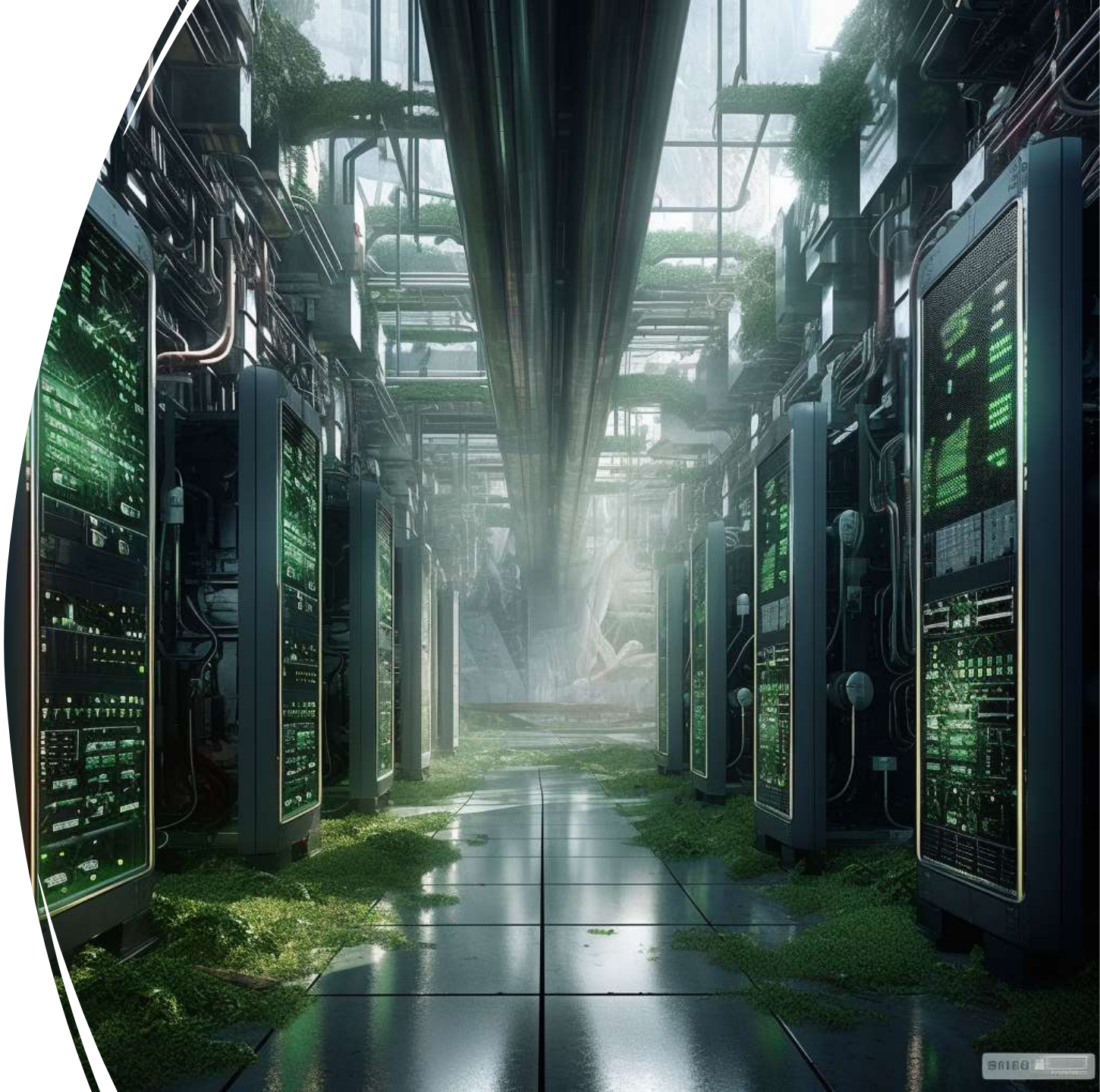
Entwicklung von Sprachmodellen

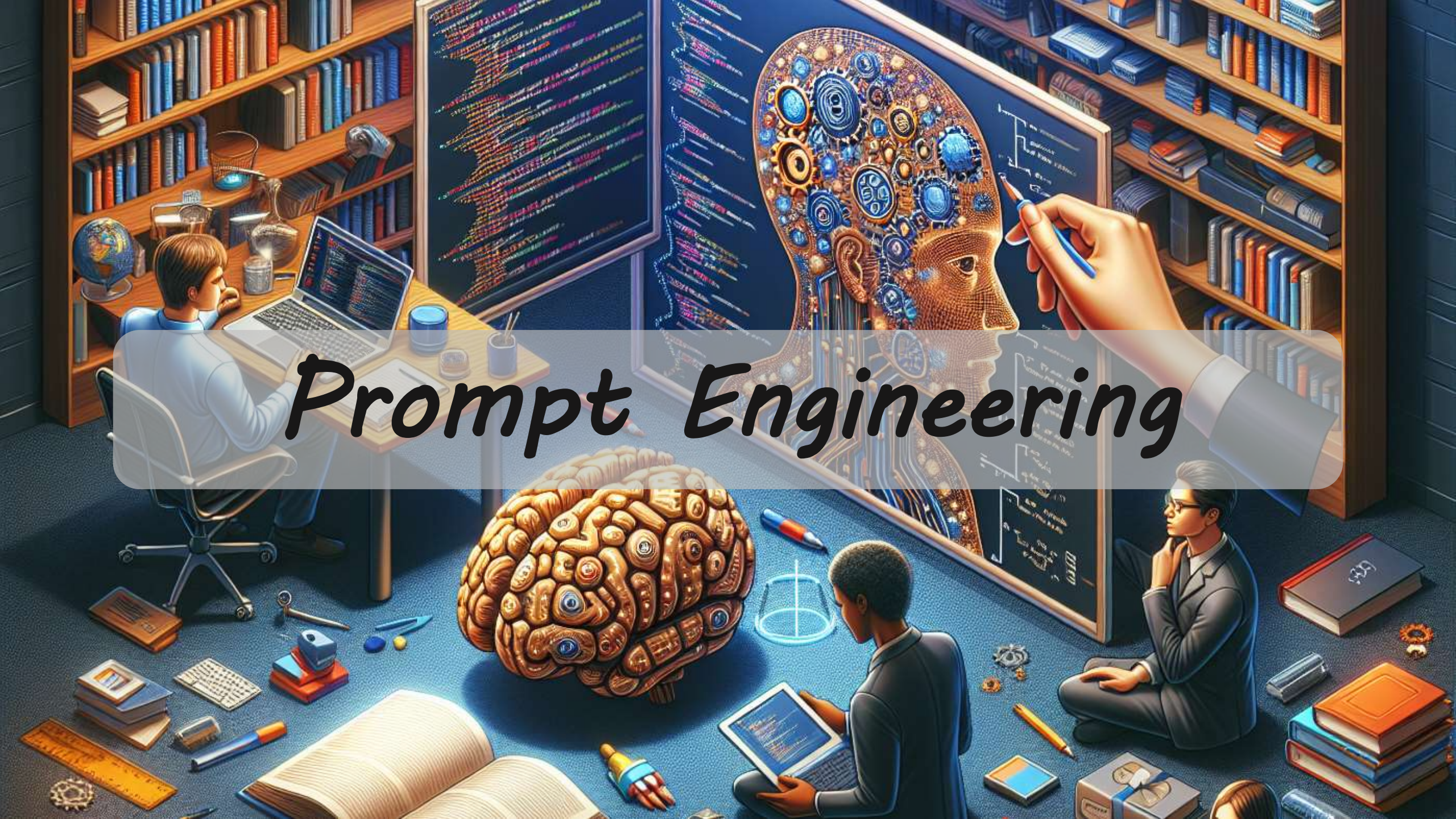
- Transformer und Attention Mechanism
  Das Transformer-Modell, das erstmals 2017 vorgestellt wurde, brachte einen Durchbruch in der Sprachmodellierung.
- Es führte den Attention-Mechanismus ein, der es Modellen ermöglicht, auf relevante Teile des Inputs zu 'achten‘.
- Das Transformer-Modell wurde zur Grundlage für viele fortschrittliche Sprachmodelle wie BERT und GPT.

- Aktuelle Entwicklungen
  Heutige Sprachmodelle, wie GPT-4, sind extrem leistungsstark und können menschenähnlichen Text erzeugen.
- Sie werden in einer Vielzahl von Anwendungen eingesetzt, von Chatbots bis hin zu Textvervollständigung.
- Trotz ihrer Leistungsfähigkeit gibt es immer noch Herausforderungen, wie z.B. die Kontrolle über generierte Outputs und ethische Bedenken."

