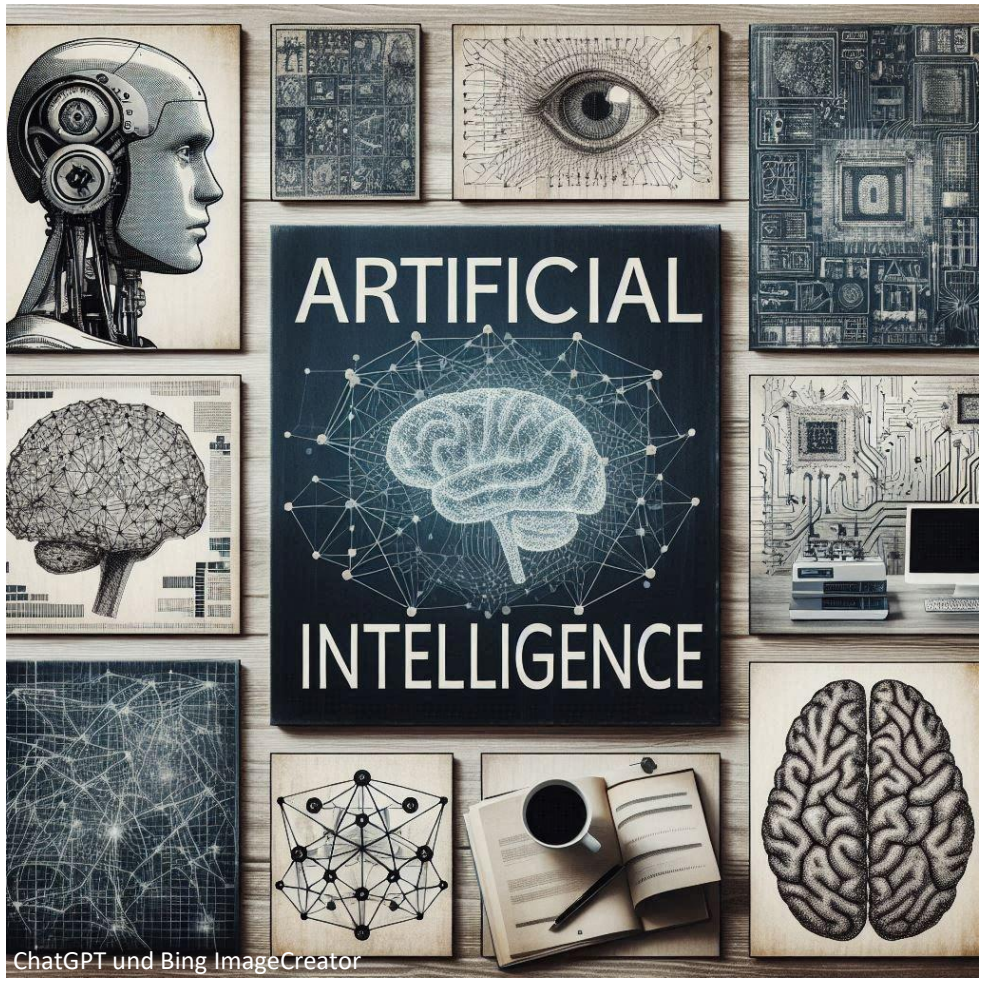
Leibniz Universität
IT Services

Leibniz
Universität
Hannover

LUHKI - LLM für die LUH

Überblick/Schlagworte zur Künstlichen Intelligenz und Vorstellung des Services LUHKI.

Was ist Künstliche Intelligenz (KI)?



