



# Künstliche Intelligenz

## Mehr Vertrauen mit Datenschutz

### **Fokus KMU – KI datenschutzkonform einsetzen**

**Michael Will**

Präsident

Bayerisches Landesamt für Datenschutzaufsicht

# Wer steht heute vor Ihnen?



## Michael Will

Präsident beim Bayerischen Landesamt für Datenschutzaufsicht (BayLDA)

### Was ist das BayLDA?

- Datenschutzaufsichtsbehörde für alle nicht-öffentlichen Stellen in Bayern
- Dienstsitz ist Ansbach
- 34 Mitarbeiterinnen und Mitarbeiter
- Zuständig für ca. 700 TSD Verantwortliche in Bayern, davon
  - ca. 600.000 kleine und mittlere Unternehmen (KMU)
  - ca. 4.000 Start-Ups
  - ca. 13.000 (Sport-)Vereine
  - ca. 60.000 niedergelassene Ärztinnen und Ärzte



## Zeitenwende – KI: Der Zugang zu mächtigen KI Modellen ist nur einen Klick entfernt



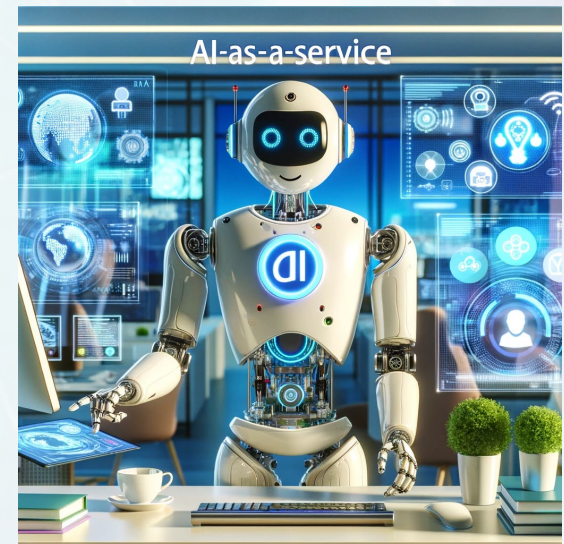
Bislang war für die Nutzung von KI erforderlich:

- Viele (personenbezogene) Daten
- Knowhow im Bereich Data Science
- Viel Geld für Investitionen in Rechenleistung



Mit Aufkommen von ChatGPT & Co. braucht es:

- Innovative Geschäftsideen
- Zugang zu KI-as-a-Service
- Moderne Regulierungsbehörden





# KI-as-a-Service am Beispiel Chat-GPT

ChatGPT 4 -

- You  
Wie kann Digitalisierung und KI bei kleineren und mittleren Unternehmen gelingen?
- ChatGPT  
Die Digitalisierung und der Einsatz von Künstlicher Intelligenz (KI) in kleineren und mittleren Unternehmen (KMU) bieten zahlreiche Möglichkeiten zur Effizienzsteigerung, Kostenreduzierung und zur Entwicklung neuer Geschäftsmodelle. Hier sind einige Strategien und Tipps, wie dies erfolgreich umgesetzt werden kann:

- Klar definierte Ziele und Strategie:** KMU sollten zunächst ihre spezifischen Bedürfnisse und Ziele in Bezug auf Digitalisierung und KI identifizieren. Das kann die Automatisierung bestimmter Prozesse, die Verbesserung der Kundeninteraktionen oder die Entwicklung neuer, datengetriebener Dienstleistungen umfassen.
- Schulung und Kompetenzaufbau:** Eines der größten Hindernisse für die erfolgreiche Implementierung von KI in KMU ist oft ein Mangel an Know-how. Investitionen in Schulungen und Weiterbildung für Mitarbeiter sind daher entscheidend.
- Partnerschaften und Netzwerke:** KMU haben oft nicht die Ressourcen, um große KI-Teams zu beschäftigen. Daher kann die Zusammenarbeit mit Universitäten, Forschungseinrichtungen oder spezialisierten IT-Dienstleistern sinnvoll sein.