Zukunft der Sprachmodelle

- Die Zukunft der Sprachmodelle könnten kleinere, effizientere Modelle sein, die weniger Rechenleistung benötigen.
- Außerdem könnten wir Modelle sehen, die besser in der Lage sind, mit Menschen zu interagieren und auf ihre Bedürfnisse einzugehen.
- Es besteht auch ein starker Bedarf an Modellen, die ethisch wertvolle und verantwortungsvollere Entscheidungen treffen können.




Prompt Engineering

Prompts bauen
Best Practices bei der Strukturierung

Klarheit

Ein guter Prompt sollte eindeutig und nicht missverständlich formuliert sein.

Spezifität

Ein guter Prompt sollte so spezifisch wie möglich sein. Grenze die Frage bestmöglich ein.

Kontext

Ein guter Prompt sollte den Kontext der Anfrage berücksichtigen. Gebe entsprechend Hintergrundinformationen.

Anleiten

Es kann hilfreich sein, das gewünschte Format der Antwort im Prompt anzugeben. Beispiel: "Liste drei Gründe auf, warum..."

Erprobung und Anpassung

Experimentiere und passe Prompts an, um zu sehen, welche die besten Ergebnisse liefern.

Ein Beispiel eines guten Prompts

Klarheit

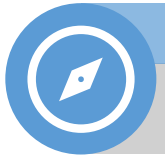
Eindeutig formulieren.

Spezifität

Thema eingrenzen.

Kontext

Hintergrundinfos ergänzen.



Anleiten

Format vorgeben.

Erprobung und Anpassung

Trial and Error.

Initialer Prompt:

Schreib mir einen Aufsatz über KI oder Roboter.

Besserer Prompt:

Du bist Teil der Abteilungsleitung in einer Versicherung. Schreibe mir einen informativen Aufsatz mit einer Länge von einer Seite über den möglichen **Einsatz von KI** in Versicherungen. Zielgruppe sind nicht-informatische Sachbearbeiter in einer Versicherung.

Folgefrage:

Vertiefe mir bitte den Punkt über die Risiken.

Risiken von Sprachmodellen

Fehlinformation und Desinformation: Generierung von ungenauen oder irreführenden Informationen; Potenzielle Nutzung für Desinformation und Propaganda.

Unbeabsichtigte Bias: Fortsetzung von bestehenden Vorurteilen durch Trainingsdaten; Risiko von diskriminierenden oder parteiischen Ergebnissen.

Datenschutz und Privatsphäre: Bedenken hinsichtlich des Datenschutzes, insbesondere wenn Modelle auf sensiblen Daten trainiert werden; Notwendigkeit, die Privatsphäre der Benutzer zu schützen.

Missbrauch: Gefahr des Missbrauchs leistungsstarker Sprachmodelle für schädliche Zwecke; Notwendigkeit von Kontrollmechanismen zur Verhinderung von Missbrauch.

Abhängigkeit von KI: Zunehmende Integration von KI in unseren Alltag führt zu wachsender Abhängigkeit; Wichtigkeit des Verständnisses der Grenzen der KI.

Inhaltsverzeichnis

Aktueller Stand zum EU AI Act

EUROPÄISCHE
KOMMISSION

Brüssel, den 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

ZUR FESTLEGUNG HARMONISIERTER VORSCHRIFTEN FÜR KÜNSTLICHE INTELLIGENZ (GESETZ ÜBER KÜNSTLICHE INTELLIGENZ) UND ZUR ÄNDERUNG BESTIMMTER RECHTSAKTE DER UNION

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

Inhalt des EU AI Acts nach dem Vorschlag der EU Kommission

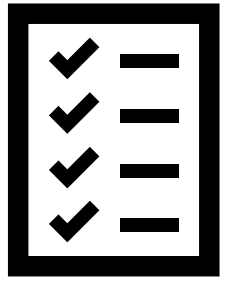
Was sind die Ziele der Kommission?

Es muss gewährleistet sein, dass die auf dem Unionsmarkt in Verkehr gebrachten und verwendeten KI-Systeme sicher sind und die bestehenden Grundrechte und die Werte der Union wahren.

Zur Förderung von Investitionen in KI und innovativen KI muss Rechtssicherheit gewährleistet sein.