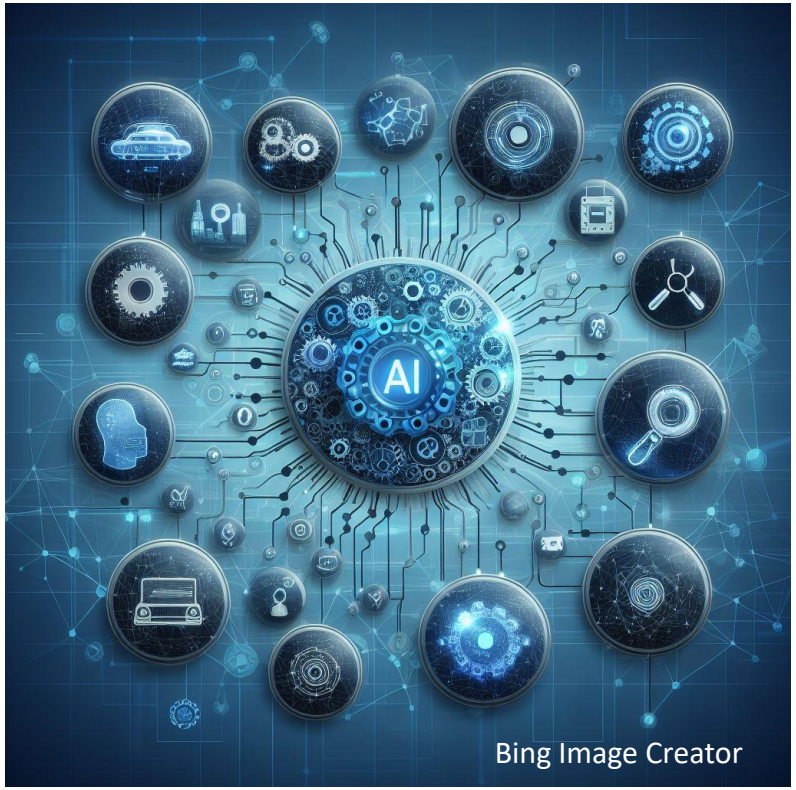
„Künstliche Intelligenz (KI), auch artifizielle Intelligenz (AI), englisch artificial intelligence, ist ein Teilgebiet der Informatik, das sich mit der Automatisierung intelligenten Verhaltens und dem maschinellen Lernen befasst." (https://de.wikipedia.org/wiki/Künstliche_Intelligenz)

Beispiele für Anwendungsmöglichkeiten

- Kommunikation und Unterhaltung: Sprachassistenten, Chatbots
- Transport: Navigation, Autonomes Fahren, Verkehrssteuerung
- E-Commerce und Einzelhandel: Produktempfehlungen, Bestandsmanagement
- Gesundheitswesen: Diagnosetools, virtuelle Assistenten
- Energie: Energieverbrauchsprognose, Kraftwerkssteuerung, Netzmanagement
- Industrie: Vorausschauende Wartung, Qualitätskontrolle, Roboterautomation
- Landwirtschaft: Drohnen und Sensoren zur Überwachung von Feldern, Ertragsvorhersage

Herausforderung – KI an der LUH

- KI bzw. KI-Tools sind nicht ein Produkt sondern eine Basistechnologie für viele Anwendungsbereiche und Werkzeuge
- Extrem hohe Dynamik (Modelle, Tools, Einsatzszenarien)
- Viele verschiedene Modelle/Tools (z.B. Liste mit mehr als 2.000 KI-Tools unter https://buzzmatic.net/ai-tools-die-ultimative-liste/)
- Spezifischer Einsatz in unterschiedlichen Forschungs-/Anwendungsbereichen
- Rechtliche Herausforderungen insb. Vergabe-, Lizenz- und Datenschutzrecht (siehe auch Cloud-Strategie der LUH https://www.intern.uni-hannover.de/de/vademecum/detail/id/1255)
- Fokus auf generativer KI /LLM (Large Language Modelle)



