



# KI nutzen, ohne Daten preiszugeben

Dr. Frank Michler (Inhouse-AI)

Web: <https://inhouse-ai.de>

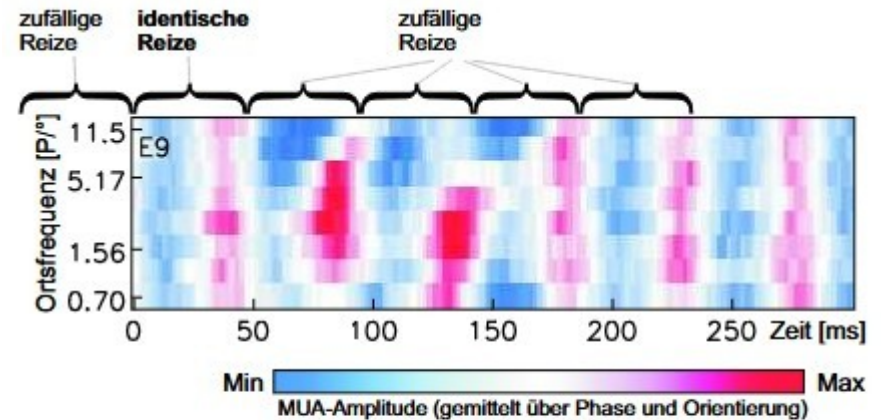
E-Mail: [info@inhouse-ai.de](mailto:info@inhouse-ai.de)

LinkedIn: <https://www.linkedin.com/in/dr-frank-michler-9b554940/>



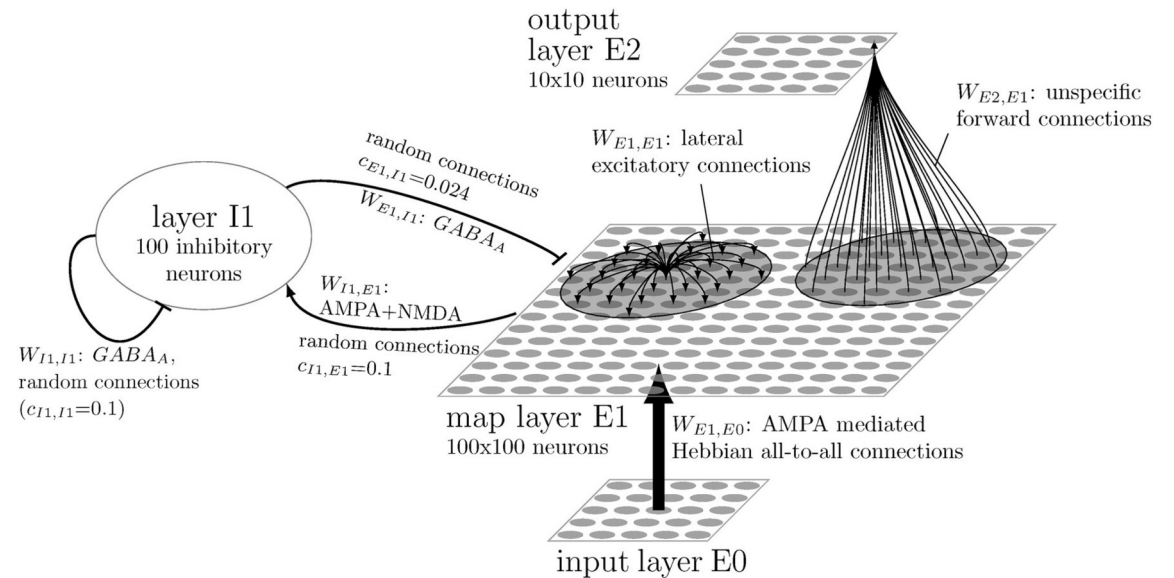
- Anwendungsfälle: Was ist möglich mit KI?
- Risiken von Cloud-KI
- Was können lokale KI-Systeme?
- Grundlagen für lokale KI
- 3 Startpunkte für KI im Unternehmen
- Fragen der Teilnehmer