Governance und die wirksame Durchsetzung des geltenden Rechts zur Wahrung der Grundrechte sowie die Sicherheitsanforderungen an KI-Systeme müssen gestärkt werden.

Die Entwicklung eines Binnenmarkts für rechtskonforme, sichere und vertrauenswürdige KI-Anwendungen muss erleichtert werden und es gilt, eine Marktfragmentierung zu verhindern.



Welche Grundrechte sieht die EU als gefährdet?

- Durch ihre besonderen Merkmale (z. B. Undurchsichtigkeit, Komplexität, Datenabhängigkeit, autonomes Verhalten) kann die Verwendung von KI dazu führen, dass einige, der in der EU Grundrechtecharta (im Folgenden die „Charta“) verankerten, Grundrechte verletzt werden. Der Vorschlag zielt darauf ab, diese Grundrechte in hohem Maße zu schützen und durch einen klar festgelegten risikobasierten Ansatz verschiedene Ursachen für Risiken anzugehen.

Welche Grundrechte sieht die EU betroffen?

- die Würde des Menschen (Artikel 1),
  die Achtung des Privatlebens und der Schutz personenbezogener Daten (Artikel 7 und 8),
  die Nichtdiskriminierung (Artikel 21)
  und die Gleichheit von Frauen und Männern (Artikel 23).
  Recht auf Meinungsfreiheit (Artikel 11)
  und auf Versammlungs- und Vereinigungsfreiheit (Artikel 12)

Für wen gilt der EU AI Act?

Diese Verordnung gilt für:

1.

a) Anbieter, die KI-Systeme in der Union in Verkehr bringen oder in Betrieb nehmen, unabhängig davon, ob diese Anbieter in der Union oder in einem Drittland niedergelassen sind;

b) Nutzer von KI-Systemen, die sich in der Union befinden;

c) Anbieter und Nutzer von KI-Systemen, die in einem Drittland niedergelassen oder ansässig sind, wenn das vom System hervorgebrachte Ergebnis in der Union verwendet wird.

2.

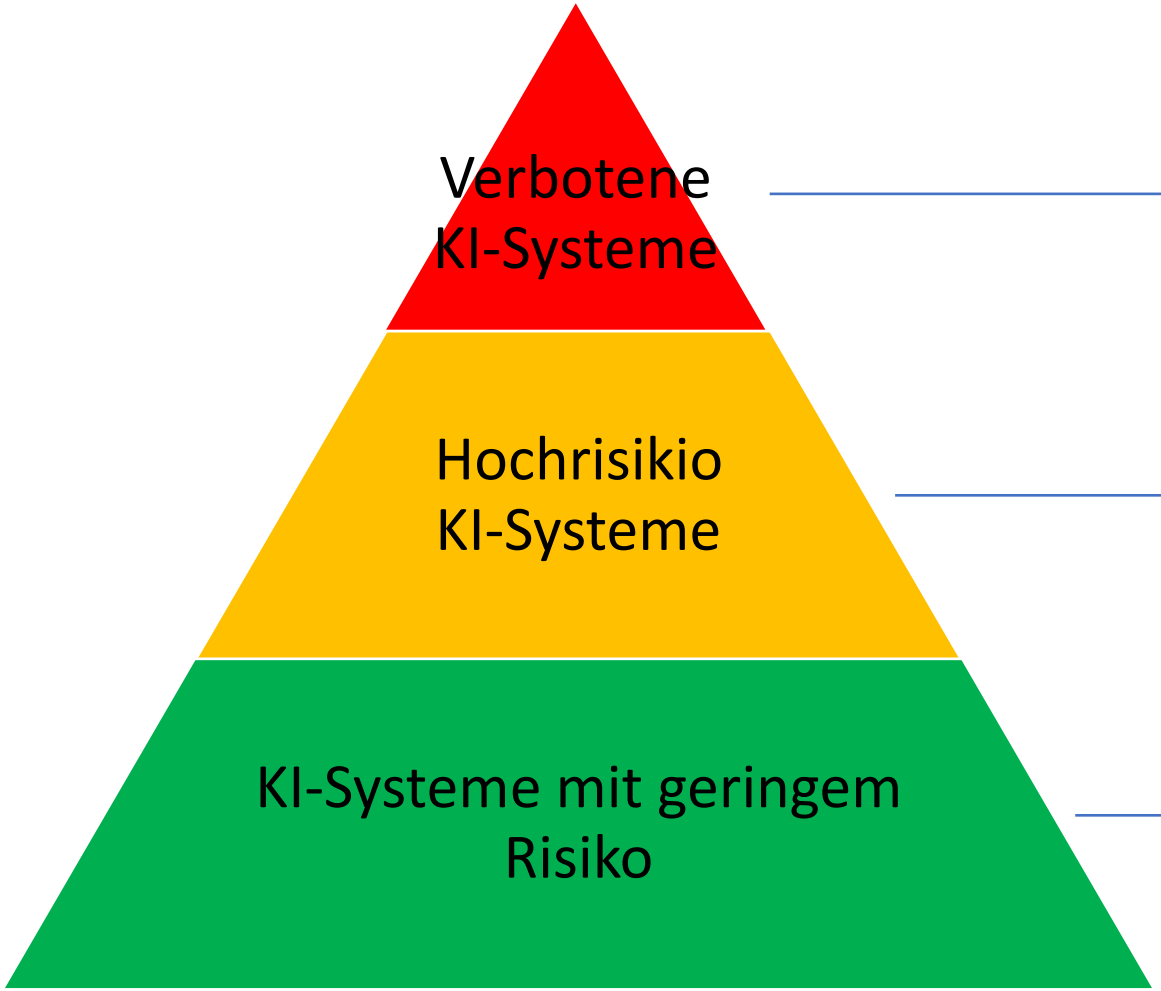
Diese Verordnung gilt nicht für KI-Systeme, die ausschließlich für militärische Zwecke entwickelt oder verwendet werden.