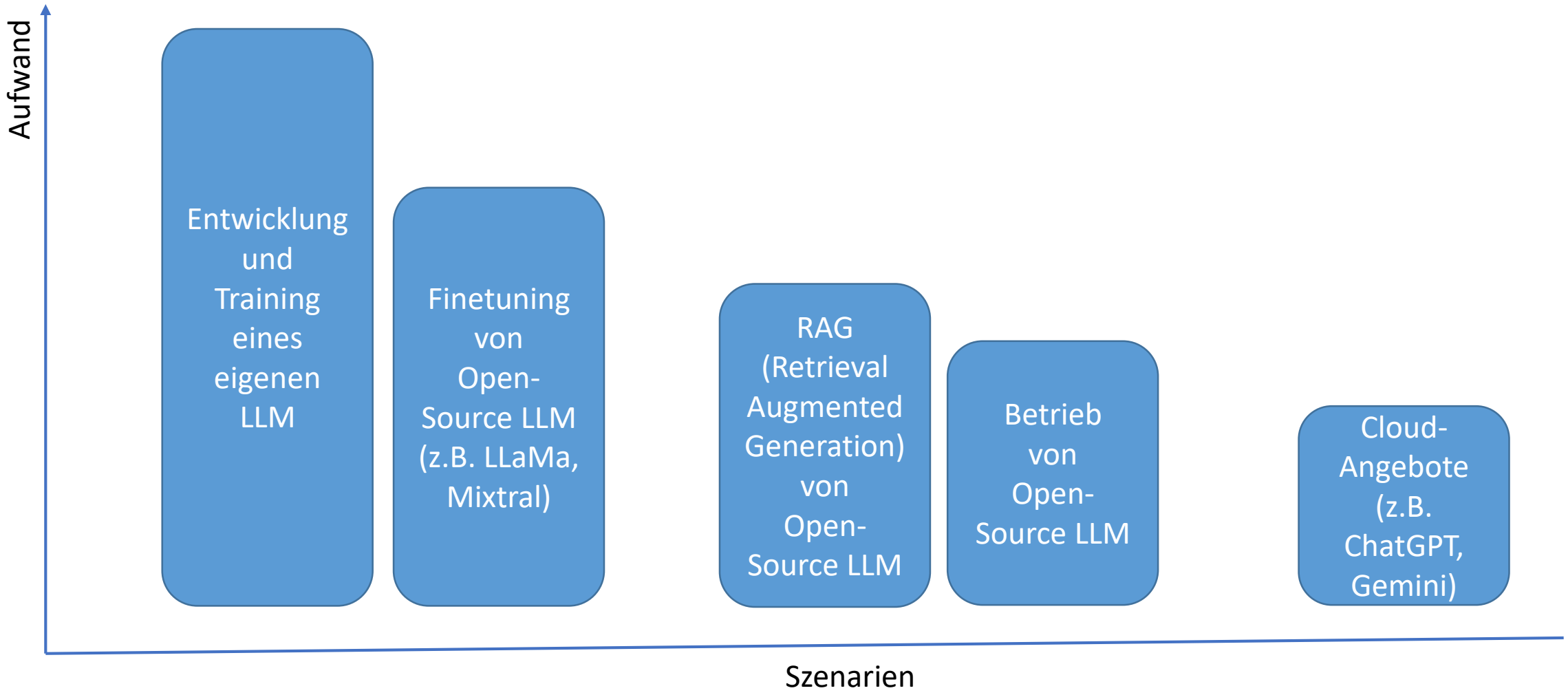
Was sind Large Language Models (LLM)

- Modelle die trainiert (Pretrained) sind natürliche Sprache (Prompts) zu verstehen und einen gewünschten Output zu generieren. Dabei wird ein Transformer (Deep Learning-Architektur) verwendet.
- Chat GPT – Generative Pretrained Transformer
- Text zu Text, Text zu Bild, Text zu Audio, Text zu Video, Audio zu Text,...
- Große Sprachmodelle mit hundert Milliarden bis zu einigen Billionen Parametern
- Sehr hohe Hardwareanforderungen (GPUs und Speicher) zum Training solcher Modelle
- Ausführung der Modelle (Inferenz) mit geringeren Ressourcen möglich
- Große Datenmengen zum Training eines Modells notwendig (Datengrundlage häufig das Internet)
- Entwicklung von Multimodalmodellen die mit jeder Art von Eingabe (Text, Bild, Video, Audio) beliebigen Output (Text, Bild, Audio, Video) erstellen können