Weboberfläche



▼ Making an API request

After you have Python configured and an API key setup, the final step is to send a request to the OpenAI API using the Python library. To do this, create a file named `openai-test.py` using the terminal or an IDE.

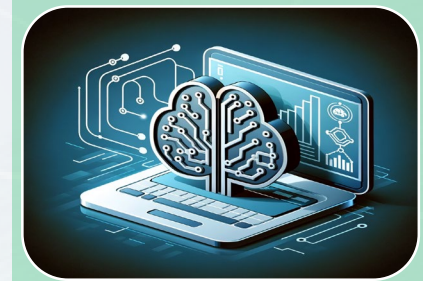
Inside the file, copy and paste one of the examples below:

```

1 from openai import OpenAI
2 client = OpenAI()
3
4 completion = client.chat.completions.create(
5     model="gpt-3.5-turbo",
6     messages=[
7         {"role": "system", "content": "You are a poetic assistant, skilled in explaining"},
8         {"role": "user", "content": "Compose a poem that explains the concept of recursion"}
9     ]
10 )
11
12 print(completion.choices[0].message)

```

Software-Schnittstelle



Datenauswertung



Chat-Bots



Übersetzungen



Texte verstehen



Workflows optimieren



Kreative  
Datenverknüpfungen



Programmierhilfen

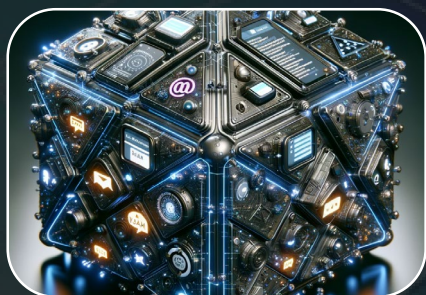


Grafik- und  
Videoerzeugung

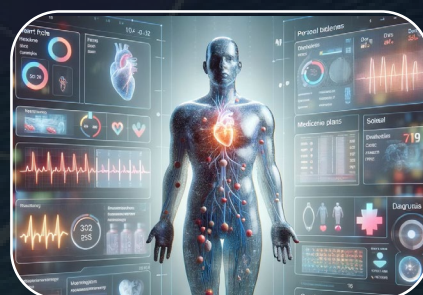
KI-as-a-Service



# KI hat enorm viel Potential – aber auch dunkle Seiten



Spam-Bots &  
Fake-News



Gläserne Bürger



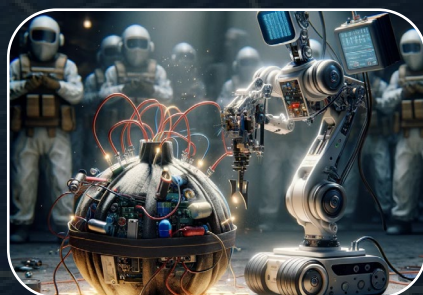
Deep Fakes



Unfälle durch KI



Verseuchung  
des Internets



Anleitungen zum  
Bombenbau



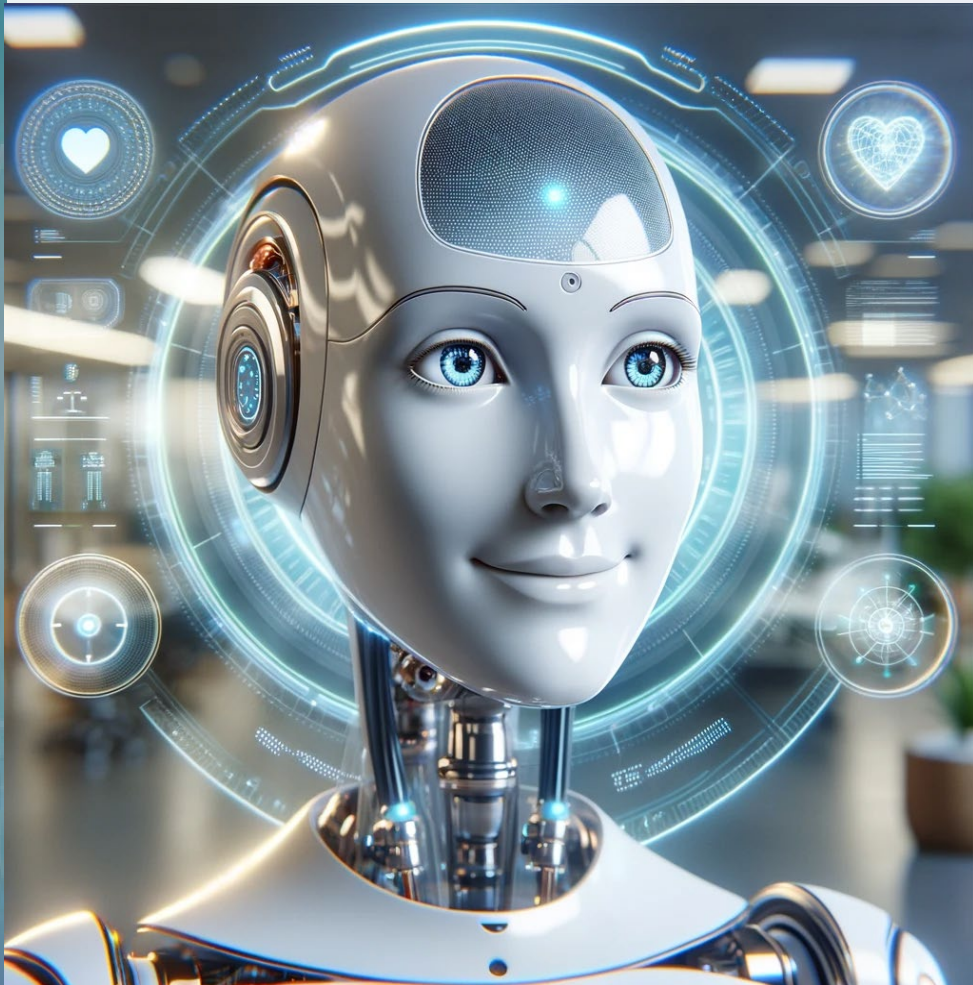
Diskriminierungen



Manipulation  
von Kindern



# KI und Datenschutz – Was ist das Ziel



- Die DSGVO regelt die Verarbeitung personenbezogener Daten
- Die DSGVO ist eine gestaltende Verordnung: Es sollen alle redlichen Geschäftsmodelle ermöglicht werden
- Zugleich sind die Grundrechte und Grundfreiheiten der Bürger zu schützen