…

Wie ist KI hier definiert?

Ein KI-System ist eine mit Daten und Algorithmen trainierte, also angelernte bzw. auch weiter lernende Software, die in der Lage ist, sich zur Erfüllung ihrer Zwecke und Aufgaben selbst zu optimieren und Probleme zu lösen, indem sie eigenständig Muster erkennt, Schlussfolgerungen zieht und Entscheidungen vorbereitet oder trifft.

Der EU AI Act kennt 3 Risikogruppen



Artikel 5 EU AI Act:
Sammeln biometrischer Daten, Ausnutzung einzelner Gruppen, Emotionsanalyse im Arbeitsbereich usw.

Artikel 6 EU AI Act:
Das System trifft autonome Entscheidungen, ist als Sicherheitsbaustein in Produkten integriert usw.

KI-Systeme mit denen Menschen direkt interagieren können wie z.B.: Chatbots usw.

Verbotene KI-Systeme

Verbotene KI-Systeme sind durch den EU AI Act in ihrer Anwendung ausgeschlossen!

Welche Anforderungen werden an Hoch-Risikosystem gestellt?

Es muss ein Risikomanagementsystem eingerichtet, angewandt, dokumentiert und aufrecht erhalten werden:

Artikel 2 II:
(2) Das Risikomanagementsystem versteht sich als ein kontinuierlicher iterativer Prozess während des gesamten Lebenszyklus eines KI-Systems, der eine regelmäßige systematische Aktualisierung erfordert. Es umfasst folgende Schritte:

a) Ermittlung und Analyse der bekannten und vorhersehbaren Risiken, die von jedem Hochrisiko-KI-System ausgehen;

b) Abschätzung und Bewertung der Risiken, die entstehen können, wenn das Hochrisiko-KI-System entsprechend seiner Zweckbestimmung oder im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird;

c) Bewertung anderer möglicherweise auftretender Risiken auf der Grundlage der Auswertung der Daten aus dem in Artikel 61 genannten System zur Beobachtung nach dem Inverkehrbringen;

d) Ergreifung geeigneter Risikomanagementmaßnahmen gemäß den Bestimmungen der folgenden Absätze.
…

Anforderungen an Hochrisiko-KI-Systeme

Artikel 10: Daten und Daten-Governance
Hochrisiko-KI-Systeme, in denen Techniken eingesetzt werden, bei denen Modelle mit Daten trainiert werden, müssen mit Trainings-, Validierungs- und Testdatensätzen entwickelt werden, die den in den Absätzen 2 bis 5 genannten Qualitätskriterien entsprechen.