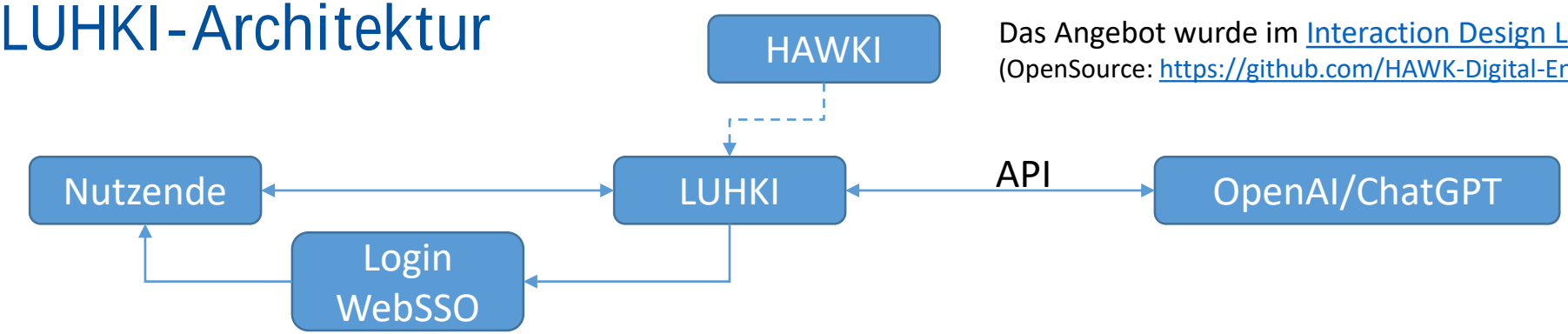
Risiken beim Einsatz von LLM

- Halluzinationen: es können falsche oder irreführende Informationen generiert werden.
- Es besteht die Gefahr von Urheberrechtsverletzungen, wenn durch das LLM urheberrechtlich geschützte Texte (ganz oder teilweise) generiert werden.
- Bias und Diskriminierung in Trainingsdaten kann zu Texten führen, die den Wertvorstellungen der LUH widersprechen (Alignment Problem of LLM).
- Jailbreaking von LLMs: Nutzende versuchen die Sicherheits- und Filterfunktionen des LLM durch Anfragetechniken zu umgehen oder zu manipulieren. Das Modell soll z.B. dazu gebracht werden missbräuchliche oder bekanntermaßen schädliche Inhalte zu generieren, wie etwa Anweisungen zu illegalen Aktivitäten oder Hassrede.
- Erstellung von DeepFakes (Audio, Bilder, Videos) z.B. zur Desinformation, Identitätsdiebstahl, Rufschädigung, Cyberangriffe.
- Viele neue Angriffsszenarien mit und über LLM.

Betriebs-/Einsatzmodelle von LLM



LUHKI-Architektur



Das Angebot wurde im Interaction Design Lab der HAWK entwickelt.
(OpenSource: https://github.com/HAWK-Digital-Environments/HAWKI)

- LUHKI ist eine im LUIS betriebene Webanwendung (OpenSource-Entwicklung HAWKI)
- Anmeldung erfolgt via LUH-WebSSO
- Anfragen werden von LUHKI (LUIS-Server) an OpenAI/ChatGPT derzeit Modell GPT-4o (Release Mai 2024) via API an ChatGPT geschickt und die Rückantwort dargestellt
- OpenAI sieht nur Anfragen von LUHKI und nicht von welchen Nutzenden die Anfrage gestellt wurde
- Keine Chat-Historie
- Nur Textgenerierung
- Vordefinierte Views mit Prompt-Artefakten
- Zentrale Abwicklung der Kosten über das LUIS, für Nutzende und Einrichtung entstehen keine Kosten

Nutzungsbedingungen zum Umgang mit LUHKI

- Müssen bei erstem Login bestätigt werden
- Hinweis, dass die OpenAI API verwendet wird
- Was ist verboten:
  - Eingabe personenbezogener Daten über sich selbst oder über andere.
  - Nutzung der Dienste für illegale, schädliche oder missbräuchliche Aktivitäten.
  - Verletzung, Missbrauch oder Verstoß gegen die Rechte anderer.
  - Modifikation, Kopie, Vermietung, Verkauf oder Verteilung unserer Dienste.
  - Automatisches oder programmgesteuertes Extrahieren von Daten oder Output.
  - Behauptung, dass der Output von Menschen erstellt wurde, wenn dies nicht der Fall ist.
  - Beeinträchtigung oder Störung der Dienste oder Umgehung von Schutzmaßnahmen.
  - Verwendung von Output zur Entwicklung konkurrierender Modelle.

Was zu beachten ist: Sie sind verantwortlich für den von Ihnen bereitgestellten Input und den daraus resultierenden Output. Sie müssen sicherstellen, dass Ihr Input keine Rechte verletzt und dass Sie über alle notwendigen Rechte, Lizenzen und Genehmigungen für die Bereitstellung des Inputs verfügen.

Qualität der Ergebnisse und Umgang mit Eingaben: Die Nutzung des Dienstes kann zu ungenauem oder fehlerhaftem Output führen. Es ist wichtig, dass Sie den Output kritisch prüfen und nicht unreflektiert verwenden.

