

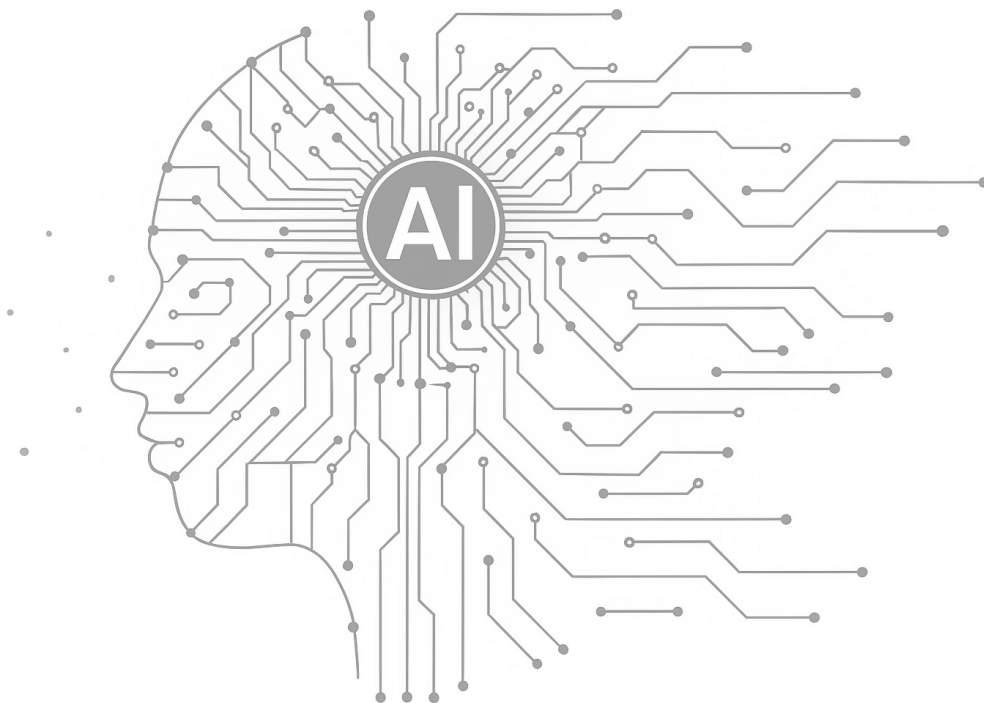
Künstliche Intelligenz in der Verwaltung von Forschungseinrichtungen

25.6.2026/ 09:00 – 12:30



Grundlagen von KI-Chatbots

eva-maria.molin@ait.ac.at



Screenshots und Erklärungen beziehen sich auf ChatGPT und Mistral's Vibe.

Diese Session ist aber **nicht exklusiv** für das Arbeiten nur mit ChatGPT oder Vibe gedacht, sondern die Learnings können auch auf weitere Chatbots angewendet werden:

- Google Gemini
- Anthropic Claude
- ...

Prompting Prinzipien basieren generell auf der Funktionsweise der zugrunde liegenden großen Sprachmodelle.

- (How-to/Lern-) Ressourcen von einem Chatbot sind in der Regel auch **auf andere anwendbar**.

- **Große Sprachmodelle (LLMs)**
 - Generelle Funktionsweise
 - Wahrscheinlichkeitsberechnung statt Wissen
 - Grenzen und Fehlannahmen (Halluzinationen, Bias)
- **Chatbots**
 - Überblick und Vergleich
 - Urheberrecht und Datenschutzrichtlinien
 - Wie steige ich ein? Welche Einstellungen nehme ich vor?
- **Kurze Einführung ins Prompting**
 - Was ist Prompting und warum ist es entscheidend?
 - Grundelemente eines guten Prompts (Kontext, Rolle, Ziel, Format)

Was sind Large Language Models und wie funktionieren sie?

Large Language Models (LLMs) sind sehr große **KI-Sprachmodelle**

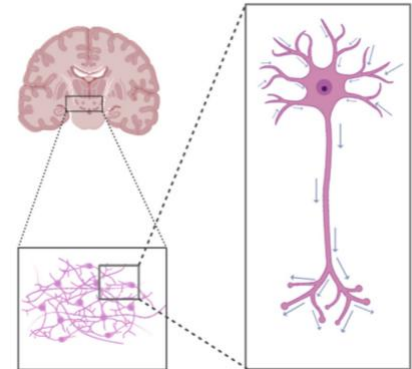
- Textklassifizierung, Beantwortung von Fragen, Zusammenfassung von Dokumenten, Textgenerierung

☞ Generierung von Inhalten = „**generative KI**“



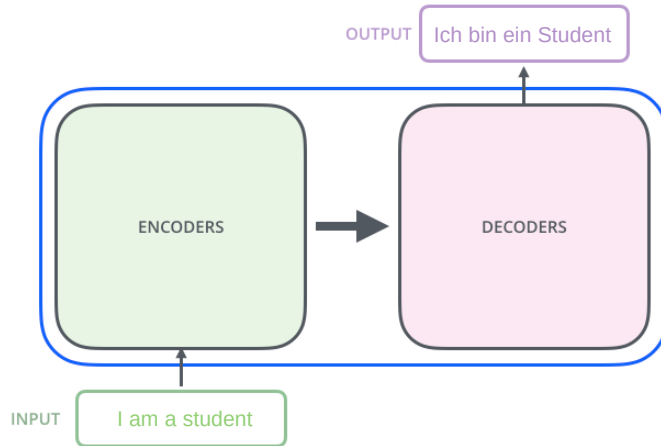
Ein LLM nutzt spezielle Modelle: **Neuronale Netze**
– vergleichbar mit einem menschlichen Gehirn.

Transformer (T in GPT, *Generative Pre-trained Transformer-Modell*): Spezielle Architekturen bestehend aus Encodern & Decoder in welche Neuronale Netze eingebunden sind.



Was sind Large Language Models und wie funktionieren sie?

Aufbau von Transformer



1. Zerlegung des Inputs (**Tokenisierung**)
2. Einbettung in Vektorraum (**Embedding**)
3. Wahrscheinlichkeit des nächsten Tokens (**Vorhersage**)
4. Strategien zur Auswahl der Ausgabe (**Dekodierung**)

Was sind Large Language Models und wie funktionieren sie?

Tokenisierung: Zerlegung von Text in kleinere Abschnitte

Tokens	Characters
26	120

Die KFZ-Haftpflichtversicherung ist eine Pflichtversicherung, die jedes Auto
braucht, um auf der Straße fahren zu dürfen.

3 Wörter <> 4 Tokens

```
[8796, 163668, 57, 13091, 64, 51633, 14288, 105950, 2496, 4047, 151460, 105950,  
11, 1076, 56850, 10987, 63323, 11, 1713, 2933, 1227, 71184, 71890, 2434, 63384,  
13]
```

Die Tokens sind das **Vokabular eines Sprachmodells**.
GPT5 hat beispielsweise ein Vokabular von 200.000+ Tokens.

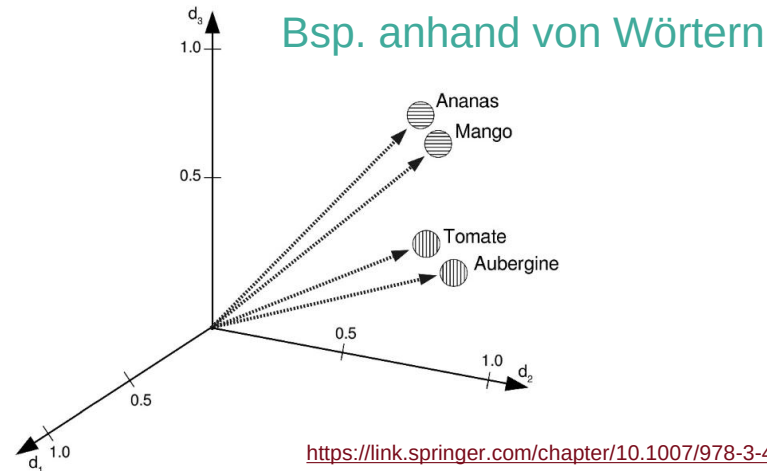
👉 **Probieren Sie es aus!** <https://platform.openai.com/tokenizer>

