Universität Bremen

Handreichung

zur Nutzung von Chat-AI in der Academic Cloud der GWDG an der Universität Bremen

Stand: August 2025

Präambel

Die Universität Bremen bietet ab sofort einen sicheren Zugang zu generativen KI-Diensten (GenKI) über die Academic Cloud der GWDG. Nach einem einjährigen Testlauf steht dieser Dienst nun universitätsweit für alle Angehörigen zur Verfügung. Um sicherzustellen, dass Sie diese Ressourcen bestmöglich nutzen können, wurde nachfolgende Handreichung erstellt, welche die wichtigsten Informationen und Richtlinien für die Nutzung der GenKI-Dienste enthält. Bitte lesen Sie diese sorgfältig durch, sie bildet die Voraussetzungen für die gestattete Nutzung der Dienste.

Universität Bremen

Grundlagen

Die Universität Bremen ermöglicht über die Academic Cloud der GWDG (Gesellschaft für wissenschaftliche Datenverarbeitung mbH), einer gemeinsamen Einrichtung der Georg-August-Universität Göttingen und der Max-Planck-Gesellschaft (www.gwdg.de), einen datenschutzkonformen Zugang zu verschiedenen Modellen generativer KI (genKI). Diese genKI-Services heißen ChatAI. Die Nutzung ist freiwillig. Der Zugriff erfolgt mit den Anmeldedaten des Accounts an der Universität Bremen über ein Webinterface („föderierte Anmeldung“). Darüber können verschiedene OpenSource Modelle, die selbst gehostet sind (intern), und auch kommerzielle Modelle (extern gehostet), wie ChatGPT von OpenAI, genutzt werden. Die Vorteile sind:

- Die GWDG verarbeitet alle Daten gemäß der DSGVO
- Es wurde ein Vertrag zum Schutz der Nutzer:innendaten mit der GWDG abgeschlossen. Für die Anmeldung werden von der GWDG nur die Daten zur Prüfung der Authentifizierung und Autorisierung verarbeitet – dies ist vertraglich abgesichert
- Auch bei extern gehosteten Tools ist keine Weitergabe von personenbezogenen Daten der Nutzer:innen von der GWDG an die externen Dienstleister erforderlich (Hinweis: Inhalte der Eingaben (Prompts) müssen aber ungefiltert weitergegeben werden)
- Die eingegebenen Daten werden nicht zum Training der KI-Modelle genutzt
- Die Eingaben werden nicht auf den Servern der GWDG gespeichert, sondern nur lokal im genutzten Browser. Beim externen Modell (ChatGPT) behält sich Microsoft aber vor die Daten bis zu 30 Tage zu speichern, um Missbrauch vorzubeugen.

https://academiccloud.de/services/chatai/

Die sichere Bereitstellung der KI-basierten Systeme durch die Universität Bremen über die GWDG entbindet nicht von der **eigenen Verantwortung** für die Eingabe von Inhalten, die kritische Überprüfung von Ergebnissen und ihrer Verwendung.

Die Nutzung **externer generativer KI-basierter Systeme (außerhalb von Chat-AI der GWDG) wird nicht empfohlen**, eine Ausnahme können Forschungsprojekte bilden. Die Freie Hansestadt Bremen bereitet derzeit die Einführung eines verwaltungs-spezifischen KI-basierten Systems vor (LLMoin), das auch den Verwaltungsmitarbeiter:innen der Universität Bremen zur Verfügung gestellt werden soll.

Diese Handreichung wird laufend aktualisiert, um den sich verändernden technischen, rechtlichen und ethischen Anforderungen Rechnung zu tragen.

Universität Bremen

Handlungsempfehlungen

- **Reflektierter Einsatz**

  Nutzen Sie generative KI stets überlegt: Was sind ihre Ziele und welche Ergebnisse erwarten Sie? Kennen Sie die Funktionsweise, die Stärken und Schwächen des genutzten Modells? Wissen Sie was Sie eingeben und wie Sie Ausgaben nutzen dürfen?