- Biologie: Schwerpunkt Hirnforschung

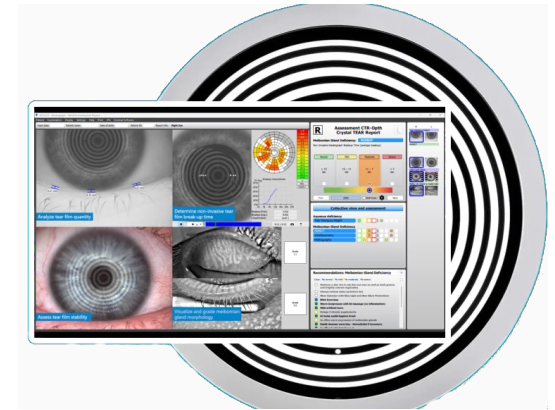


**Abbildung 4.18:** Zeitverlauf bei schneller Reizung (Beispiel vom 27.03.02, Kanal E9). Im Zeitverlauf ist der Rhythmus der Reizsequenz ( $f=21,2$  Hz,  $T=47,2$  ms) erkennbar. Das zweite und dritte Aktivitätsmaximum sind Reiz-spezifisch, während die anderen Maxima für alle Ortsfrequenzen eine ähnliche Amplitude haben.

- Biologie: Schwerpunkt Hirnforschung
- Promotion: Simulation Neuronaler Netze



- Biologie: Schwerpunkt Hirnforschung
- Promotion: Simulation Neuronaler Netze
- Softwareentwicklung seit 2008
  - Messtechnik
  - Medizintechnik
  - Bahntechnik



# Digitale Souveränität

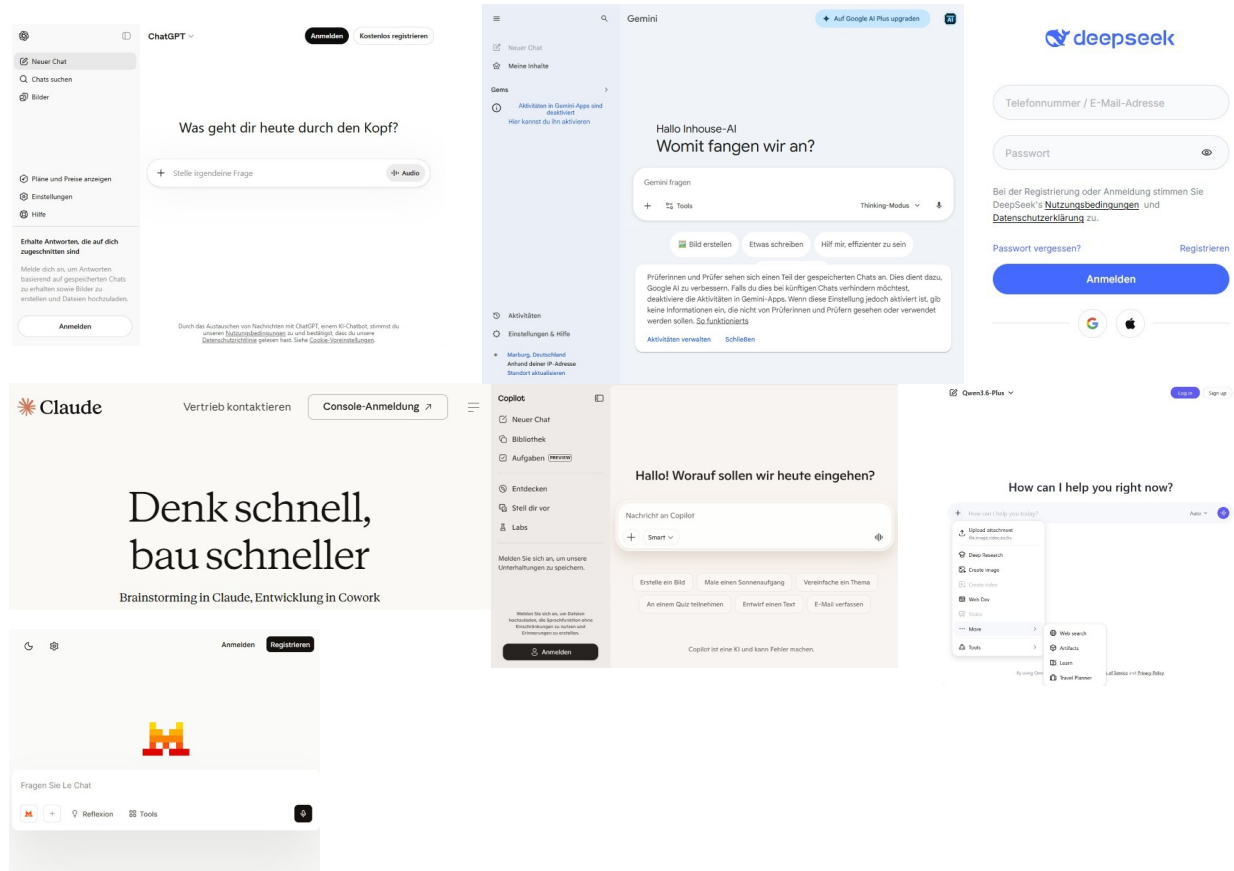
- **Anwendungsfälle: Was ist möglich mit KI?**
- Risiken von Cloud-KI
- Was können lokale KI-Systeme?
- Grundlagen für lokale KI
- 3 Startpunkte für KI im Unternehmen
- Fragen der Teilnehmer