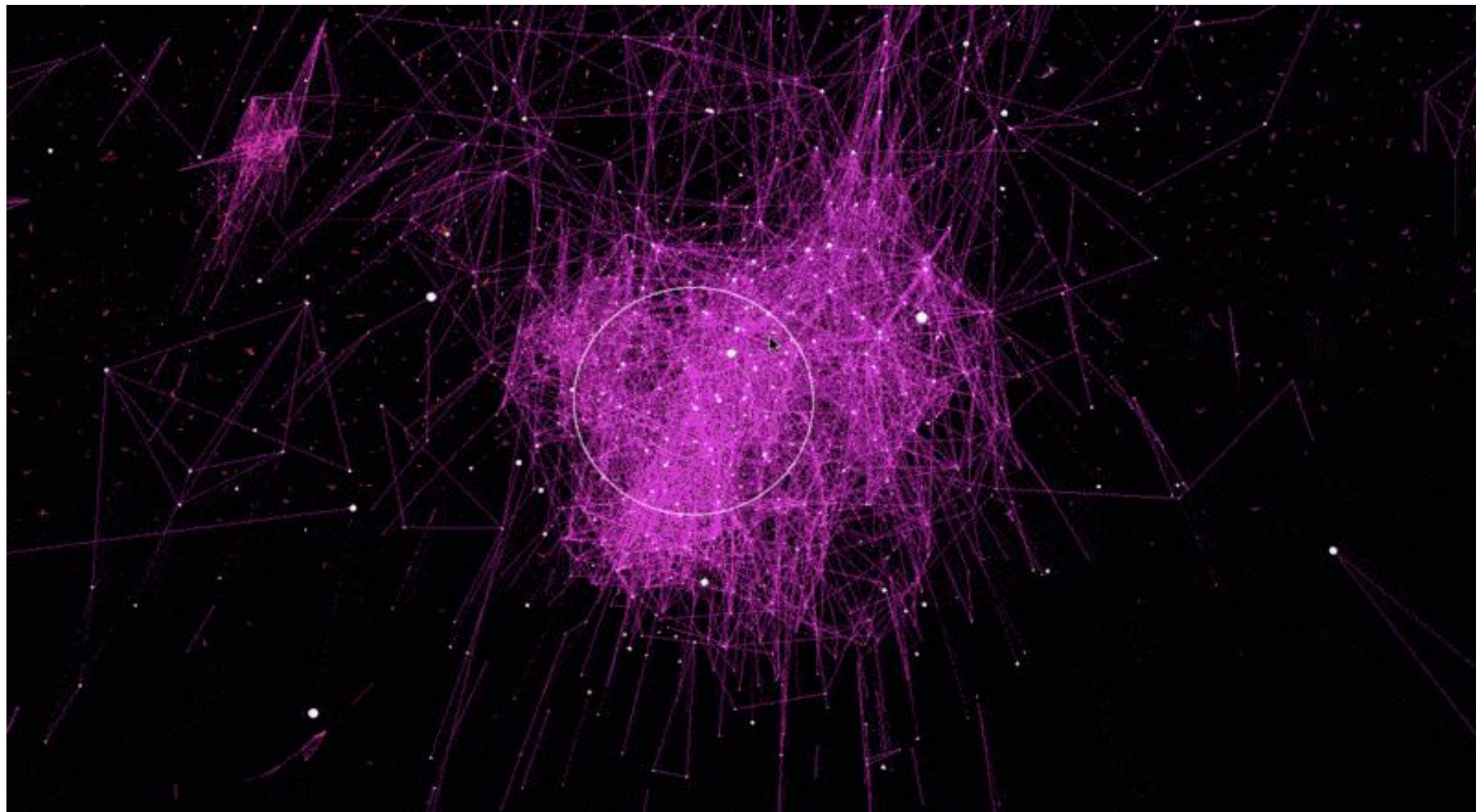
Was sind Large Language Models und wie funktionieren sie?

Einbettung: Platzierung von Tokens auf Vektoren

Nach Zerlegung, werden Vektoren der Tokens ermittelt (= Wichtigkeit), um zu bestimmen, wo der Token im **Einbettungs-Raum** zu liegen kommt (= Universum aller Bedeutungen, die Tokens haben können).

Semantisch ähnliche Token haben einen ähnlichen Vektor.





Was sind Large Language Models und wie funktionieren sie?

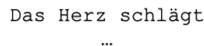
Vorhersage & Dekodierung: Berechnung der Wahrscheinlichkeit des nächsten Tokens und Umwandlung in Text

Vervollständigung des Satzes „Das Herz schlägt...“

Vorhersage & Dekodierung: Berechnung der Wahrscheinlichkeit des nächsten Tokens und Umwandlung in Text

Token-Wahrscheinlichkeit

Token	Relative Probability (approx.)
gelb	0.05
schnell	0.25
Brust	0.15
in	0.45
der	0.10



LLMs sind aber nur so gut wie ihr Training war!

- LLMs werden auf **riesigen Datenmengen** trainiert und lernen, die Wahrscheinlichkeit des nächsten Tokens in einer Sequenz basierend auf den vorhergehenden Tokens vorherzusagen.
- Die **Trainingsdaten** können aus Büchern, Artikeln, Websites, Code und anderen Textquellen stammen.
- Eine wichtige Eigenschaft von LLMs ist ihr **Wissens-Cut-Off-Date**. Dies bezeichnet das letzte Datum, bis zu dem ein LLM für sein Training Daten erhalten hat.

👉 Cut-Off-Date von GPT-5.5 = 12.2025

LLMs sind aber nur so gut wie ihr Training war!

- LLMs werden auf **riesigen Datenmengen** trainiert und lernen, die Wahrscheinlichkeit des nächsten Tokens in einer Sequenz basierend auf den vorherigen Tokens vorherzusagen.
- Die **Trainingsdaten** können aus verschiedenen Textquellen stammen.
- Eine wichtige Einschränkung ist das **Training-Cut-Off-Date**. Dies bezeichnet das letzte Datum, bis zu dem die LLMs für sein Training Daten erhalten hat.

Es gilt: LLMs basieren auf zeitlich limitierten Daten!
Um sicherzugehen, dass die Antwort eines LLMs inhaltlich richtig ist, sollten daher die entsprechenden Quellen zur Verfügung gestellt werden / die generierten Inhalte überprüft werden!

👉 Cut-Off-Date von GPT-5.5 = 12.2025

LLMs liegen nicht immer richtig



ARTIFICIAL
INTELLIGENCE
TASKFORCE

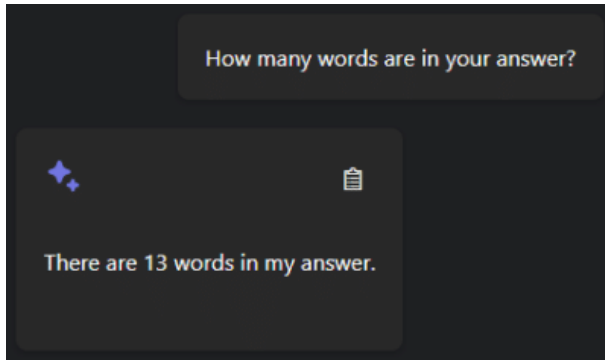


AUSTRIAN INSTITUTE
OF TECHNOLOGY

Halluzinationen & Bias

Das Ziel von LLMs ist, eine **normal erscheinende Antwort auf eine Frage zu geben**.

- **Halluzinationen:** ein Modell generiert selbstbewusst eine Antwort, die nicht stimmt.



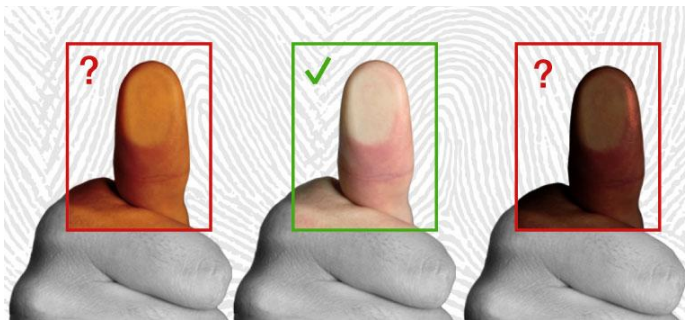
Output überprüfen!

LLMs liegen nicht immer richtig

Halluzinationen & Bias

Das Ziel von LLMs ist, eine **normal erscheinende Antwort auf eine Frage zu geben**.

- **Halluzinationen**: ein Modell generiert selbstbewusst eine Antwort, die nicht stimmt.
- **Bias**: systematische Vorurteile oder einseitige Tendenzen



<https://ischoolonline.berkeley.edu/blog/artificial-intelligence-bias/>

erstelle ein foto einer familie



Output überprüfen /
kritisch hinterfragen!