  Prüfen und verifizieren Sie die Ausgaben immer mit Primär- und Fachquellen oder Rücksprache mit Expert:innen.

- **Kritisches Hinterfragen**

  Geben Sie keine Texte oder Ergebnisse ungeprüft weiter, übernehmen Sie Verantwortung für die Weiterverwendung und bewerten Sie die Ausgabe sorgfältig. Sind die Informationen plausibel, richtig und ethisch vertretbar? Liegen möglicherweise Verzerrungen und Diskriminierungen vor?

- **Datenschutz**

  Geben Sie keine personenbezogenen Daten in die genKI-Systeme ein (Ausnahme: vorliegende Rechtsgrundlage oder Einwilligung). Prüfen Sie, ob Ausgaben personenbezogene Daten beinhalten, die nicht weitergegeben werden dürfen.

- **Informationssicherheit**

  Geben sie keine vertraulichen Daten in KI-Systeme ein. Beachten Sie die Klassifizierung und Sensibilität Ihrer Informationen.

- **Urheberrecht**

  Achten Sie darauf, keine urheberrechtlich geschützten Inhalte einzugeben oder zu veröffentlichen. Prüfen Sie die Ausgaben, ob Verletzungen des Urheberrechts vorliegen und wer Rechte an KI-generierten Inhalten hat. Im Zweifelsfalle veröffentlichen sie keine KI-generierten Inhalte.

- **Ethische Aspekte**

  Hinterfragen Sie Ergebnisse auf mögliche Verzerrungen oder Fehldarstellungen; Kennzeichnen Sie Inhalte, die mit KI generiert wurden und dokumentieren Sie ggfs. den Einsatz nachvollziehbar.

- **Verbotene Anwendungsfälle**

  Generative KI darf nicht eingesetzt werden zur Erstellung von Profilen, zur automatisierten Benotung, Erstellung von Gutachten, Plagiaten oder irreführender/intransparenter Informationen

- **Nutzen Sie zur Unterstützung diese Checkliste zum rechtskonformen Umgang mit generativen KI-Diensten**

  Checkliste genKI

Universität Bremen

Beratungs- und Unterstützungsangebote

- zentrale Anlaufstelle für Anfragen und zum Projekt **GenKI@UHB**,
  https://www.uni-bremen.de/digitale-transformation/projekte/genkiuhb
  Email an: genki@uni-bremen.de

- zu **genKI in Studium und Lehre**
  Referat 13
  Link zu den Empfehlungen zur Nutzung für Lehre und Studium
  ZMML
  Link zu den Informationen des ZMML zur Nutzung künstlicher Intelligenz

- **Datenschutz und Informationssicherheit**
  Link zum Informations- und Serviceportal von DSB und ISB

Kernbegriffe generativer KI

Generative Künstliche Intelligenz (KI)

KI-Anwendungen, die auf Basis trainierter Daten aus einer Eingabe (Prompt) automatisch Inhalte wie Texte, Bilder, Töne, Videos oder Programmcode erzeugen.

Large Language Models (LLMs)

Textgenerierende Systeme (z. B. ChatGPT, Llama, Gemini, Claude), die mit großen Datenmengen trainiert werden. Sie verstehen Inhalte nicht inhaltlich, sondern berechnen die statistisch wahrscheinlichste nächste Zeichen- oder Wortfolge. Fehlerhafte, erfundene oder inhaltlich falsche Ausgaben („Halluzinationen“) sind möglich.

Halluzinationen

Die KI gibt überzeugend formulierte, aber inhaltlich falsche Informationen aus. Inhalt und Argumentation wirken stimmig, sind jedoch vom KI-System frei erfunden.

Bias / Verzerrungen

Vorurteile oder Fehldarstellungen in den Trainingsdaten oder Modellen können sich auf die Ausgaben der KI übertragen und zu Diskriminierung (z. B. Ungleichbehandlung von Personengruppen) führen.

Verabschiedet vom Rektorat am 12.08.2025