- Buchhaltung:
  - Eingehende Rechnungen (halb- oder voll) automatisch verbuchen
- Dokumenten-Management
  - Eingescannte Dokumente mit Metadaten versehen
    - Datum
    - Titel
    - Autor
    - Zusammenfassung
    - Schlagworte

- Wissens-Management
  - Dokumentationen interner Abläufe erzeugen
  - Zugriff auf Wissen
  - Auffinden relevanter Dokumente
- Angebotserstellung
- Vor-Verarbeitung von Kundenanfragen
  - Wer ist zuständig?  
Service? Vertrieb? Geschäftsführung?

# Anbieter für Cloud-KI


- chatgpt.com
- claude.ai
- copilot.microsoft.com
- gemini.google.com
- chat.qwen.ai
- kimi.com
- chat.deepseek.com
- chat.mistral.ai



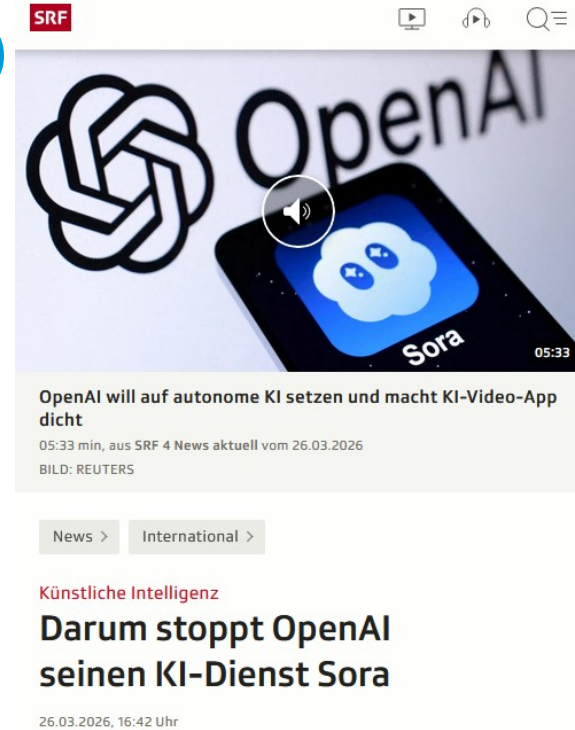
- Anwendungsfälle: Was ist möglich mit KI?
- **Risiken von Cloud-KI**
- Was können lokale KI-Systeme?
- Grundlagen für lokale KI
- 3 Startpunkte für KI im Unternehmen
- Fragen der Teilnehmer

- Kein Einfluss auf Funktionsweise (Systemprompts, Zensur, ...)

## Chat paused

Opus 4.7's safety filter  flagged this chat. Due to its advanced capabilities, Opus 4.7 has additional safety measures that occasionally pause normal, safe chats. We're working to improve this. Continue your chat with Sonnet 4, [send feedback](#), or [learn more](#).