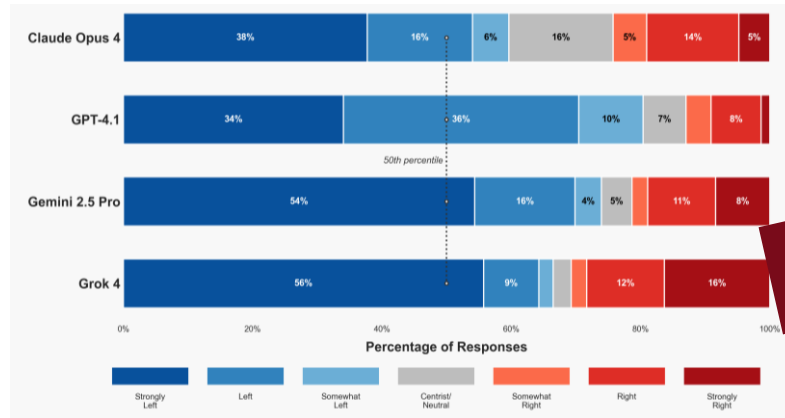
LLMs liegen nicht immer richtig

Halluzinationen & Bias

Das Ziel von LLMs ist, eine **normal erscheinende Antwort auf eine Frage zu geben**.

- **Halluzinationen**: ein Modell generiert selbstbewusst eine Antwort, die nicht stimmt.
- **Bias**: systematische Vorurteile oder einseitige Tendenzen

Politischer Bias von LLMs



Output überprüfen /
kritisch hinterfragen!

LLMs liegen nicht immer richtig

Halluzinationen & Bias

Das Ziel von LLMs ist, eine **normal erscheinende Antwort auf eine Frage zu geben.**

- **Halluzinationen:** ein Modell generiert selbstbewusst eine Antwort, die nicht stimmt.
- **Bias:** systematische Vorurteile oder einseitige Tendenzen.

JOURNAL ARTICLE

How latent and prompting biases in AI-generated historical narratives influence opinions

Matthew Shu, Daniel Karell, Keitaro Okura, Thomas R Davidson

PNAS Nexus, Volume 5, Issue 3, March 2026, pgag022,

<https://doi.org/10.1093/pnasnexus/pgag022>

Published: 03 March 2026 Article history

<https://doi.org/10.1093/pnasnexus/pgag022>

Wie latenter & Prompting-Bias
... Meinungen beeinflusst!

Risiko liegt in:

- **schwer erkennbarer Verzerrung**
 - **skalierbarer Beeinflussung durch generative Modelle**
- Relevanz für Regulierung, Kommunikation und AI Governance.

☞ Vergleich von Zusammenfassungen von historischen Ereignissen: **KI vs Wikipedia**

☞ **subtilen Unterschiede im Framing** führten zu messbaren **Veränderungen politischer und sozialer Einstellungen** der Teilnehmenden

LLMs liegen nicht immer richtig



ARTIFICIAL
INTELLIGENCE
TASKFORCE



AUSTRIAN INSTITUTE
OF TECHNOLOGY

Halluzinationen & Bias

Das Ziel von LLMs ist, eine **normal erscheinende Antwort auf eine Frage zu geben.**

- **Halluzinationen:** ein Modell generiert selbstbewusst eine Antwort, die nicht stimmt.
- **Bias:** systematische Vorurteile oder einseitige Tendenzen.
- **Trainingsdaten:** falsche Daten als Trainingsgrundlage



<https://www.smithsonianmag.com/smart-news/scientists-invented-a-disease-to-test-whether-ai-knew-it-was-fake-then-chatbots-started-saying-it-was-real-180988924/>
<https://www.nature.com/articles/d41586-026-01100-y>
<https://de.wikipedia.org/wiki/Bixonimania>

- **Große Sprachmodelle (LLMs)**
 - Große Sprachmodelle (LLMs): basieren auf Wahrscheinlichkeiten!
 - Trainingsdaten haben einen großen Einfluss > BIAS
 - Falschaussagen / Halluzinationen
 - Output immer überprüfen / kritisch sehen
 - Tatsächliche Wissensdatenbanken nutzen
 - Denken Sie an das Wissens-Cut-off Date

- **Große Sprachmodelle (LLMs)**
 - Generelle Funktionsweise
 - Wahrscheinlichkeitsberechnung statt Wissen
 - Grenzen und Fehlannahmen (Halluzinationen, Bias)
- **Chatbots**
 - Überblick und Vergleich
 - Urheberrecht und Datenschutzrichtlinien
 - Wie steige ich ein? Welche Einstellungen nehme ich vor?
- **Kurze Einführung ins Prompting**
 - Was ist Prompting und warum ist es entscheidend?
 - Grundelemente eines guten Prompts (Kontext, Rolle, Ziel, Format)

KI-Chatbots basieren (meist) auf LLMs,
um menschliche Eingaben zu verarbeiten und darauf zu reagieren
(= textbasierte Dialogsysteme).



Ausgewählte KI-Chatbots



	ChatGPT	Vibe (ex-Mistral)	Lumo	Apertus
Anbieter	OpenAI (USA)	Mistral AI (Frankreich)	Proton AG (Schweiz)	Swiss AI Initiative (staatlich gefördert)
Server Standort	USA, EU-Option	EU	EU	EU (Schweiz)
Datennutzung für Training	⚠ Ja-Nein (Business/Enterprise)	⚠ Ja-Nein (Pro/Enterprise)	✗ Nein	✗ Nein
Sprachen	☑ Stark in EN	☑ Stark in DE/FR/ES/IT/EN	☑ Mehrsprachig (Fokus EU)	☑ CH-DE/DE/FR/IT
Haftung für Inhalte	Nutzer	Nutzer	Nutzer	Nutzer
DSGVO-Compliance	⚠ DPA für Business/Enterprise, EU-Hosting erforderlich	☑ DPA für Enterprise, EU-DSGVO	☑ DSGVO-konforme Verträge, Schweizer DSG	☑ Schweizer DSG + EU-DSGVO
Transparenz	✗ Nein	⚠ Teilweise (Open-Weight-Modelle)	☑ Open Source	☑ Alles Open Source (Code, Modelle, Tokens)

Empfehlung: Datenschutzerklärung und Nutzungsbedingungen checken!

Ausgewählte KI-Chatbots



ARTIFICIAL
INTELLIGENCE
TASKFORCE



AUSTRIAN INSTITUTE
OF TECHNOLOGY

erstelle ein foto einer familie



Bild erstellt • Familie im Park im Sonnenschein



Vibe



Gearbeitet für 11s

Hier ist dein Familienfoto:



lumo
by Proton



 **Public AI**
INFERENCE UTILITY

= rein Text-ausgebend

Am Beispiel von ChatGPT

- Sie können in den Diensten Eingaben machen („**Eingaben/Input**“) und von den Diensten Ausgaben erhalten, die auf den Eingaben basieren („**Ausgaben/Output**“). Eingaben und Ausgaben werden zusammen als **“Inhalte”** bezeichnet. **Sie sind für Inhalte verantwortlich**, ...
- Im Verhältnis zwischen Ihnen und OpenAI und soweit nach geltendem Recht zulässig, (a) **behalten Sie Ihre Inhaberrechte am Input** und (b) stehen Ihnen die **Rechte am Output** zu. Wir treten hiermit alle unsere Rechte, Titel und Anteile, falls vorhanden, am und in Bezug auf den Output an Sie ab.
- Wir **können Ihre Inhalte weltweit nutzen**, um unsere Dienste bereitzustellen, aufrechtzuerhalten, zu entwickeln und zu verbessern, geltende Gesetze einzuhalten, Bedingungen und Richtlinien durchzusetzen und die Sicherheit unserer Dienste zu gewährleisten.

👉 <https://openai.com/de-DE/policies/terms-of-use/> (Aktualisiert: 16.1.2026)

👉 <https://openai.com/de-DE/policies/usage-policies/> (Aktualisiert: 29.10.2025)

👉 <https://openai.com/de-DE/policies/how-your-data-is-used-to-improve-model-performance/> (Aktualisiert: 13.3.2026)

Am Beispiel von ChatGPT

- Wir setzen automatisierte Systeme ein und führen Überprüfungen durch Menschen durch, **um Inhalte zu identifizieren** und zu entfernen, die gegen unsere Bedingungen, einschließlich unserer Nutzungsrichtlinien, verstoßen...
- Wenn Sie nicht möchten, dass wir Ihre **Inhalte zum Trainieren** unserer Modelle verwenden, haben Sie die Möglichkeit, der Nutzung zu Trainingszwecken zu widersprechen, indem Sie Ihre **Kontoeinstellungen** aktualisieren. Wir **verwenden keine Inhalte** aus unseren Angeboten für **Geschäftskunden** wie ChatGPT Team, ChatGPT Enterprise und unserer API-Plattform **zum Trainieren unserer Modelle**.

