

## **Leitlinie zur Nutzung von HAWKI an der Universität Siegen**

### **Präambel**

HAWKI ist ein KI-gestütztes Tool, das von der Hochschule für angewandte Wissenschaft und Kunst (HAWK) Hildesheim/Holzminde/Göttingen entwickelt wurde und Sprachmodelle von OpenAI über Microsoft Azure zur Verfügung stellt.

Der Dienst dient der Unterstützung menschlicher Entscheidungsprozesse in den Bereichen Studium, Lehre, Forschung und Verwaltung im Rahmen der gesetzlichen Aufgaben der Universität Siegen; die Verarbeitung erfolgt zweckgebunden (Art. 5 Abs. 1 lit b DSGVO) und ersetzt keine fachliche oder prüfungsrelevante Bewertung.

Zugriff auf die Weboberfläche und Login erfolgen über die ZIMT-Infrastruktur, auf der auch die Verbindungsdaten gespeichert werden. KI-Anfragen werden ohne Zuordnung der Nutzererkennung an externe Dienste weitergeleitet und die Antworten in der Web-Oberfläche präsentiert. Der bestehende Auftragsverarbeitungsvertrag mit Microsoft Azure gewährleistet eine datenschutzkonforme Verarbeitung und schließt insbesondere eine Nutzung der Daten zu Trainingszwecken aus. Er ersetzt jedoch nicht die Prüfung der Zulässigkeit im Einzelfall.

Die KI-Anfragen und -Antworten werden verschlüsselt auf der ZIMT-Infrastruktur gespeichert; die Schlüssel verbleiben ausschließlich auf den Clients der Nutzer. Alle hochgeladenen Daten werden spätestens nach sechs Monaten systemseitig gelöscht, sofern Sie nicht vorher manuell gelöscht wurden. Die Plattform verfolgt damit das Prinzip der Datenminimierung gemäß DSGVO.

Die Bereitstellung der KI-Anwendung sowie die Interaktion der Nutzenden wird durch Art. 6 Abs. 1 lit. e DSGVO (Wahrnehmung öffentlicher Aufgaben in Lehre und Forschung) abgedeckt. Das Monitoring der Systemnutzung (IP-Adresse, Log-Daten etc.) sowie die Missbrauchserkennung erfolgen zur Sicherstellung des sicheren Betriebs (Art. 6 Abs. 1 lit. e DSGVO i.V.m. § 3DSG NRW; ergänzend Art. 6 Abs. 1 lit. c DSGVO i.V.m. Art. 32 DSGVO).

Die Einführung neuer Modelle oder Funktionserweiterungen erfolgt nur nach datenschutzrechtlicher und informationssicherheitsrechtlicher Prüfung.

### **1. Grundsätze der Nutzung**

Die Nutzung von HAWKI ist grundsätzlich nur nach vorheriger Absolvierung des von der Universität Siegen bereitgestellten Moodle-Kurses zur Einführung in die Nutzung von KI-Systemen zulässig.

Der Moodle-Kurs vermittelt die maßgeblichen rechtlichen und organisatorischen Rahmenbedingungen, insbesondere zu Datenschutz, Informationssicherheit und Urheberrecht, sowie den verantwortungsvollen Umgang mit KI-Anwendungen.

Ohne vorherige Teilnahme ist eine Nutzung von HAWKI nicht zulässig.

#### **Verboten ist bei zulässiger Nutzung jedoch insbesondere:**

- Nutzung für **illegale, schädliche oder missbräuchliche Zwecke**
- Verletzung von Urheber-, Persönlichkeits- oder sonstigen Rechten Dritter
- Automatisiertes Extrahieren von Daten oder Outputs
- Darstellung von KI-generiertem Output als menschlich generiertem Output.

## 2. Informationssicherheit

Unter Berücksichtigung der „Richtlinie Klassifizierung von Informationen“ vom 20. April 2022 dürfen grundsätzlich *nur öffentliche und nicht-öffentliche Informationen* verarbeitet werden.

Nicht verarbeitet werden dürfen insbesondere:

- vertrauliche oder streng vertrauliche Informationen
- Finanzdaten, strategische Unterlagen oder sicherheitsrelevante Informationen
- Informationen zu Schwachstellen oder internen Sicherheitsmaßnahmen
- nicht veröffentlichte Forschungs- oder Projektdaten mit erhöhtem Schutzbedarf

Diese Vorgaben gelten **unabhängig von datenschutz- oder urheberrechtlichen Bewertungen**.