- Kein Einfluss auf Funktionsweise (Systemprompts, Zensur, ...)
- Dienste können abgeschaltet werden (z.B. Sora)



- Kein Einfluss auf Funktionsweise (Systemprompts, Zensur, ...)
- Dienste können abgeschaltet werden (z.B. Sora)
- Daten landen auf fremden Servern
  - Geschäftsgeheimnisse
  - Mitarbeiterdaten
  - Kundendaten
- Datenschutz
  - DSGVO



**vertrauliche  
Firmendaten**

Baidu  
Alibaba

**China**



Google  
Amazon  
Microsoft  
OpenAI

**USA**



- 2013: Edward Snowden übergibt NSA-Dokumente an Journalisten
- „Kunden“ des NSA u.a.:
  - Wirtschaftsministerium
  - Landwirtschaftsministerium
  - Energie-Ministerium

## AUFKLÄRUNGSZIEL DEUTSCHLAND

### KUNDEN UND AUFGABEN DER NSA

Präsentationsfolie aus den Snowden-Unterlagen zu Kunden und internen Interessensgruppen der NSA.



Die Snowden-Unterlagen zeigen es deutlich, die NSA hat eine klare Vorstellung, wer ihre Kunden sind. Ihr Geschäftsmodell ist es, die eigene Tätigkeit so auszurichten, dass genug wichtige Ziele überwacht werden, um den Entscheidern und Informationsabnehmern ständig wertige Informationen und Dienste liefern zu können.

#### BEWERTUNG

Kunden der NSA haben in Teilen ein natives Interesse an ökonomischen Aspekten.

- Chefjustiziar von Microsoft France bei Anhörung in Frankreich:
  - **Microsoft kann Datenschutz nicht zusichern**

## Keine Garantien: Microsoft muss EU-Daten an USA übermitteln

In einer Anhörung musste der Chefjustiziar von Microsoft France zugeben: Es gibt keine Garantie, dass EU-Daten vor einer Übermittlung in die USA sicher sind.



- Chefjustiziar von Microsoft France bei Anhörung in Frankreich:
  - **Microsoft kann Datenschutz nicht zusichern**
- Konsequenzen in Frankreich



RedaktionsNetzwerk Deutschland

RND+ entdecken Newsletter Ticker Politik Krieg in Nahost Russlands Krieg Klima

Startseite > Politik > Warum Frankreich Microsoft den Rücken kehrt: Der Weg zur digitalen Souverän

Digitale Souveränität

**+ Frankreich will sich von US-Tech-Konzernen lösen**

Adieu Microsoft: Frankreich setzt auf Linux.  
Quelle: Donati/RND (Montage); Fotos: lewing@isc.tamu.edu, Freepik, IMAGO/Telmo Pinto

Anhören

Alle Ministerien sind angehalten, europäische Alternativen für digitale Systeme und Werkzeuge zu finden. Auch die Umstellung von Microsoft auf

- Chefjustiziar von Microsoft France bei Anhörung in Frankreich:
  - **Microsoft kann Datenschutz nicht zusichern**
- Konsequenzen in Frankreich
- Schweiz: Abkehr von MS



The screenshot shows a news article from SRF (Schweizer Radio und Fernsehen) dated 19.04.2026 at 10:18 Uhr. The article is titled "Abkehr von Microsoft: Bund will Abhängigkeit reduzieren" and is categorized under "Bedenken wegen Datensicherheit". The article discusses the Swiss government's plan to reduce its dependence on Microsoft products, mentioning an investment of hundreds of millions of francs in Microsoft licenses and the possibility of replacing them with independent open-source software.

**SRF** News > Schweiz >

**Bedenken wegen Datensicherheit**

## Abkehr von Microsoft: Bund will Abhängigkeit reduzieren

19.04.2026, 10:18 Uhr

TEILEN

- Hunderte Millionen Franken hat der Bund in den letzten Jahren in Microsoft-Lizenzen investiert.
- Nun plant er, vom US-Konzern unabhängiger zu werden. Das bestätigt die Bundeskanzlei gegenüber der [«NZZ am Sonntag»](#).
- Eine Machbarkeitsstudie zeige, dass ein Ersatz durch unabhängige Open-Source-Software möglich sei.

Der Bund plant laut der «NZZ am Sonntag» eine allmähliche Abkehr von Microsoft-Produkten. «Die Bundesverwaltung strebt an, ihre Abhängigkeit von Microsoft schrittweise und langfristig zu reduzieren», bestätigte ein Sprecher der Bundeskanzlei der Zeitung.