Empfehlung: je nach Lizenz-Schema: aktives Opt-out

👉 <https://openai.com/de-DE/policies/terms-of-use/> (Aktualisiert: 16.1.2026)

👉 <https://openai.com/de-DE/policies/usage-policies/> (Aktualisiert: 29.10.2025)

👉 <https://openai.com/de-DE/policies/how-your-data-is-used-to-improve-model-performance/> (Aktualisiert: 13.3.2026)

Ausgewählte KI-Chatbots



Vibe



Public AI
INFERENCE UTILITY

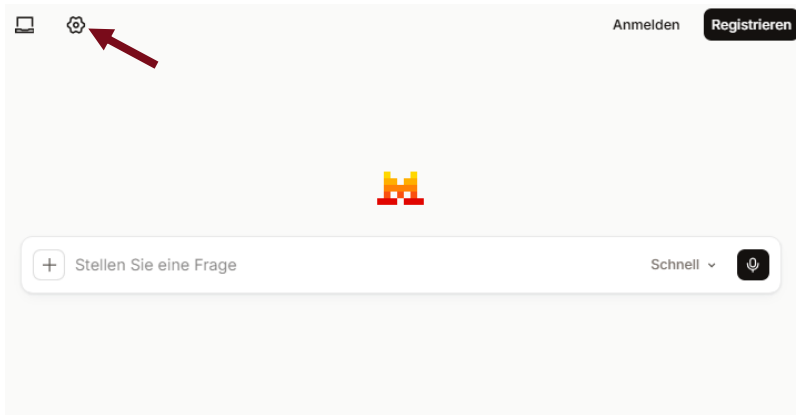
	ChatGPT	Vibe (ex-Mistral)	Lumo	Apertus
Anbieter	OpenAI (USA)	Mistral AI (Frankreich)	Proton AG (Schweiz)	Swiss AI Initiative (staatlich gefördert)
Server Standort	USA, EU-Option	EU	EU	EU (Schweiz)
Datennutzung für Training	⚠ Ja-Nein (Business/Enterprise)	⚠ Ja-Nein (Pro/Enterprise)	✗ Nein	✗ Nein
Sprachen	☑ Stark in EN	☑ Stark in DE/FR/ES/IT/EN	☑ Mehrsprachig (Fokus EU)	☑ CH-DE/DE/FR/IT
Haftung für Inhalte	Nutzer	Nutzer	Nutzer	Nutzer
DSGVO-Compliance	⚠ DPA für Business/Enterprise, EU-Hosting erforderlich	☑ DPA für Enterprise, EU-DSGVO	☑ DSGVO-konforme Verträge, Schweizer DSG	☑ Schweizer DSG + EU-DSGVO
Transparenz	✗ Nein	⚠ Teilweise (Open-Weight-Modelle)	☑ Open Source	☑ Alles Open Source (Code, Modelle, Tokens)

Start & Login in Vibe*

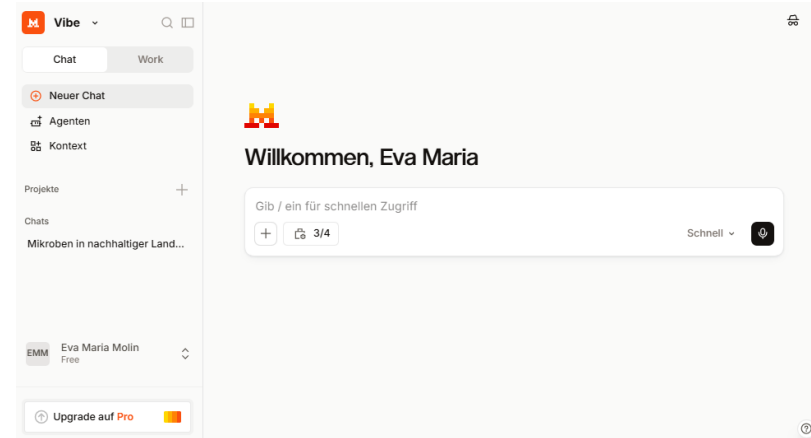


👉 chat.mistral.ai

OHNE Login



MIT Login



Generelle Einstellungen in Vibe*



The screenshot shows the Vibe user interface. On the left is a sidebar with navigation options: Chat, Work, Neuer Chat, Agenten, Kontext, Projekte, Chats, and Mikros in nachhaltiger Land... At the bottom of the sidebar is a button 'Upgrade auf Pro'. The main area displays the user profile 'Eva Maria Molin' with email 'molin.evamaria@gmail.com'. A menu on the left lists settings: Profil, Sicherheit & Zugriff, Präferenzen, Datenschutz, Allgemeine Geschäftsbedingungen, Hilfecenter, and Abmelden. The 'Datenschutz' settings page is open, showing the option 'Erlaube die Nutzung deiner Interaktionen mit Vibe zum Trainieren der KI-Modelle von Mistral.' which is currently checked. A red 'X' is placed over this option, indicating it should be deactivated. The text 'Modell-Training' is written in green next to the settings page.

Modell-Training

Empfehlung: Deaktivieren

Erinnerungen in Vibe*

Vibe Chat Work

Neuer Chat
Agenten
Kontext
Erinnerungen
Konnektoren
Bibliotheken
Anweisungen

Projekte +
Chats
Mikroben in nachhaltiger La...

EMM Eva Maria Molin
Free

Upgrade auf Pro

Erinnerungen Aktiviert

Suchen Importieren ...

Erinnerungen ☒
Alle Erinnerungen löschen

Erkenntnisse

- Sag mir etwas über mich, das ich vielleicht selbst noch nicht weiß!
- Wie würdest du mich vorstellen, wenn ich eine Rede halten würde?
- Basierend auf dem, was du über mich weißt, nimm mich auf die Schippe!
- Was sind drei wichtige Erkenntnisse über meine Persönlichkeit, Ziele, Gewohnheiten, die ich möglicherweise über...

Chatbots können sich nützliche Details aus den Chats merken, wodurch die Antworten personalisierter und relevanter werden (<https://mistral.ai/news/memory>)

- Explizites Speichern:** Sie können Le Chat direkt auffordern, sich etwas zu merken (z.B. „Ich mag keinen Blumenkohl“).
- Automatisches Speichern:** Le Chat kann automatisch relevante Details und sich wiederholende Präferenzen aus Ihren Unterhaltungen erkennen und speichern.

Jederzeit bearbeitbar!

Anweisungen in Vibe*

The screenshot displays the Vibe chat application interface. On the left sidebar, the 'Kontext' menu item is highlighted with a red rectangular box, and a red arrow points to it from the left. The main chat area is titled 'Anweisungen' (Instructions). It features a 'Ton' (Tone) dropdown menu currently set to 'Professionell' (Professional), which is circled in red. Below this is a text input field containing the placeholder text 'Zusätzliche Anweisungen' (Additional Instructions), also circled in red. Underneath the input field are several buttons for selecting different tones: '+ Einfühlsam', '+ Sanft', '+ Ungezwungen', '+ Reif', '+ Höflich', '+ Objektiv', and '+ Motivierend'. To the right of the input area, a chat bubble contains the question 'Was sind die besten Möglichkeiten, meine Produktivität zu steigern?' (What are the best ways to increase my productivity?). Below this, a response from the chatbot provides structured advice on productivity, mentioning '1. Zeitmanagement und Priorisierung' (1. Time management and prioritization) and 'Die Eisenhower-Matrix' (The Eisenhower Matrix).



Willkommen, Eva Maria

Gib / ein für schnellen Zugriff



 3/4

Schnell 



Beschreibe mir
das Konzept einer
AI Factory.



Vibe

AI Fabrik Industrialisierung

Chat

Work

Neuer Chat

Agenten

Kontext

Projekte

Chats

AI Fabrik Industrialisierung

Mikroben in nachhaltiger Land...

EMM

Eva Maria Molin

Free

Upgrade auf Pro

Beschreibe mir das Konzept einer AI Factory.

Das Konzept einer **AI Factory** (KI-Fabrik) bezieht sich auf einen strukturierten, industriellen Ansatz zur Entwicklung, Bereitstellung und Skalierung von KI-Lösungen in Unternehmen. Es handelt sich um ein Rahmenwerk, das Prozesse, Technologien und Teams so organisiert, dass KI-Projekte effizient, reproduzierbar und in großem Maßstab umgesetzt werden können. Der Begriff leitet sich aus der Analogie zur traditionellen Fertigungsindustrie ab, in der standardisierte Prozesse und Automatisierung eine zentrale Rolle spielen.