Ihre Eingaben werden nicht von LUHKI, aber ohne Personenbezug, von OpenAI für 30 Tage gespeichert, um einen eventuellen Missbrauch festzustellen. Nach 30 Tagen werden die Daten gelöscht. Ihre Eingaben werden nicht zur Weiterentwicklung des Dienstes verwendet.

Spezifische Bestimmungen

Für Studierende:

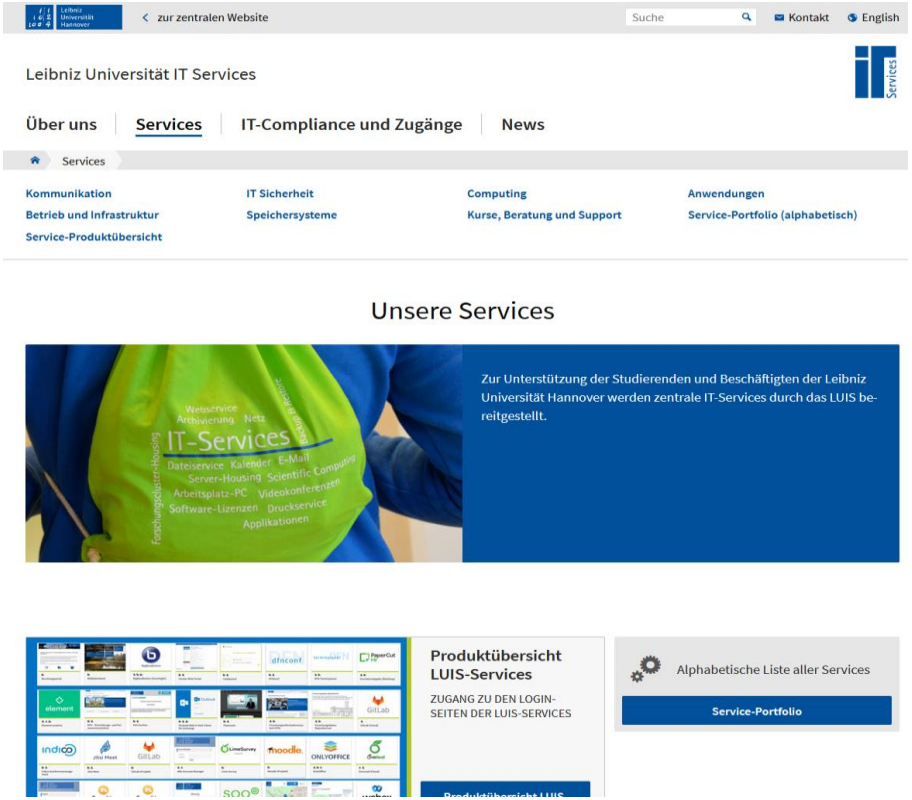
- Verwenden Sie LUHKI zur Unterstützung Ihres Lernprozesses, aber verlassen Sie sich nicht auf die generierten Antworten (Stichwort Halluzination).
- Teilen Sie keine persönlichen Daten oder Informationen über LUHKI.
- Sie übernehmen die Autorenschaft für jeglichen Output. Damit bürgen Sie für die Qualität der Antwort und übernehmen die Verantwortung für den Inhalt. Die Nutzung von generativer KI und die Art des Beitrags ist gegenüber Kommiliton*innen und Lehrenden und in sämtlichen darauf aufbauenden Medienprodukten transparent zu machen.
- Jegliche Nutzung für spezifische Veranstaltungen oder Studien-/Prüfungsleistungen ist mit den verantwortlichen Lehrenden vorab abzuklären.

Für Mitarbeitende/Lehrende:

- Geben Sie keine Inhalte ein, die Geheimhaltungsverträgen oder entsprechende Vertragsklauseln unterliegen, oder die ausschließlich für interne Zwecke gedacht sind. Achten Sie außerdem darauf, dass bei der Eingabe keine personenbezogenen Daten enthalten sind.
- Es dürfen nur Inhalte zur Verarbeitung in LUHKI eingegeben werden, für die Sie selbst alleinige Urheber*in sind oder explizit die urheberrechtliche Erlaubnis zur Verarbeitung innerhalb einer generativen KI haben.
- Sie dürfen in LUHKI keine Studien-, Prüfungs- und sonstige Leistungen der Studierenden verarbeiten.
- Wenn Sie LUHKI als ergänzendes Werkzeug zur Vorbereitung von Lehrmaterialien nutzen, stellen Sie sicher, dass alle Inhalte auf ihre Richtigkeit, Vollständigkeit und Relevanz überprüft werden.