## Bloomberg

● [Live TV](#) [Markets](#) ▾ [Economics](#) [Industries](#) [Tech](#) [Politics](#) [Businessweek](#) [Opinion](#) [Video](#) [More](#) ▾

Technology  
AI

# Samsung Bans Staff's AI Use After Spotting ChatGPT Data Leak


- Employees accidentally leaked sensitive data via ChatGPT
- Company preparing own internal artificial intelligence tools

By [Mark Gurman](#)

May 2, 2023 at 12:48 AM UTC

*Updated on May 2, 2023 at 5:54 AM UTC*



 Gift this article

- Mai 2023
- Mitarbeiter hatten interne Daten in ChatGPT eingegeben
  - Quellcode
- Samsung erließ Verbot der generativen KI-Tools
- Umstieg auf eigene interne KI-Tools

- Anwendungsfälle: Was ist möglich mit KI?
- Risiken von Cloud-KI
- **Was können lokale KI-Systeme?**
- Grundlagen für lokale KI
- 3 Startpunkte für KI im Unternehmen
- Fragen der Teilnehmer

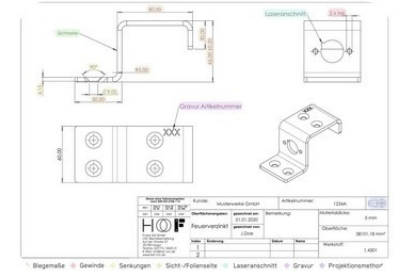
- Papier-Dokumente digitalisieren
  - Metadaten aus gescannten Zeichnungen extrahieren
  - DEMO:  
Cloud (Gemini)  
vs.  
lokal (gemma-4)

Prompt:

Extrahiere folgende Metadaten aus der Zeichnung:

- Datum aus dem Feld "gezeichnet am:"
- Autor aus dem Feld "gezeichnet von:"
- Kunde aus dem Feld "Kunde:"
- Artikelnummer aus dem Feld "Artikelnummer:"

ChatGPT



Extrahiere folgende Metadaten aus der Zeichnung:

- Datum aus dem Feld "gezeichnet am:"
- Autor aus dem Feld "gezeichnet von:"
- Kunde aus dem Feld "Kunde:"
- Artikelnummer aus dem Feld "Artikelnummer:"

Hier sind die extrahierten Metadaten aus der Zeichnung:

- **gezeichnet am:** 01.01.2020
- **gezeichnet von:** J.Doe
- **Kunde:** Musterwerke GmbH
- **Artikelnummer:** 1234A