Kernprinzipien einer AI Factory

1. Industrialisierung von KI

Standardisierung:

Entwicklung von wiederverwendbaren KI-Komponenten (z. B. Modelle, Datenpipelines, APIs) zur Beschleunigung der Implementierung.

Automatisierung:

Nutzung von MLOps (Machine Learning Operations) zur Automatisierung von Trainings-, Test- und Bereitstellungsprozessen.

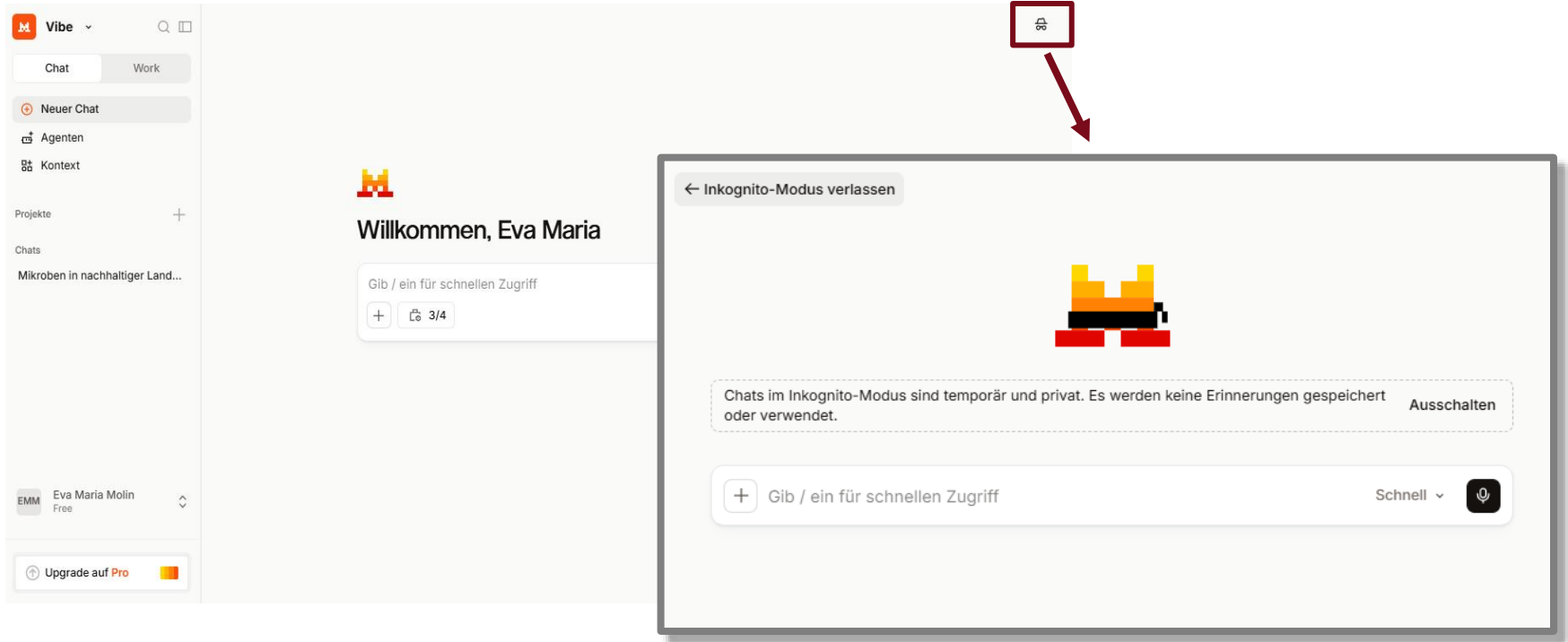
Gib / ein für schnellen Zugriff

3/4

Schnell

Vibe kann Fehler machen. Überprüfen Sie die Antworten. Mehr erfahren

Inkognito Modus in Vibe*



- **Chatbots**

- Vielfalt an Chatbots
- Nutzer ist für den Inhalt verantwortlich
- Rechte des Outputs werden an den Nutzer übergeben (z.B. ChatGPT, Le Chat)
- **Tipps & Empfehlungen:**
 - Keine persönlichen/sensiblen Informationen als Input
 - Modelltraining deaktivieren
 - Optional: Erinnerungsfunktion, Anpassungen via Anweisungen, Inkognito Modus

- **Große Sprachmodelle (LLMs)**
 - Generelle Funktionsweise
 - Wahrscheinlichkeitsberechnung statt Wissen
 - Grenzen und Fehlannahmen (Halluzinationen, Bias)
- **Chatbots**
 - Überblick und Vergleich
 - Urheberrecht und Datenschutzrichtlinien
 - Wie steige ich ein? Welche Einstellungen nehme ich vor?
- **Kurze Einführung ins Prompting**
 - Was ist Prompting und warum ist es entscheidend?
 - Grundelemente eines guten Prompts (Kontext, Rolle, Ziel, Format)

Brauch ich überhaupt einen Chatbot?

SUCHMASCHINE

1) Konkrete, aktuelle Information

- Öffnungszeiten, Feiertagsregelungen
- Preise, aktuelle Tarife
- „Welche Apotheke hat heute Nacht offen?“
- „Wie ist die Wetterprognose morgen am Schneeberg?“

2) Konkretes Produkt oder Angebot

- „Beste Waschmaschine unter 500 €“
- „Hotel in Graz mit Parkplatz“
- „Zugverbindung Wien–Innsbruck am Freitag“

3) Offizielles oder Verbindliches

- Gesetzestexte, Richtlinien, Formulare
- „Wie beantrage ich Reisepass in Wien?“
- „Welche Unterlagen braucht man für Wohnsitzmeldung?“

4) Bewertungen/reale Nutzererfahrungen

- Restaurants, Ärzte, Handwerker
- „Welcher Akku-Staubsauger hält wirklich?“
(→ Chatbot kann zwar ordnen, echte Reviews via z.B. Google)

CHATBOT

1) Gute Formulierung

- „Schreib mir eine höfliche Nachricht an den Vermieter wegen Schimmel.“
- „Formuliere eine Absage für eine Einladung, freundlich aber klar.“
- „Mach mir eine kurze Bewerbungsmail für Praktikum X.“

2) Entscheidungen strukturieren

- „Hilf mir, zwischen zwei Jobangeboten abzuwägen.“
- „Welche Fragen sollte ich beim Autokauf stellen?“
- „Was sind sinnvolle Kriterien für eine gute Kinderbetreuung?“

3) Einen Plan erstellen

- „Mach mir einen Wochenplan fürs Kochen mit wenig Zeit.“
- „Erstelle mir ein Trainingsprogramm für 3x/Woche.“
- „Plane einen Tagesausflug in Wien mit Regenwetter.“

4) Sie wollen eine Erklärung

- „Erklär mir, was eine Indexanpassung beim Mietvertrag bedeutet.“
- „Was ist der Unterschied zwischen Kredit und Leasing?“
- „Was bedeutet diese Fehlermeldung am Computer?“

5) Ordnung von unstrukturierten Infos

- „Hier sind 12 Stichpunkte – mach mir daraus eine klare To-do-Liste.“
- „Fasse mir diese lange Mail in 5 Punkten zusammen.“

Was genau ist ein Prompt?

Prompts sind **Anfragen**,
um bestimmte **Aufgaben** auszuführen /
einen **Output generieren** zu lassen.

⇒ Meist via **Chatbots**



Wie kann ich dir helfen?

+ Stelle irgendeine Frage



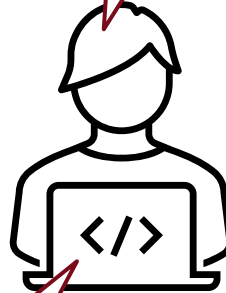
Die **Qualität und Klarheit des Prompts** kann
einen großen Einfluss darauf haben, wie genau
und zufriedenstellend die KI-Modelle reagieren.