Artikel 11: Technische Dokumentation
Die technische Dokumentation eines Hochrisiko-KI-Systems wird erstellt, bevor dieses System in Verkehr gebracht oder in Betrieb genommen wird, und ist stets auf dem neuesten Stand zu halten.

Artikel 12: Aufzeichnungspflicht
Hochrisiko-KI-Systeme werden mit Funktionsmerkmalen konzipiert und entwickelt, die eine automatische Aufzeichnung von Vorgängen und Ereignissen („Protokollierung“) während des Betriebs der Hochrisiko-KI-Systeme ermöglichen. Diese Protokollierung muss anerkannten Normen oder gemeinsamen Spezifikationen entsprechen.

Weitere Anforderungen

Artikel 14: Menschliche Aufsicht
Hochrisiko-KI-Systeme werden so konzipiert und entwickelt, dass sie während der Dauer der Verwendung des KI-Systems – auch mit geeigneten Werkzeugen einer Mensch-Maschine-Schnittstelle – von natürlichen Personen wirksam beaufsichtigt werden können.

Artikel 17: Qualitätsmanagementsystem
Anbieter von Hochrisiko-KI-Systemen richten ein Qualitätsmanagementsystem ein, das die Einhaltung dieser Verordnung gewährleistet. Dieses System wird systematisch und ordnungsgemäß in Form schriftlicher Regeln, Verfahren und Anweisungen dokumentiert und umfasst mindestens folgende Aspekte:…

Artikel 28: Pflichten der Händler, Einführer, Nutzer oder sonstiger Dritter
In den folgenden Fällen gelten Händler, Einführer, Nutzer oder sonstige Dritte als Anbieter für die Zwecke dieser Verordnung und unterliegen den Anbieterpflichten gemäß Artikel 16: a) wenn sie ein Hochrisiko-KI-System unter ihrem Namen oder ihrer Marke in Verkehr bringen oder in Betrieb nehmen.

Überwachung

- Und wie wird die Einhaltung überwacht?

  Artikel 30 Notifizierende Behörden:
  Jeder Mitgliedstaat sorgt für die Benennung oder Schaffung einer notifizierenden Behörde, die für die Einrichtung und Durchführung der erforderlichen Verfahren zur Bewertung, Benennung und Notifizierung von Konformitätsbewertungsstellen und für deren Überwachung zuständig ist.

- Was ist die Folge für einen Verstoß?