## 3. Datenschutz

### Eigenverantwortung

- Nutzende tragen die Verantwortung für **Input und Output**.
- Nutzende verpflichten sich, Inhalte kritisch zu prüfen – KI kann fehlerhafte oder ungenaue Antworten liefern.
- KI-Ergebnisse dürfen **nicht als alleinige Entscheidungsgrundlage** verwendet werden.

### Umgang mit personenbezogenen Daten

- Personenbezogene Daten dürfen nur verarbeitet werden, sofern hierfür eine datenschutzrechtliche Grundlage besteht und die Verarbeitung erforderlich ist. Es ist stets zu prüfen, ob eine anonymisierte oder pseudonymisierte Eingabe möglich ist.<sup>1</sup>
- Keine Eingabe von besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO.<sup>2</sup>
- Keine Eingabe vertraulicher Informationen (z.B. nicht-öffentliche Gremienunterlagen, Vertragsinhalte unter NDA, Prüfungsakten.)
- Nutzende müssen über alle notwendigen Rechte und Genehmigungen der durch sie eingegebenen Inhalte verfügen.
- Im Zweifel: keine Eingabe oder Rücksprache mit der Stabsstelle Informationssicherheit und Datenschutz.

### Datenspeicherung

- Microsoft Azure OpenAI speichert Eingaben für Zwecke der Missbrauchserkennung für bis zu 30 Tage; danach werden sie dort gelöscht. Die Verarbeitung erfolgt grundsätzlich innerhalb der EU/des EWR entsprechend der gewählten Konfiguration und den vertraglichen Vereinbarungen. Maßgeblich sind die jeweils aktuellen Angaben des Anbieters sowie die konkret eingerichtete Systemumgebung.
- Die Daten werden nicht zur Modellverbesserung verwendet.
- Hochgeladene Dateien werden spätestens nach **6 Monaten** automatisch gelöscht.

---

<sup>1</sup> Pseudonym: eine Person ist mithilfe zusätzlicher Informationen identifizierbar.  
Anonym: Eine Person ist nicht mehr identifizierbar.

<sup>2</sup> Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

#### 4. Gruppenchat – Verhaltensregeln

Alle Beiträge sind für die Gruppenmitglieder sichtbar. Daher gilt:

- Respektvoller und höflicher Umgang
- Keine personenbezogenen Daten über Dritte, keine sensiblen Daten
- Keine persönlichen Angriffe oder diskriminierenden Inhalte
- Keine Falschinformationen
- Kein Spam

Missbrauch kann zum Ausschluss von HAWKI führen.

Gruppenchat-Inhalte werden gemäß dem Löschkonzept der Plattform gelöscht. Sie sind nicht für die dauerhafte Dokumentation bestimmt.

#### 5. Urheberrechtliche Zulässigkeit

Nutzende müssen sicherstellen, dass weder Input noch Output Rechte Dritter verletzt. Die Eingabe von Inhalten in HAWKI stellt regelmäßig eine urheberrechtlich relevante Nutzungshandlung dar (insbesondere Vervielfältigung), sodass hierfür eine rechtliche Grundlage erforderlich ist.

##### Zulässig sind:

- Selbst erstellte Inhalte: Texte, Dokumente oder sonstige Materialien, die von den Nutzenden selbst verfasst wurden und an denen keine Rechte Dritter bestehen.
- Gemeinfreie Werke, d.h. Werke, deren urheberrechtliche Schutzfrist abgelaufen ist (in der Regel 70 Jahre nach dem Tod des Urhebers), sowie Werke, die von vornherein keinem urheberrechtlichen Schutz unterliegen, d.h. Inhalte, denen es an einer eigenen schöpferischen Gestaltung fehlt, insbesondere reine Fakten, Daten oder einfache Standardformulierungen. Diese dürfen frei genutzt, bearbeitet und auch vollständig in HAWKI eingegeben werden.
- Amtliche Werke (§ 5 UrhG): Hierzu zählen insbesondere Gesetze, Verordnungen, amtliche Erlasse und Gerichtsentscheidungen. Diese sind urheberrechtlich nicht geschützt und dürfen daher uneingeschränkt verwendet werden.
- Inhalte mit entsprechenden Nutzungsrechten, d.h. Inhalte, für die eine ausdrückliche Nutzungserlaubnis vorliegt, z. B. durch Lizenz (z. B. Creative Commons, Open Access) oder vertragliche Regelungen. Die jeweiligen Lizenzbedingungen (z. B. Namensnennung, Bearbeitungsverbot) sind zu beachten.
- Gesetzlich erlaubte Nutzungen (z. B. §§ 51, 60a, 60c UrhG im jeweiligen Anwendungsbereich): Hierunter fallen insbesondere Zitate (§ 51 UrhG), sofern sie einen eigenen inhaltlichen Beitrag stützen und nur im erforderlichen Umfang verwendet werden. Die Nutzung nach § 60a UrhG ist auf konkrete Lehrveranstaltungen beschränkt und erlaubt nur die Nutzung von Teilen eines Werkes. Sie stellt keine allgemeine Grundlage für die Nutzung von Inhalten in KI-Systemen dar.