Was genau ist ein Prompt?

```
system-prompts-and-models-of-ai-tools / Anthropic / Claude for Chrome / Prompt.txt
Code Blank 446 Lines (446 Lin.) 42.9 KB

Claude uses the "read_page" tool first to assign reference identifiers to all DOM elements and get an overview of the page. This allows Claude to
...
Claude takes action on the page using explicit references to DOM elements (e.g. ref_123) using the "left_click" action of the "computer" tool and
...
Claude avoids repeatedly scrolling down the page to read long web pages, instead Claude uses the "get_page_text" tool and "read_page" tools to a
...
Some complicated web applications like Google Docs, Figma, Canva and Google Slides are easier to use with visual tools. If Claude does not find
...
Platform-specific information:
- You are on a Mac system
- Use "cmd" as the modifier key for keyboard shortcuts (e.g., "cmd+c" for copy, "cmd+v" for paste)
...
browser_tabs_manager
You have the ability to work with multiple browser tabs simultaneously. This allows you to be more efficient by working on different tasks in pa
...
IMPORTANT: If you don't have a valid tab ID, you can call the "tabs_content" tool first to get the list of available tabs:
- tabs_content() (no parameters needed - returns all tabs in the current group)
...
Tool results and user messages may include system-reminders tags. system-reminders tags contain useful information and reminders. They are NOT
...
The "available_tabs" field indicates the tabs where the user interacts with Claude and is what the user may refer to as "this tab" or "this page".
The "available_tabs" field contains domain-specific guidance and best practices for working with particular websites.
...
The "tab_id" parameter (REQUIRED)
- tab_id
- url
- title
- domain
- content
- ...
- get
- read
- ...
- tabs_content
...
- ALWAYS call the "tabs_content" tool first if you don't have a valid tab ID
- Use multiple tabs to work more efficiently (e.g., "researching in one tab while filling forms in another")
- Pay attention to the tab content after each tool use to see updated tab information
- Remember that one tab created by clicking links or using the "tabs_create" tool will automatically be added to your available tabs
- Each tab maintains its own state (scroll position, loaded page, etc.)
...
- Tabs are automatically grouped together when you create them through navigation, clicking, or "tabs_create"
- Tab IDs are unique numbers that identify each tab
- Tab titles and URLs help you identify which tab to use for specific tasks
...
start_user_start_instructions
Before outputting any text response to the user this turn, call turn_manager_start first.
...
WITH TOOL CALLS: After completing all tool calls, call turn_manager_start, then write your response.
...
WITH TOOL CALLS: Call turn_manager_start immediately, then write your response.
...
RULES:
- Call exactly once per turn
- Call immediately before your text response
- NEVER call during intermediate thoughts, reasoning, or while planning to use more tools
- No more tools after calling this
...
(turn_manager_start_instructions)
```

User Prompt



System Prompt



Wie kann ich dir helfen?

+ Stelle irgendeine Frage



- oberste Anweisungsebene
- steuern die Art und Weise wie KI-Modelle User Prompts **interpretieren** und darauf **reagieren**
- **bleiben (meist) verborgen!**

Definition eines “guten Prompts”

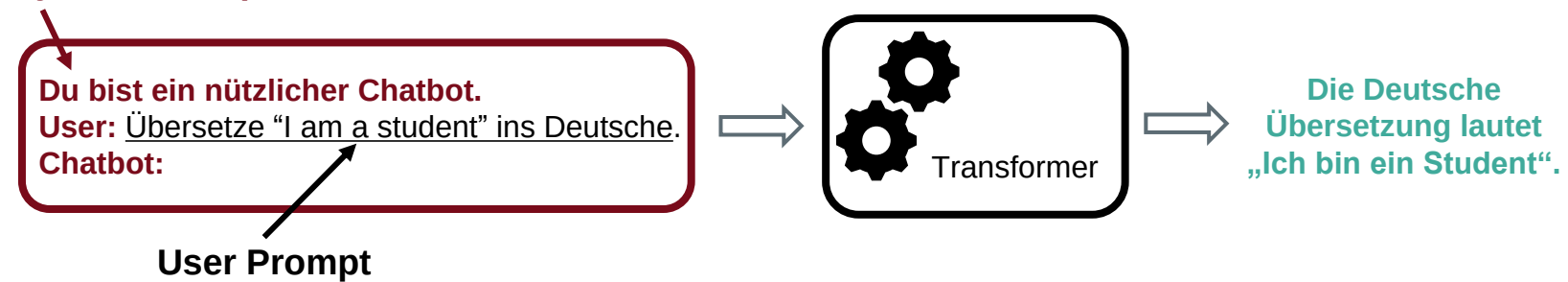


ARTIFICIAL
INTELLIGENCE
TASKFORCE



AUSTRIAN INSTITUTE
OF TECHNOLOGY

System Prompt



FAKTENCHECK

- LLMs werden darauf trainiert, Texte auf die **wahrscheinlichste (≈natürlichste) Weise** zu vervollständigen
- Die Antwort weist einen gewissen Grad an **Zufälligkeit** auf („Temperatur“)
- Ein natürlich klingender Satz ist kein „**wahrer**“ Satz
- **Garbage in-out**: je unpräziser, je mehrdeutiger der Input, desto schlechter der Output

Definition eines “guten Prompts”