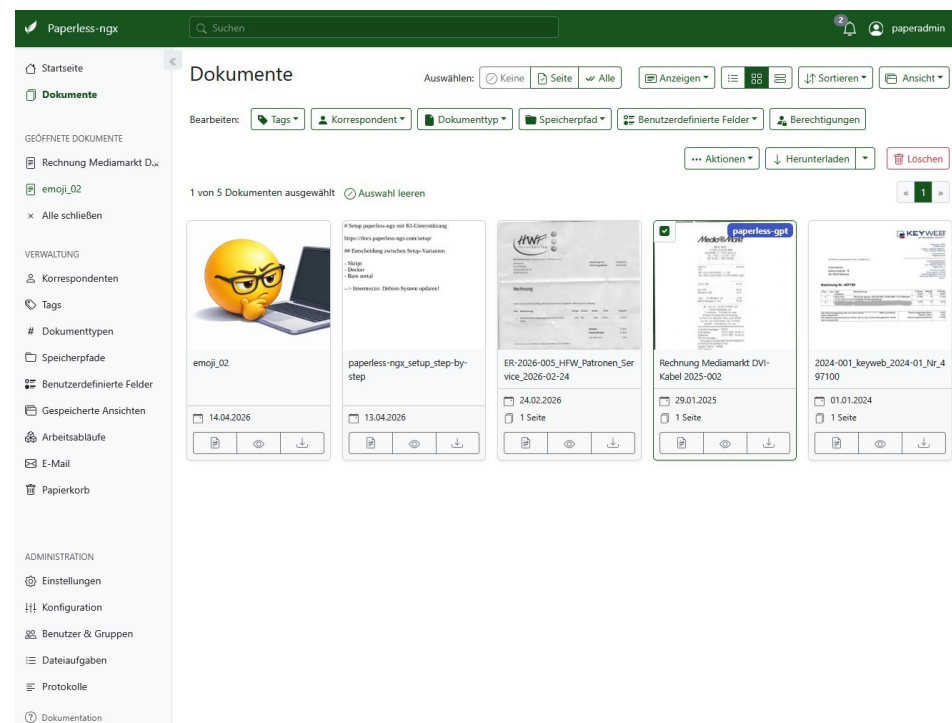
📄 👍 🗑️ ↶ ↷ ⋮

+ Stelle irgendeine Frage



ChatGPT kann Fehler machen. Überprüfe wichtige Informationen. Siehe [Cookie-Voreinstellungen](#).

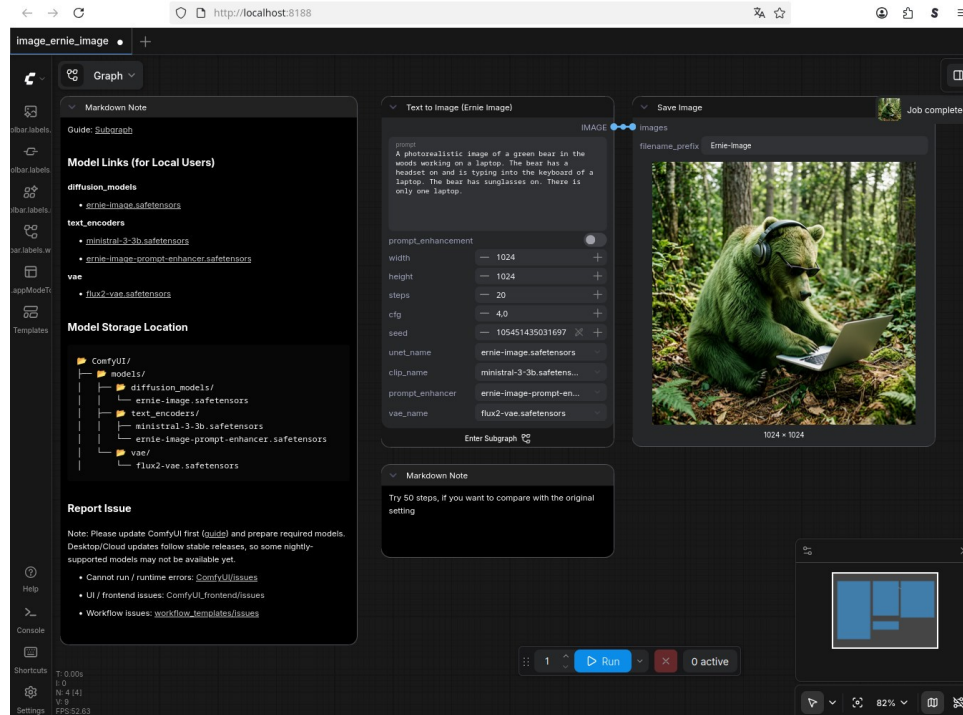
- Wissens- und Dokumenten-Management
  - Recherche in PDFs:  
z.B.: „Welche ähnlichen Aufträge hatten wir letztes Jahr?“
  - Open Source DMS:  
Paperless-ngx + KI-Plugins



- Kundenkommunikation und Support
  - Erstellen von Support-Tickets + Zusammenfassung + Prio
  - E-Mail-Antwortvorschläge

# Alternative: Lokale KI-Systeme

- Marketing-Materialien generieren (Bilder, Audio, Video)



- Anwendungsfälle: Was ist möglich mit KI?
- Risiken von Cloud-KI
- Was können lokale KI-Systeme?
- **Grundlagen für lokale KI**
- 3 Startpunkte für KI im Unternehmen
- Fragen der Teilnehmer