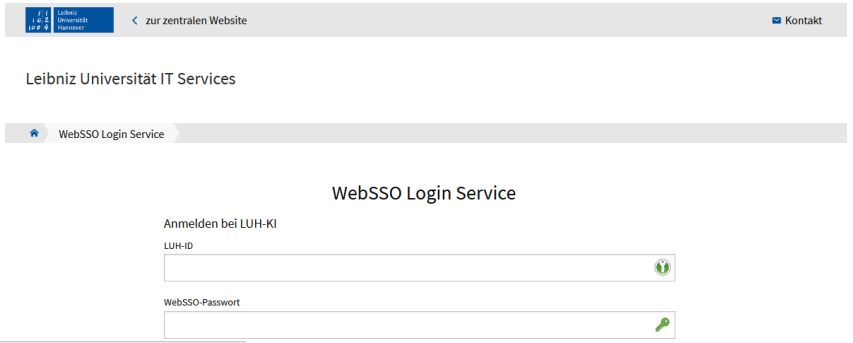
https://luhki.uni-hannover.de

https://www.luis.uni-hannover.de/de/services



https://go.lu-h.de/portal

WebSSO



Leibniz Universität Hannover

Sie sind dabei auf diesen Dienst zuzugreifen:
LUH-KI von Leibniz Universität Hannover

Beschreibung dieses Dienstes:
LUH-KI ist eine didaktische Schnittstelle für Universitäten basierend auf der OpenAI-API.

An den Dienst zu übermittelnde Informationen	
PrincipalName	[redacted]@uni-hannover.de
Name	**Thomas Rupp**
Statusgruppe(n)	**member@uni-hannover.de** **staff@uni-hannover.de** **employee@uni-hannover.de**
User-ID	[redacted]
Organisation	**Leibniz Universität Hannover**
Statusgruppe(n)	**member** **staff** **employee**
eduPersonEntitlement	**Zugang zu Informationsbibliotheken (siehe Definition)**
UniqueId	[redacted]@uni-hannover.de
Heimorganisation	**uni-hannover.de**
Typ der Heimorganisation (international)	**EU-Bildungseinrichtung**

Die oben aufgeführten Informationen werden an den Dienst weitergegeben, falls Sie fortfahren. Sind Sie einverstanden, dass diese Informationen bei jedem Zugriff auf diesen Dienst an ihn weitergegeben werden?

Wählen Sie die Dauer, für die Ihre Entscheidung zur Informationsweitergabe gültig sein soll:

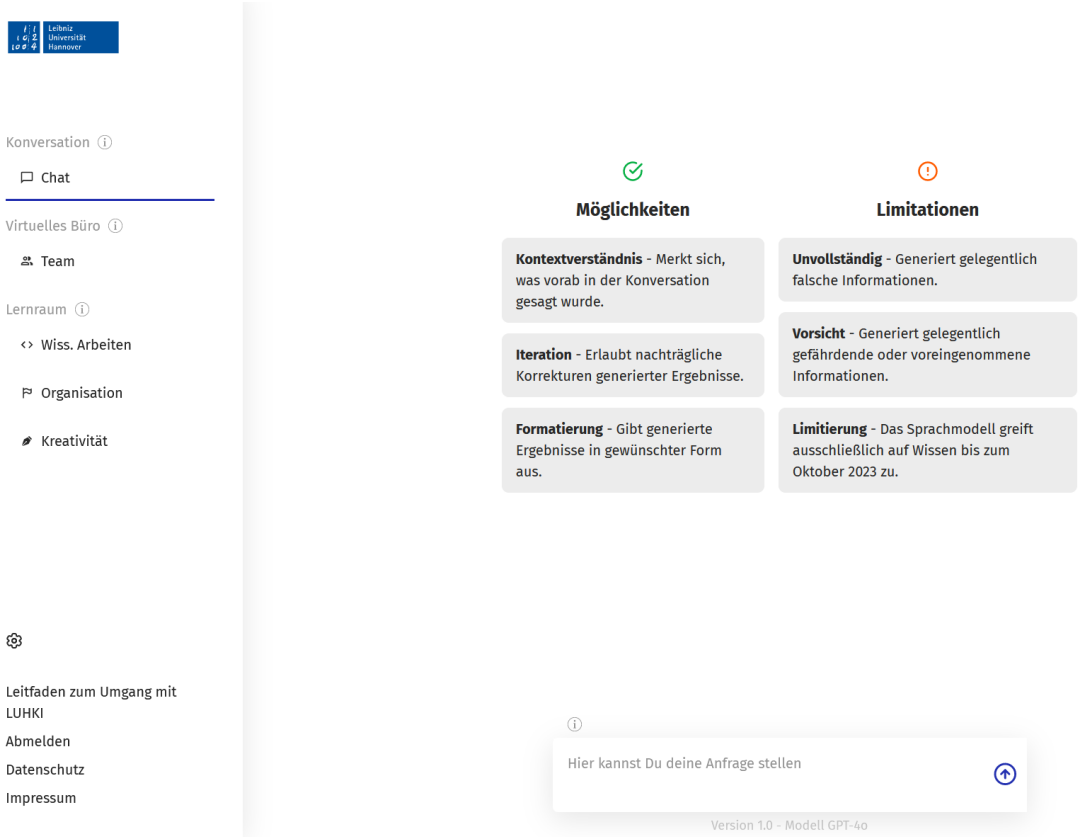
- ○ Bei nächster Anmeldung erneut fragen.
  - • Ich bin einverstanden, meine Informationen dieses Mal zu senden.
- ◉ Erneut fragen, wenn sich die Informationen ändern, welche diesem Dienst weitergegeben werden.
  - • Ich bin einverstanden, dass dieselben Informationen in Zukunft automatisch an diesen Dienst weitergegeben werden.
- ○ Nicht mehr fragen
  - • Ich bin einverstanden, dass **alle** meine Informationen an **jeden** Dienst weitergegeben werden.

Diese Einstellung kann jederzeit mit der Checkbox auf der Anmeldeseite widerrufen werden.