- Unfaire Geschäftspraktiken und kriminelle Angriffe sollen dagegen verhindert werden
- Künstliche Intelligenz und Datenschutz sind kein Widerspruch – wenn grundlegende Punkte beachtet werden



# KI und Datenschutz: Building Blocks

- **Rechtsgrundlagen**
  - Auch KI-Verarbeitungen brauchen eine Rechtsgrundlage
  - Es bietet sich meist die Interessensabwägung an
  - Bei hochsensitiven Gesundheitsdaten: Sonderregelungen oder einfach die Patienten um eine Einwilligung bitten
- **Umgang mit Hochrisiko-KI**
  - Die Datenschutzfolgenabschätzung ist das Mittel der Wahl
  - Ziel: Datenschutzrisiken in den Griff zu bekommen (z.B. Diskriminierungen)
  - Nützt auch der Vertrauensbildung in die eigenen Produkte
  - Sollten hohe Restrisiken bestehen bleiben: es besteht ein Anspruch (und auch Pflicht) auf Konsultation beim BayLDA



# KI und Datenschutz: Building Blocks

- **Umgang mit „Halluzinationen“**
  - KI hat mit dem Menschen schon eines gemein: sie macht Fehler
  - „Halluzinationen“: Gravierende und strukturelle Fehler werden überzeugend und sprachlich korrekt wiedergegeben
  - Deswegen: Sprunghaftes Fehlerverhalten erwarten und den Umgang damit einplanen
- **Mitarbeiter schulen**
  - KI braucht weiterhin den Menschen in der Wertschöpfungskette
  - Diese sind über den KI-Einsatz zu informieren und über mögliche KI-Risiken zu schulen – damit bei gravierenden KI-Fehlverhalten eingegriffen werden kann
- **Betroffenenrechte und KI**
  - Informieren, Auskunft erteilen, Korrigieren und Löschen – die Betroffenenrechte stellen ein wichtiges Fundament der DS-GVO dar
  - Bei innovativer KI kann dies teils noch herausfordern sein – gut, falls die Aufsichtsbehörde beraten kann