# Was brauche ich für lokale KI?



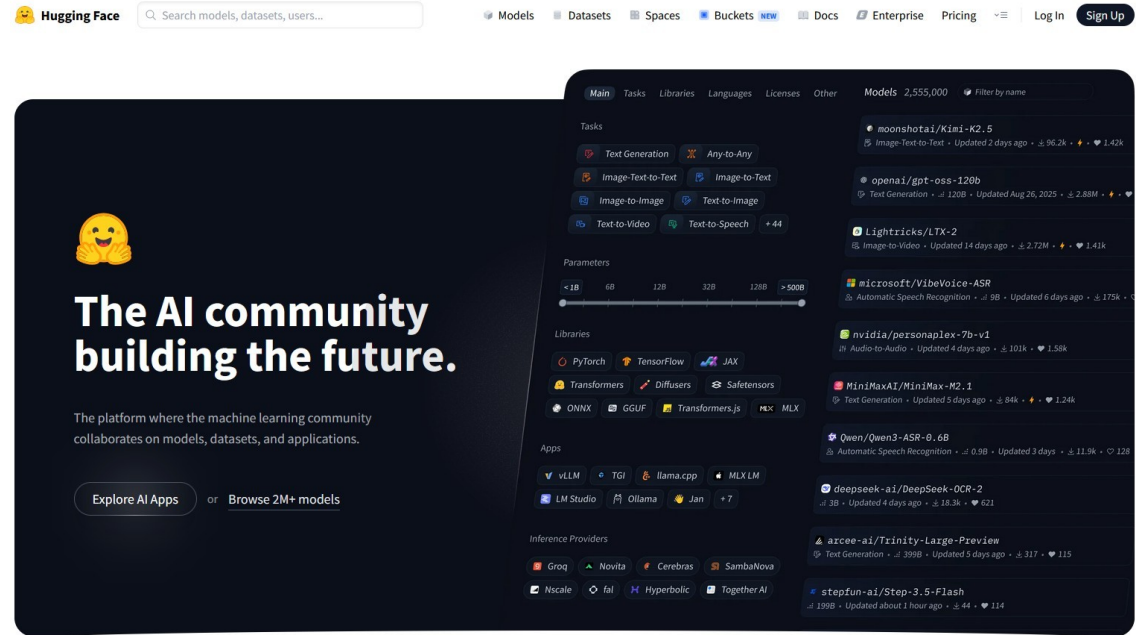
- Modelle
- Hardware
- Software
- Schnittstellen
- Eigene Entwickler oder externe Dienstleister

# „Open Weights“ Modelle



<https://huggingface.co/>

- Meta: Llama-4
- Google: gemma-4
- OpenAI: gpt-oss-20b
- Alibaba: Qwen3.6
- DeepSeek: DeepSeek-R1
- Moonshot AI: Kimi
- Mistral AI: Mistral 7B



- Büro
  - 3.500 bis 7.000 €



- Büro
  - 3.500 bis 7.000 €
- Serverraum
  - 9.000 €  
(Inferenz)
  - bis 50.000 €  
(Modell-Training)



- Büro
  - 3.500 bis 7.000 €
- Serverraum
  - 9.000 €  
(Inferenz)
  - bis 50.000 €  
(Modell-Training)
- Private Cloud
  - 400 bis  
1.000 € / Monat



- Tower-PC mit RTX 5090 (32 GB VRAM)
  - ~ 6.000 – 7.000 € → schneller für mittelgroße quantisierte Modelle
- NVIDIA DGX Spark u.ä. (128 GB unified memory)
  - ~ 3.500 – 5.000 € → Inferenz mit großen Modellen (bis 200B)
- PrimeLine GPU Server mit RTX 4500 Blackwell (32 GB VRAM)
  - Ab 9000 €
- PrimeLine GPU Server mit 4 RTX Pro 6000 Blackwell (384 GB VRAM)
  - Ab 50.000 € → Modell-Training

- 24 GB VRAM: 420 – 500 € / Monat
  - Keyweb „KI-Machine M“
  - IONOS AP2-10 GPU
- 96 GB VRAM: ab 1.000 € / Monat
  - IONOS IP4-50 GPU

- Inferenz-Server (ermöglicht Anfragen an KI-Modell)
  - Llama.cpp
  - Ollama
  - vLLM
- MCP-Server (gibt der KI Zugriff auf interne Systeme)
  - Dateien, Datenbanken, E-Mail, ...
- KI-Bildgenerierung
  - ComfyUI
  - Automatic1111

- Anwendungsfälle: Was ist möglich mit KI?
- Risiken von Cloud-KI
- Was können lokale KI-Systeme?
- Grundlagen für Lokale KI
- **3 Startpunkte für KI im Unternehmen**
- Fragen der Teilnehmer

- KI-Potentiale ermitteln
  - Welche Abläufe lassen sich automatisieren?
  - Welche Automatisierung verspricht den größten Nutzen?
- Pilotprojekt
  - Was kann KI?  
→ Erfahrung und Wissen durch praktische Nutzung
- Mitarbeiter schulen
  - Was kann KI? Was kann sie nicht?
  - Wann ist Cloud-KI ok, und wann nicht?