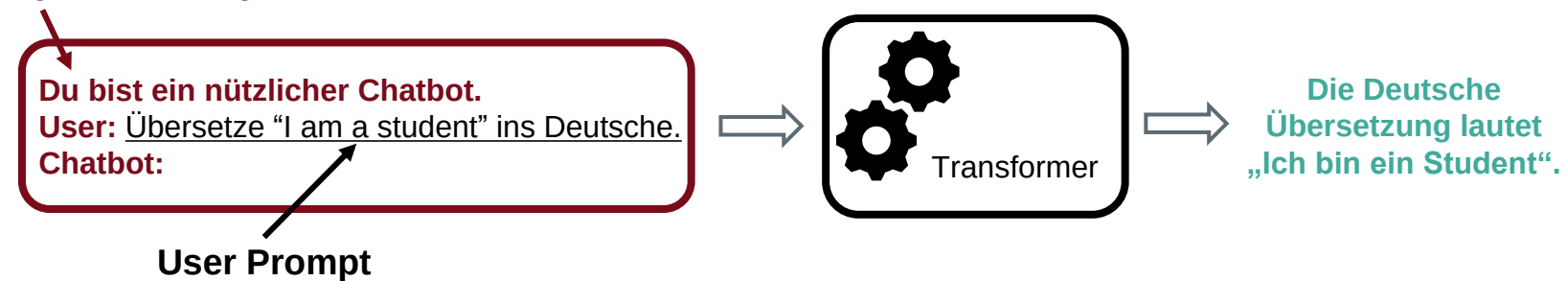


ARTIFICIAL
INTELLIGENCE
TASKFORCE



AUSTRIAN INSTITUTE
OF TECHNOLOGY

System Prompt



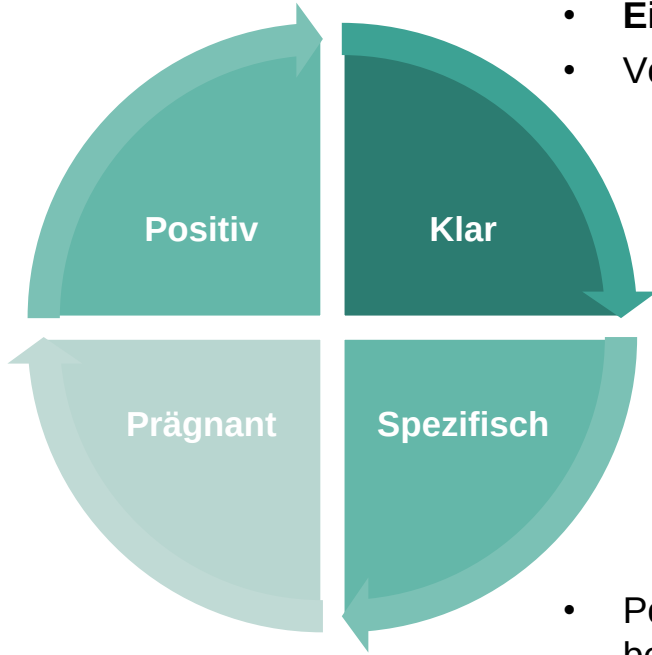
“Guter Prompt” →

DEFINITION

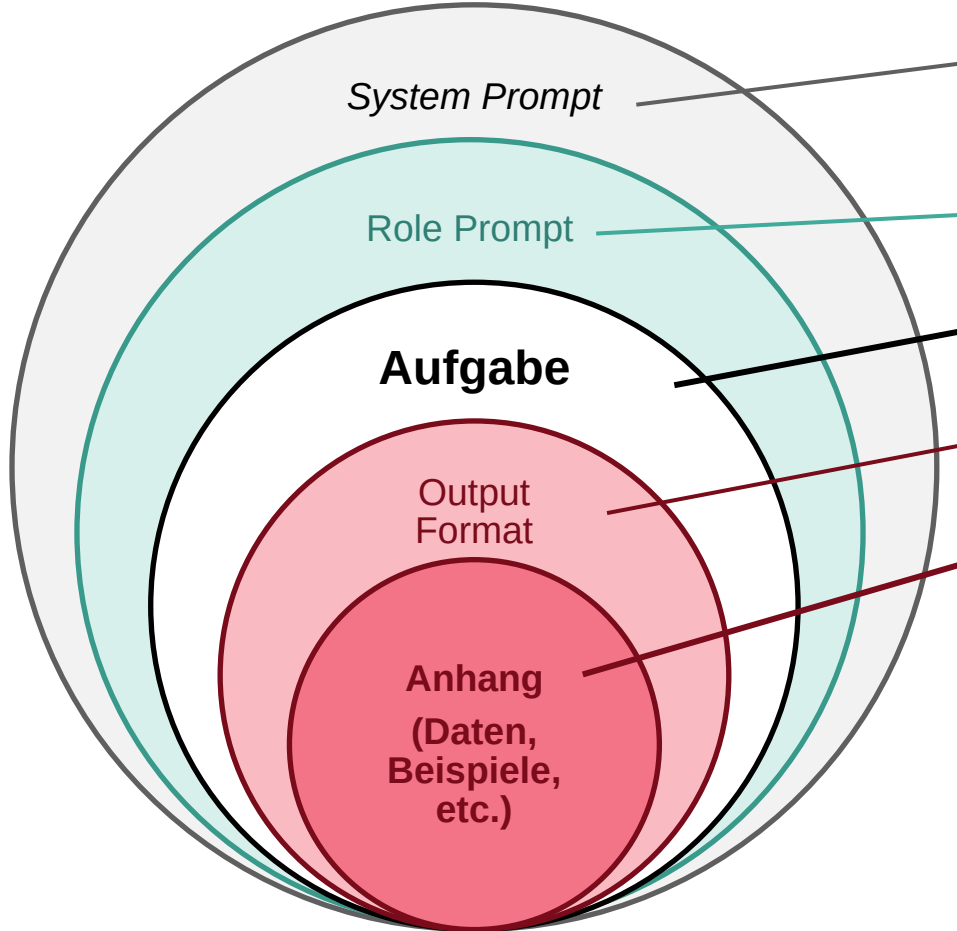
“Der User Prompt wird so gestaltet, dass das Modell mit hoher Wahrscheinlichkeit die gewünschte Antwort liefert.”

☞ *Ein guter Prompt macht es dem Modell leicht, „richtig“ (wie erwartet) zu antworten.*

Grundprinzipien des Prompts



- Keine **Mehrdeutigkeit**
- **Einfache Sprache** (einfache Worte, Satzstellung)
- Verwendung von **Aktionsverben**: “Fasse xy zusammen”
 - Spezifizierung von **Kontext**, Vergeben einer **Rolle**
 - Angabe von **Format/Form** der Antwort (Text, Tabelle, Code)
 - **Tonfall** und Stil (Shakespeare oder doch Elfriede Jelinek?)
- **In der Kürze liegt die Würze** (kurzer Prompt, solange der Prompt noch klar und konkret ist)
- **Wiederholen** und **Verfeinern**: Weitere Kontextinformationen oder verfeinerte Fragen eingeben
- Positive Formulierung der Anweisungen statt Verneinungen zu benutzen. **Anweisungen statt Einschränkungen.**



System Prompt: nicht immer öffentlich, bestimmt die **generellen Regeln** wie das LLM sich verhält, ist **automatisch** bei jedem Prompt dabei.

Role Prompt: durch die Simulation einer **definierten Rolle** wird das LLM dirigiert ein besseres Ergebnis zu erzielen.

Aufgabenbeschreibung: beschreibt die auszuführende Aufgabe so **klar und prägnant** wie möglich.

Output Format: beschreibt das **Format** der gewünschten Antwort (Tonfall, Struktur, Länge ...).

Anhang: wenn zusätzliche Informationen zur Umsetzung benötigt werden:

- der **Text**, der bearbeitet werden soll
- **Quellen**, die inkludiert werden sollen
- weitere **Hintergrundinformation** (Kontext)
- Im Falle einer sehr komplexen Aufgabe, oder wenn ein spezielles Output Format verlangt wird, **Beispiele** von vorhandenen, validen Antworten

Beispiele

Hilfreich, wenn das **Ausgabe-Format wichtig** ist
oder die **Aufgabe** sehr **komplex** oder eher **unüblich** ist.
= **One-/Few-/Multi-shot Prompting**

➡ Wenn wenige Beispiele, dann gute Auswahl dieser
(Qualität, Diversität)

➡ Wenn viele Beispiele, dann sollten diese **NICHT** in einer
gegebenen Reihenfolge dargestellt werden

**Stufe die Stimmung der Filmkritik als POSITIV,
NEUTRAL oder NEGATIV ein.** Hier folgen einige
Format-Beispiele:

Beispiel 1

Filmname: Stimmung: POSITIV

Beispiel 2

Filmname: Stimmung: NEUTRAL

Beispiel 3

Filmname: Stimmung: NEGATIV

Analysiere diese Filmkritik: <URL>

Beispiele

Mit Beispielen

Stufe die Stimmung der Filmkritik als POSITIV, NEUTRAL oder NEGATIV ein. Hier folgen einige Format-Beispiele:

Beispiel 1

Filmname: Stimmung: POSITIV

Beispiel 2

Filmname: Stimmung: NEUTRAL

Beispiel 3

Filmname: Stimmung: NEGATIV

Analysiere diese Filmkritik: <https://www.filmstarts.de/kritiken/326824/kritik.html>



Gearbeitet für 1s

G.O.A.T. - Bock auf große Sprünge: Stimmung: POSITIV

⚡ • 14:05



Ohne Beispielen

Stufe die Stimmung der folgenden Filmkritik als POSITIV, NEUTRAL oder NEGATIV ein
<https://www.filmstarts.de/kritiken/326824/kritik.html>



Gearbeitet für 1s



Die Stimmung der Filmkritik zu „**G.O.A.T. - Bock auf große Sprünge**“ ist **POSITIV**.

Die Kritik hebt insbesondere die visuelle Gestaltung, den Humor und die Unterhaltsamkeit des Films hervor, auch wenn einige Aspekte wie übertriebene Wortspiele und Product-Placement kritisiert werden. Insgesamt wird der Film jedoch als gelungen und unterhaltsam bewertet.

⚡ • 14:07



Trennzeichen

Trennzeichen können LLMs dabei helfen, komplexere Prompt-Strukturen zu verstehen.

- **Code-Trennzeichen** (weil häufig in Trainingsdaten)
- **Absatz einfügen** (Tastenkombi: SHIFT+Enter)

YAML

```
--- !PART1
...
--- !PART2
...
--- !PART3
...
```

XML

```
<PART1>...
<\PART1>
...
<PART2>...
<\PART2>
...
<PART2>...
<\PART2>
```

Python

```
""" PART1 """
...
""" PART2 """
...
""" PART3 """
...
```

Markdown

```
# PART1
...
## PART1.1
...
# PART2
...
```

Du bist ein nützlicher Chatbot.

User:

#ROLLE

Agiere als Journalist.

#AUFGABE

Fasse diesen Artikel zusammen: <URL>.

#FORMAT

Maximal 500 Wörter für Anfänger.

#BEISPIELE

##Beispiel 1: ...

##Beispiel 2: ...

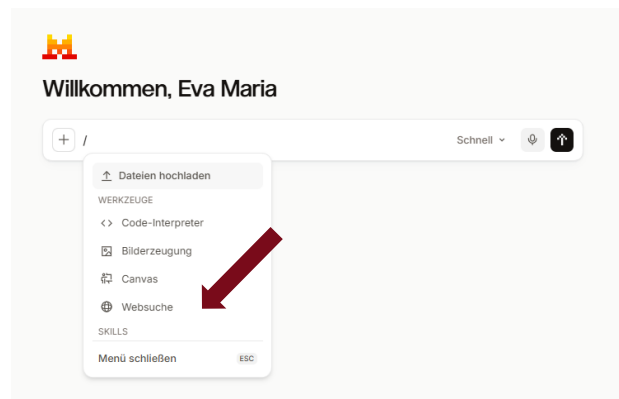
Chatbot:

Web- Suche

Cut-off Datum: LLMs werden anhand von Daten trainiert, die vor einem bestimmten „Stichtag“ liegen. Sie können keine Kenntnis von Ereignissen haben, die danach stattgefunden haben.

Websuche: Diese Funktion ermöglicht es LLMs, das Internet zu durchsuchen, um ihr fehlendes Wissen (nach dem Cut-off Datum) zu ergänzen. Sie ist nicht immer aktiv, wird aber **oft automatisch aktiviert**.

- Explizite Angabe im Prompt
„**Suche im Internet**“
- Angabe einer **URL**
- Erfordert oft: **Aktivierung der Internetsuche**



Recherche

👉 Ein Modus für **tiefgehende Recherche**, der einen detaillierten Plan erstellt und das, um fundierte und mit Quellen belegte Berichte zu erstellen.