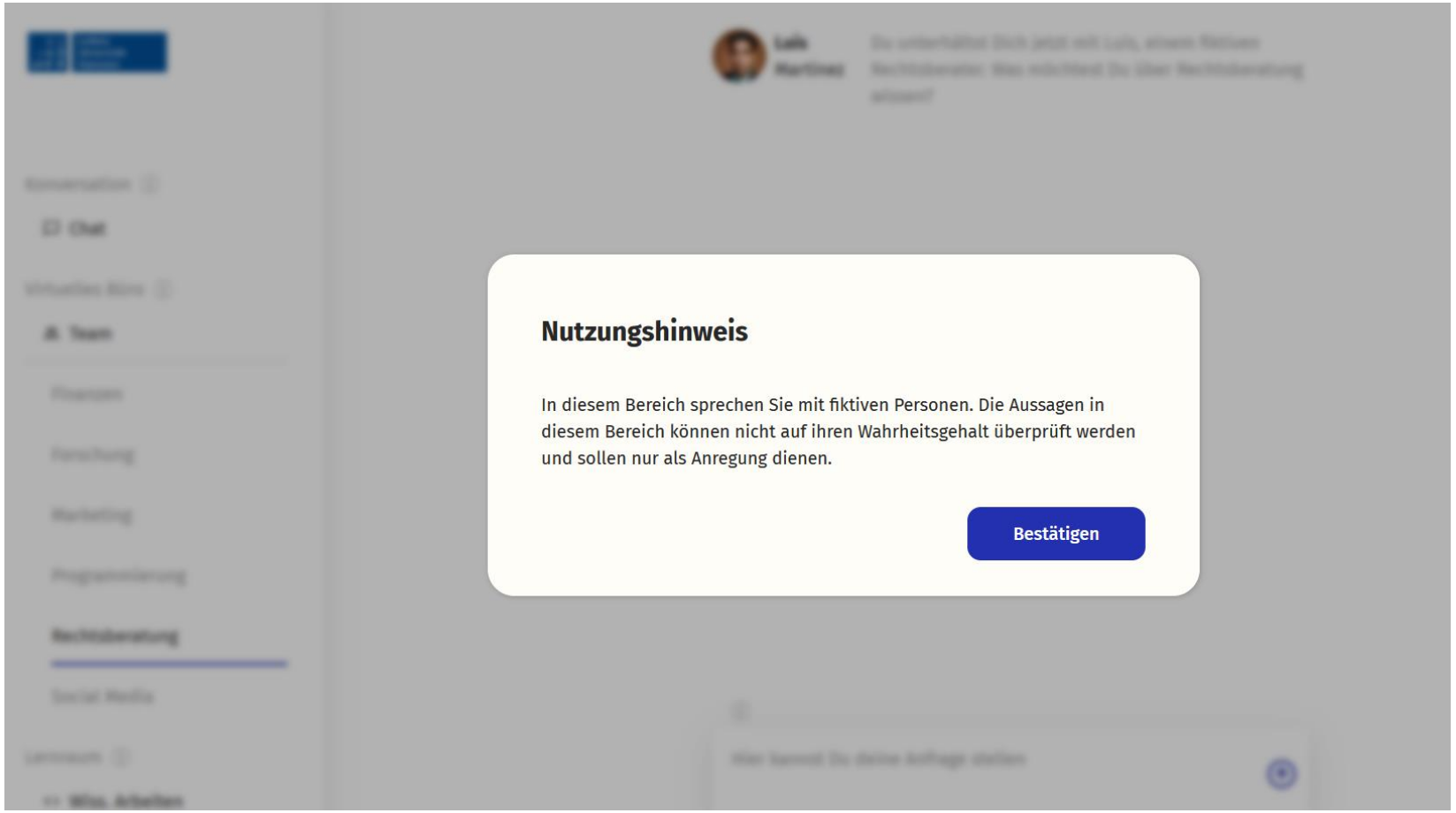
Ablehnen Akzeptieren

LUHKI


Regelungen für die Nutzung von LUHKI
Diese Nutzungsbedingungen regeln den Umgang mit LUHKI, einem Portal welches die Nutzung eines ChatGPT-Modells von OpenAI ermöglicht. Diese Regelungen sollen allen Hochschulangehörigen - Studierenden, Lehrenden und Mitarbeitenden - klare Richtlinien aufzeigen, wie an der LUH mit dieser Technologie verantwortungsbewusst umzugehen ist.
Diese Regelungen schließen sich an die von der Vizepräsidentin für Bildung formulierte Position an, „[...] dass ChatGPT besondere Optionen und Potenziale auf dem Weg zu einer innovativen Lernkultur und neu gestalteten Prüfungsformaten zu einer kompetenzorientierten Prüfungskultur bieten kann." Über die Webseite zu KI-Tools in Studium und Lehre stehen Handreichungen zur Nutzung bereit.
Bitte beachten Sie, dass diese Regelungen zur Bereitstellung von LUHKI die Nutzungsbedingungen von OpenAI ergänzen. Es liegt in der Verantwortung der Nutzerinnen und Nutzer, diese Regelungen und die o.g. Nutzungsbedingungen einzuhalten.
Wichtig:
Sie sind verantwortlich für den von Ihnen bereitgestellten Input und den


Konversation
Chat
Virtuelles Büro
Team
Lernraum
Wiss. Arbeiten
Organisation
Kreativität
Leitfaden zum Umgang mit LUHKI
Abmelden
Datenschutz
Impressum
Möglichkeiten
Kontextverständnis - Merkt sich, was vorab in der Konversation gesagt wurde.
Iteration - Erlaubt nachträgliche Korrekturen generierter Ergebnisse.
Formatierung - Gibt generierte Ergebnisse in gewünschter Form aus.
Limitationen
Unvollständig - Generiert gelegentlich falsche Informationen.
Vorsicht - Generiert gelegentlich gefährdende oder voreingenommene Informationen.
Limitierung - Das Sprachmodell greift ausschließlich auf Wissen bis zum Oktober 2023 zu.
Hier kannst Du deine Anfrage stellen
Version 1.0 - Modell GPT-4o

Nutzungshinweis



Deckt LUHKI alle Anforderungen ab?

- Nein, es gibt viele verschiedene Einsatzszenarien und KI-Use-Cases in Forschung, Lehre, Weiterbildung und Verwaltung.
- Unterschiedliche Lösungsansätze sind für unterschiedliche Use-Cases geeignet.
- LUHKI stellt einen einfachen Zugang zu einem LLM dar und kann ohne zusätzliche Registrierung genutzt werden.
- Datensparsame und –schutzkonforme Nutzungsmöglichkeit.