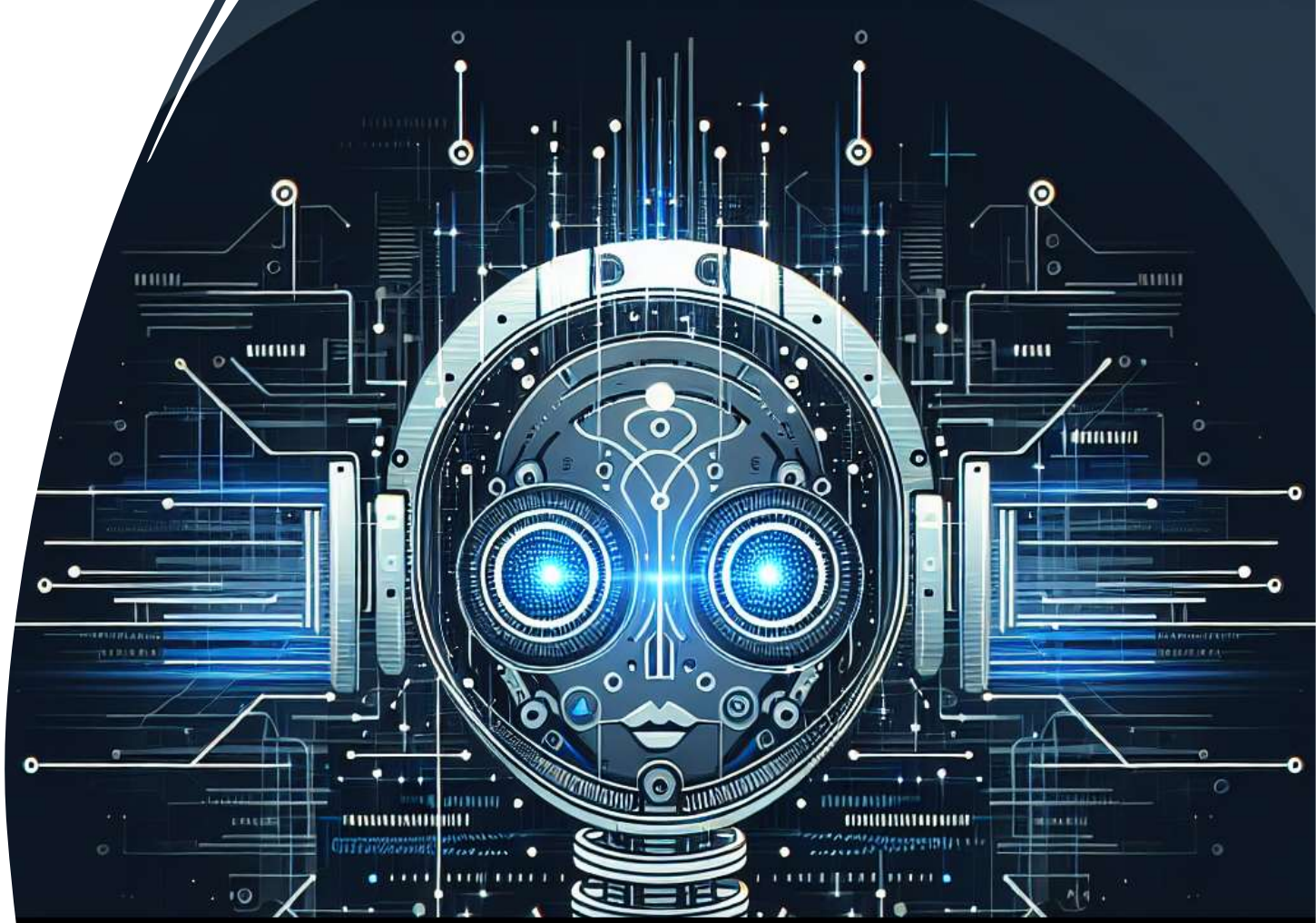
  Artikel 71: Sanktionen
  …
  III. Bei folgenden Verstößen werden Geldbußen von bis zu 30 000 000 EUR oder – im Falle von Unternehmen – von bis zu 6 % des gesamten weltweiten Jahresumsatzes DE 93 DE des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher Betrag höher ist: a) Missachtung des Verbots der in Artikel 5 genannten KI-Praktiken; b) Nichtkonformität des KI-Systems mit den in Artikel 10 festgelegten Anforderungen.

KI-Systeme mit geringem Risiko

- Hier gilt vorwiegend die Transparenzpflicht nach Artikel 52:

  I.
  Die Anbieter stellen sicher, dass KI-Systeme, die für die Interaktion mit natürlichen Personen bestimmt sind, so konzipiert und entwickelt werden, dass natürlichen Personen mitgeteilt wird, dass sie es mit einem KI-System zu tun haben, es sei denn, dies ist aufgrund der Umstände und des Kontexts der Nutzung offensichtlich.

  II….



Wie sieht der Zeitplan aus?

Der AI Act wird voraussichtlich im Mai 2024 verabschiedet.

Ab dann gilt für die Umsetzung eine Karenzzeit von 24 Monaten

Was müssen Unternehmen jetzt tun?

Es sollte eine Arbeitsgruppe gegründet werden, die sich den Fragen des EU AI Acts annimmt.

Es muss eine Gap-Analyse gemacht werden, an welchen Stellen im Unternehmen bereits KI eingesetzt wird.

Es empfiehlt sich die Gründung eines Expertenrates, der entscheidet, in welche der drei Risikogruppen die jeweiligen KI-Systeme liegen.

Insbesondere für Hochrisiko KI-Systeme muss ein Governance System etabliert werden, soweit noch nicht vorhanden.

Inhaltsverzeichnis

4.Wie ist der Inhalt von LLM rechtlich zu bewerten

Grundsätzlich gilt, dass es bisher wenig Rechtsprechung zu den Thematiken von KI und Large Langugage Modellen gibt.

Diese wird sich aber in den nächsten Jahren ändern.