- Inhouse-AI unterstützt Ihren KI-Einstieg
- Weitere Informationen auf [inhouse-ai.de](https://inhouse-ai.de)

## So starten Sie mit KI in Ihrem Unternehmen:

### KI-Potenzial-Workshop

Entdecken, wo KI in Ihrem Unternehmen wirklich weiterhilft

Viele Teams möchten KI nutzen – aber wissen nicht, welche Anwendungen sinnvoll sind oder wie sie starten sollen.

Im interaktiven KI-Potenzial-Workshop entwickeln wir gemeinsam mit Ihren Stakeholdern erste Ideen, bewerten Chancen und schaffen Klarheit über die nächsten Schritte.

- Beispiele für produktive KI-Anwendungen aus der Praxis
- Gemeinsame Erarbeitung erster Use-Cases in Gruppen
- Einschätzung von Potenzialen, Risiken und Randbedingungen
- Priorisierte Liste konkreter nächster Schritte

Mehr Erfahren

### Ihr eigener Chatbot

Proof-of-Concept für Ihr Unternehmen

In nur zwei Wochen erhalten Sie einen funktionsfähigen internen KI-Chatbot, der Ihre eigenen Dokumente nutzt – komplett ohne Cloud. Ideal, um schnell zu testen, wie KI Ihre Prozesse unterstützen kann.

- Läuft lokal – volle Datenhoheit
- Nutzt Ihre Dokumente, Richtlinien und Fachtexte
- Einfaches Web-Interface für Ihre Mitarbeiter
- Perfekt als schneller Einstieg in KI-Anwendungen

Mehr Erfahren

### Sichere KI-Nutzung

Workshop für Geschäftsführung und Mitarbeiter

Viele Unternehmen möchten KI nutzen, haben aber Angst vor Datenverlust oder Compliance-Verstößen.

In diesem Workshop lernen Ihre Teams, wie sie KI sicher, verantwortungsvoll und datenschutzkonform einsetzen können.

- Klare Regeln: Was darf man eingeben – und was nicht
- Risiken bei ChatGPT und Cloud-KI verständlich erklärt
- Sichere Alternativen für interne Nutzung
- Praxisbeispiele für produktive, aber datenschutzkonforme KI-Anwendungen

Mehr Erfahren

- Feedback unter:  
[inhouse-ai.de/webinar/feedback](https://inhouse-ai.de/webinar/feedback)

## KI-Webinar – Feedback

Vielen Dank für die Teilnahme an unserem Webinar. Ich hoffe, Sie konnten wertvolle Impulse für den Einsatz von KI in Ihrem Unternehmen mitnehmen.

Name \*

E-Mail-Adresse \*

Wie hilfreich fanden Sie das Webinar (Skala 1-5)

- 1 Überhaupt nicht hilfreich
- 2 Wenig hilfreich
- 3 Teils hilfreich
- 4 Hilfreich
- 5 Sehr hilfreich

Wie relevant waren die Inhalte für Ihr Unternehmen?

- 1 Überhaupt nicht relevant
- 2 Wenig relevant
- 3 Teilweise relevant
- 4 Relevant
- 5 Sehr relevant

Welche Themen wünschen Sie sich für zukünftige Webinare?

Möchten Sie eine individuelle Beratung zu Ihren KI-Potenzialen?

- Ja  Nein

Feedback senden

- Anwendungsfälle: Was ist möglich mit KI?
- Risiken von Cloud-KI
- Was können lokale KI-Systeme?
- Grundlagen für Lokale KI
- 3 Startpunkte für KI im Unternehmen
- **Fragen der Teilnehmer**