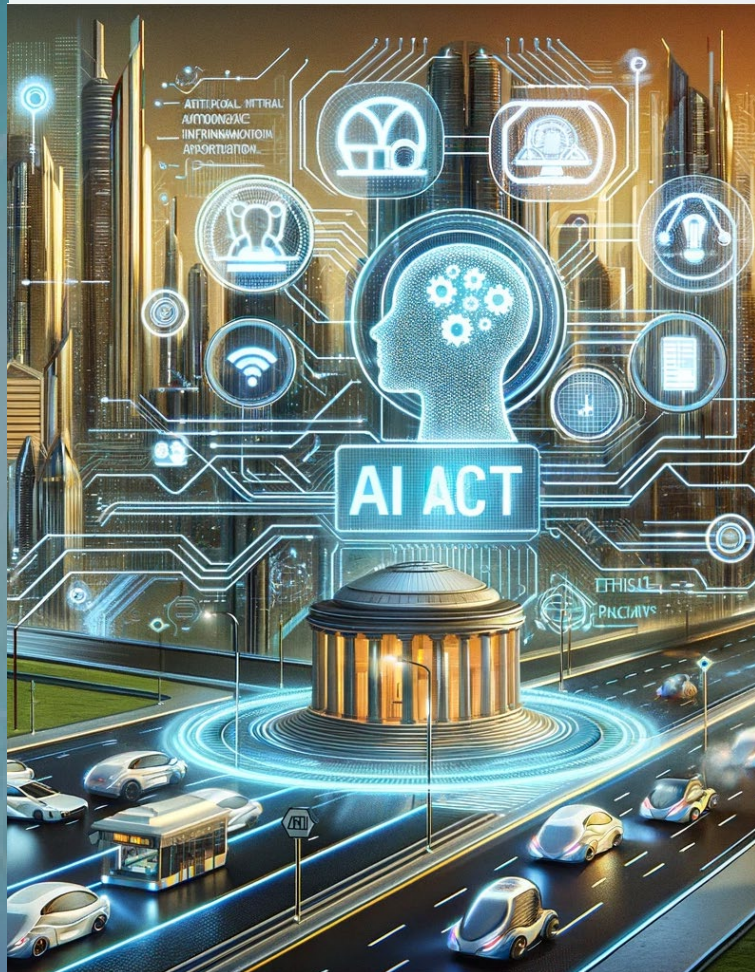
# KI und Datenschutz: Building Blocks

- **KI-as-a-Service**

- Das Training von KI-Modellen braucht sehr viel und hochqualitative Daten, viel Know-How und enorme Rechenleistung
- Auch der Betrieb von (großen) KI-Modellen erfordert höchste Rechenkapazitäten
- KI-Dienstleister bieten diese Services an und können gut datenschutzkonform genutzt werden:
  - Vertrag zur Auftragsverarbeitung mit einem seriösen Dienstleister
  - Garantien zur Drittlandsübermittlung USA sind (wieder) vorhanden: EU-US-Datenschutzframework
  - Hauptfokus bei KI: Zweckbindung der Eingabedaten in KI-Services – werden diese vom KI-Dienstleister auch für das Training von neueren KI-Modellen zu dessen Zwecken verwendet?



# KI-Regulierung: Was bringt die Zukunft



- Es kommt eine neue europäische Regulierung: KI-Verordnung
- Manche KI wird/bleibt verboten
- Hochrisiko-KI wird regulatorisch begleitet
- Normale KI hat wenig/keine Regulierung
- Die DS-GVO bleibt bestehen
- Noch offen: Wird KI in Bayern von einer Landes- oder eine Bundesbehörde begleitet?



# Vielen Dank für Ihre Aufmerksamkeit!

---

Bei mehr Interesse an Datenschutz und KI:

[www.ida.bayern.de/ki](http://www.ida.bayern.de/ki)

oder kommen Sie später zu uns an unseren Stand.