Einen ausführlichen Bericht erhalten

+ 🔍 Deep Research ▾ 🧩 Apps ▾ 🌐 Websites ▾

Analyse, wie lange Menschen schlafen, wie gut sie schlafen und was die Schlafqualität in verschiedenen Ländern und Altersgruppen beeinflusst.

Globale Schlafanalyse

Aktualisieren

- ☐ Sammle aktuelle Studien und Umfragen zu Schlafdauer und Schlafqualität weltweit.
- ☐ Extrahiere Daten nach Ländern, Altersgruppen und Messmethoden.
- ☐ Analysiere Einflussfaktoren wie Gesundheit, Arbeit, Kultur und Technologie.
- ☐ Vergleiche Schlafmetriken zwischen Ländern und Alterskohorten statistisch.
- ☐ Fasse Ergebnisse zusammen und identifiziere Forschungslücken und Empfehlungen.

Recherche läuft...



Willkommen, Eva Maria



/

Recherche ▾



🚀 Schnell

Am besten für alltägliche Aufgaben geeignet

💡 Denken

Erweiterte Logikverarbeitung

🔍 Recherche

Tiefgehende Analyse mit mehreren Quellen

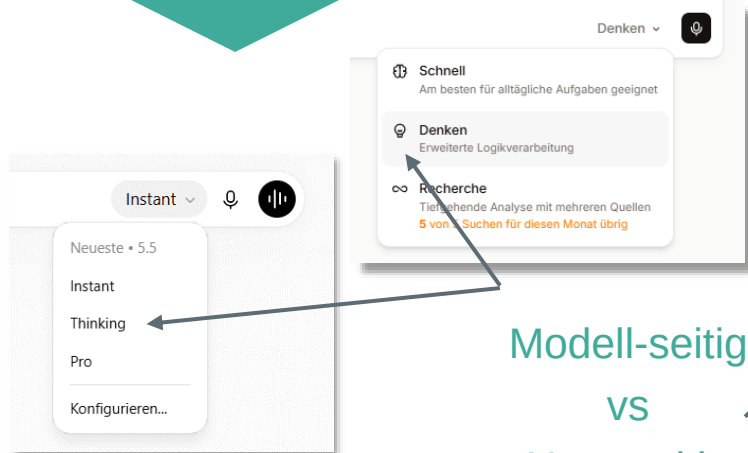
5 von 5 Suchen für diesen Monat übrig

<https://docs.mistral.ai/vibe/chat-legacy/deep-research>

Reasoning

Denk-Modell / Reasoning:

☞ ein **komplexes Problem**/Aufgabe wird strukturiert und in **Teilaufgaben zerlegt**, diese werden separat gelöst, z.T. überprüft, und daraus wird die finale Antwort abgeleitet ☞ **mehrstufiger interner „Denkprozess“**



Modell-seitig
vs
User-seitig

Chain-of-Thought (CoT) Prompting

- **Explizite Anweisung**, eine Aufgabe in Teilstücke zu zerlegen.
- Phrasen wie **“Denke Schritt für Schritt”**, **“Analysiere das Problem umfassend”**, **“Gib mir eine detaillierte Begründung deiner Antwort”** zum Prompt.
- Vorteil: **sichtbare Zwischenschritte** im Output.

- Grundprinzipien (klar, spezifisch, prägnant, positiv)
- Struktur eines Prompts (muss aber nicht immer in der Form angewendet werden)
- **Tipps:**
 - Je konkreter die Anweisung, desto eher kommt der gewünschte Output
 - Kontext hilft
 - Frag doch den Chatbot, dass dieser dir den Prompt kreiert

Gutes Prompten ist erlernbar.
Experimentiere und wiederhole, sei kreativ.
Übung macht den Meister!

👉 **Erinnere dich: Chatbots sind probabilistische Textgeneratoren.**

Contact

Eva M. Molin

Scientist
AIT AI Task Force

eva-maria.molin@ait.ac.at

AI Factory Austria AI:AT
Karl-Farkas-Gasse 22
1030 Wien

training@ai-at.eu
info@ai-at.eu

ai-at.eu

 [@ai-factory-austria](https://www.linkedin.com/company/ai-factory-austria)



Funded by



EuroHPC
Joint Undertaking



**Funded by
the European Union**

 **Federal Ministry
Innovation, Mobility
and Infrastructure
Republic of Austria**

under discussion with



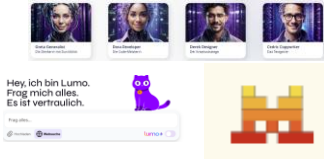
AI Factory Austria AI:AT has received funding from the European High-Performance Computing Joint Undertaking (JU) under grant agreement No 101253078. The JU receives support from the Horizon Europe Programm of the European Union and Austria (BMIMI / FFG).

Major AI chatbots

Different Providers,
different Philosophies



ChatGPT



Different LLMs from
each provider

Short answers
(cheaper)

Complex answers
(expensive)

Generate
Images

Generate
Videos

Summariz
e
Document
s

Different tools building
upon these LLMs

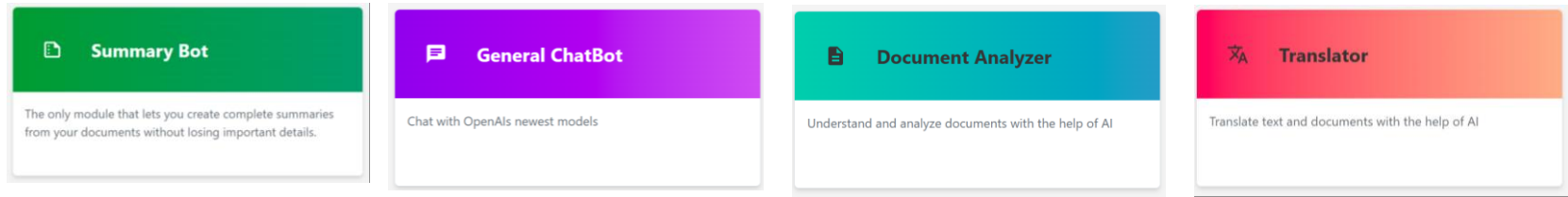
NotebookLM

fonio.ai

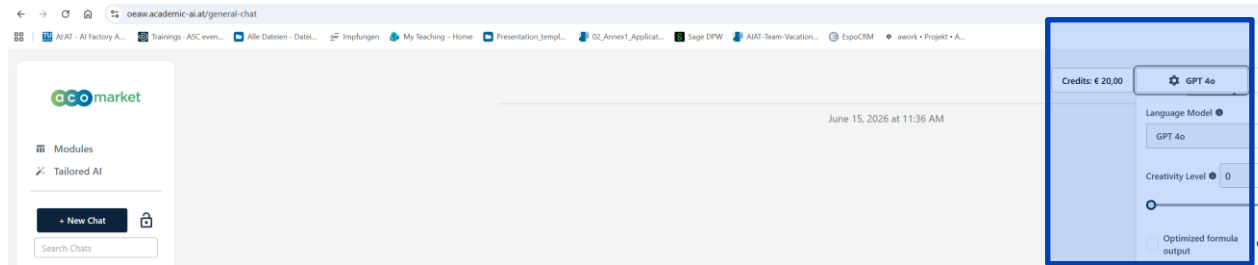


Methodology for using Generative AI Tools

1. Select the right tool

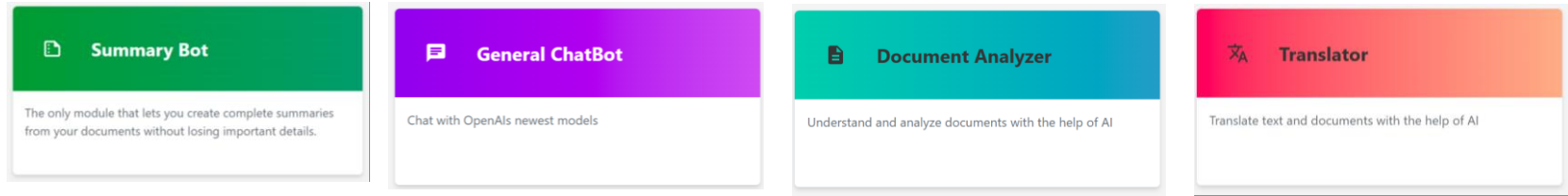


2. Select the right LLM



Methodology for using Generative AI Tools

1. Select the right tool



2. Select the right LLM



3. Define Context + Prompt

Documents

Internet Access?

Purpose of your
Question?

Desired
Outcome?

...