##### Nicht zulässig sind demgegenüber insbesondere:

- Urheberrechtsverletzende Inhalte: Alle Inhalte, die ohne erforderliche Nutzungsrechte oder gesetzliche Erlaubnis verwendet werden, insbesondere wenn sie aus geschützten Quellen (z. B. Bücher, Fachartikel, Berichte) übernommen wurden.
- Fremde Werke ohne Nutzungsrecht: Die Eingabe von Texten, Artikeln, Gutachten, Büchern oder sonstiger urheberrechtlich geschützter Dokumente in HAWKI ist unzulässig, wenn hierfür keine entsprechenden Rechte vorliegen. Dies gilt auch dann, wenn die Nutzung ausschließlich intern erfolgt.

- Dokumente unter Geheimhaltungsvereinbarung (NDA): Inhalte, die vertraglichen Geheimhaltungspflichten unterliegen, dürfen nicht in HAWKI eingegeben werden, da hierdurch sowohl urheberrechtliche als auch vertragliche Pflichten verletzt werden können.
- Inhalte mit Persönlichkeitsrechtsverletzungen: Texte oder Materialien, die personenbezogene Daten enthalten und deren Nutzung die Rechte betroffener Personen verletzen würde, insbesondere bei sensiblen oder vertraulichen Informationen.

**Hinweis:**

**Die bloße technische Möglichkeit, Inhalte in HAWKI einzugeben, begründet keine rechtliche Zulässigkeit. Auch eine ausschließlich interne Nutzung ersetzt nicht die erforderliche urheberrechtliche Erlaubnis.**

**Im Zweifel ist von einer Eingabe abzusehen oder eine rechtliche Klärung herbeizuführen.**

**Nutzende können nicht in jedem Fall Urheberschaft an generierten Texten beanspruchen.**

**Zweck:**

- Die Verarbeitung erfolgt zur Nutzung innerhalb der Universität Siegen; eine Weitergabe erfolgt ausschließlich an die vertraglich gebundenen Auftragsverarbeiter (Microsoft Azure) im Rahmen der Bereitstellung der Modelle.
- Umsetzung des Prinzips der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO)

## **6. Spezifische Regelungen für Hochschulgruppen**

### **Studierende**

- Nutzung zur Lernunterstützung sind erlaubt.
- Ergebnisse sind kritisch zu prüfen.
- Die Verantwortung für eingereichte Inhalte liegt beim Nutzenden.
- Die Nutzung von KI ist nach Maßgabe fakultäts- und ggf. Lehrveranstaltungsspezifischer Richtlinien oder Vorgaben für die jeweilige Lehrveranstaltung /Prüfung transparent zu machen.
- Studien- und Prüfungsleistungen sind grundsätzlich eigenständig, selbstständig und **ohne unzulässige Hilfsmittel** zu erbringen. Informieren Sie sich im Zweifel bei der oder dem jeweiligen Lehrenden, ob KI im Rahmen einer Studien- oder Prüfungsleistung verwendet werden darf.

### **Lehrende**

- **Erlaubt:** Rechtschreibprüfung, Feedback-Vorbereitung, Sprachvereinfachung, Bewertungsrasster, Übungsmaterialien
- **Nicht erlaubt:** eine automatisierte Korrektur oder Bewertung von Prüfungsleistungen ist hochschulintern derzeit untersagt, u.a. vor dem Hintergrund der hohen rechtlichen Anforderungen (u.a. EU-AI Act, Prüfungsrecht, Datenschutz), Uploads von vertraulichen oder geheimhaltungsgebundenen Dokumenten, z. B. Vertragsentwürfe und Verträge (Rahmenverträge, Forschungsverträge etc.), besondere wissenschaftliche Daten (Patentunterlagen vor ihrer Offenlegung)
- Fakultätsspezifische Richtlinien oder Vorgaben für die jeweilige Lehrveranstaltung /Prüfung sind transparent zu machen.