Bisher ist der generierte Inhalt von Large Language Modellen nicht urheberrechtlich geschützt.
Man darf ihn also nutzen**, es hindert aber einen Dritten nicht daran, den Inhalt zu übernehmen.**

Inhaltsverzeichnis

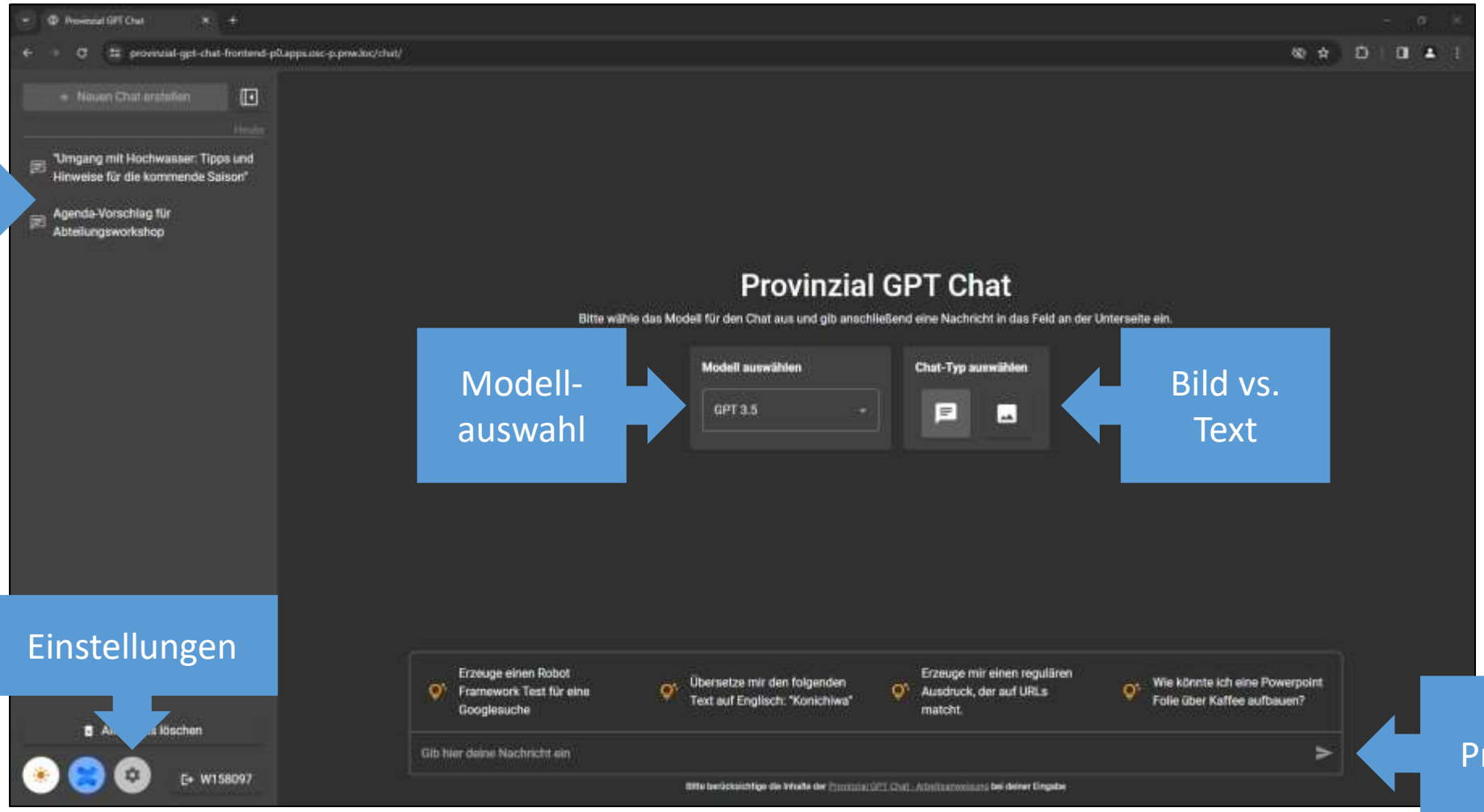
5. Worauf müssen sich Unternehmen einstellen bzw. vorbereiten

Das Thema KI wird in der nächsten Zeit immer mehr Raum einnehmen!

Es sollte bei Einführung von LLM frühzeitig eine Einbindung des Betriebsrates erfolgen. Der Einsatz von LLMs bietet für Unternehmen viele Möglichkeiten.

Unternehmen sollten Leitlinien zum Thema KI erstellen.

Zuletzt noch ein Beispiel aus der Praxis



Themen die in Zukunft relevant werden

- Deepfake
- Sora AI
- Prompt-injektion
- Generierte Betrugsbilder

ENDE