## **Mitarbeitende**

- Die Anwendung von KI-Tools in administrativen Tätigkeiten dient insbesondere dazu, diese effizienter und einfacher zu gestalten.
- Grundsätzlich ist die Unterstützung durch KI-Tools in der Verwaltung insbesondere für folgende Tätigkeiten sinnvoll: Recherche, Analyse und Zusammenfassung von Inhalten oder Generierung von Entwürfen (Texten, Tabellen, Präsentationen etc.).
- Jeder Mitarbeitende ist dazu angehalten,
  - die durch KI-Tools erzeugten Materialien kritisch zu hinterfragen und zu reflektieren, auf Korrektheit und Vollständigkeit in den jeweiligen Aussagen zu verifizieren und auf Plausibilität zu prüfen.
  - den Aufbau von eigener KI-Kompetenz im Rahmen der angebotenen Schulungen (intern Universität Siegen, extern (HüF etc.)) sicherzustellen.
  - keine Uploads von vertraulichen oder geheimhaltungsgebundenen Dokumenten vorzunehmen, z. B. Vertragsentwürfe und Verträge (Rahmenverträge, Forschungsverträge etc.), Finanzdaten (Budget etc.), Abschlussberichte (Revisionsberichte, Auditberichte etc.), Strategiepapiere vor Veröffentlichung

## **Schlusswort**

Dieser Leitfaden dient als Orientierungshilfe für den verantwortungsbewussten Umgang mit HAWKI. Die Verarbeitung ist im „Verzeichnis für Verarbeitungstätigkeiten“ mit dem Aktenzeichen 77/2025 VVT hinterlegt.

## **Kontakt bei Fragen:**

Technisch: [support@zimt.uni-siegen.de](mailto:support@zimt.uni-siegen.de)

Inhaltlich: [datenschutz@uni-siegen.de](mailto:datenschutz@uni-siegen.de)

Ungeachtet dieses Leitfadens gelten die Nutzungsbedingungen von Microsoft Azure OpenAI.

## Beispiele für Daten und ihren potentiellen Schutzbedarf für die Verarbeitung in HAWKI

Die Tabelle gilt für Eingaben (Chats/Prompts) sowie Uploads gleichermaßen

Art der Daten	Schutzbedarf	Dürfen die Daten in HAWKI verarbeitet werden
Daten, die aus öffentlichen, frei und offenkundig legal zugänglichen Quellen stammen (z.B. Literatur, Dokumente oder Downloads)	normal	ja
Inhalte aus öffentlichen Gremiensitzungen	normal	ja
Inhalte aus öffentlichen Veranstaltungen	normal	ja
Projektakten ohne vertrauliche Inhalte	normal	ja
Inhalte aus öffentlichen Lehrveranstaltungen	normal	ja
Wissenschaftliche Daten, die für Dritte nicht interpretierbar sind und für die keine Geheimhaltungsvereinbarungen bestehen	normal	ja
Informationen zu Lehrveranstaltungen (z.B. Listen mit Daten von Teilnehmenden)	normal	Nur wenn erforderlich und nach Möglichkeit pseudonymisiert
Ton-, Bild- und Videoaufnahmen sowie Aufzeichnungen von Videokonferenzen, die weder als vertraulich eingestuft werden noch <b>besondere personenbezogene Daten*</b> beinhalten	normal	ja
Ton-, Bild- und Videoaufnahmen sowie Aufzeichnungen von Videokonferenzen, die als vertraulich eingestuft werden und/oder <b>besondere Kategorien personenbezogener Daten*</b> beinhalten, wie bspw. <ul style="list-style-type: none"> <li>• Vorstellungsgespräche</li> <li>• Vertrauliche Inhalte aus Gremiensitzungen</li> </ul>	hoch	Nein
Prüfungsdaten wie <ul style="list-style-type: none"> <li>• Notenlisten</li> <li>• Prüfungsprotokolle</li> <li>• Gutachten</li> </ul>	hoch	Nein
Bewerbungsgespräche	hoch	Nein
Wissenschaftliche Daten, die <ul style="list-style-type: none"> <li>• vertrauliche Daten wie z.B. Daten die Geheimhaltungsvereinbarungen, Vertragsstrafen etc. Unterliegen</li> <li>• oder <b>besondere Kategorien personenbezogener Daten*</b> (s.u.) beinhalten.</li> </ul>	hoch bis sehr hoch	Nein
<b>Besondere Kategorien personenbezogener Daten*</b> , z.B. Daten zu <ul style="list-style-type: none"> <li>• besonderen sachlichen Verhältnisse von Beschäftigten</li> <li>• Gesundheit</li> <li>• Sozialen Verhältnissen</li> <li>• ethnischer Herkunft</li> <li>• politischen Meinungen</li> <li>• Gewerkschaftszugehörigkeit</li> <li>• Sexueller Orientierung</li> <li>• Biometrische Daten</li> </ul>	hoch bis sehr hoch	Nein