



# Richtlinie zur Nutzung von Künstlicher Intelligenz (KI) und zum Einsatz von KI-Systemen an der Universität Stuttgart

Das Rektorat der Universität Stuttgart hat in seiner Sitzung am 30.09.2025 die nachstehende Richtlinie zur Nutzung Künstlicher Intelligenz (KI) und zum Einsatz von KI-Systemen an der Universität Stuttgart beschlossen.

---

## Präambel

Die Nutzung Künstlicher Intelligenz (KI) eröffnet der Universität Stuttgart neue Möglichkeiten zur Effizienzsteigerung, Qualitätsverbesserung und Innovationsförderung. Zugleich erfordert der verantwortungsvolle Umgang mit KI-Systemen gewisse Vorgaben rechtlicher, ethischer und organisatorischer Art.

Die vorliegende Richtlinie zur KI basiert auf dem Selbstverständnis einer modernen Universität, die technologische Chancen gezielt nutzt, dabei den Schutz von Personen und deren Persönlichkeitsrechten sowie die Integrität der Organisation wahrt und ihren Umgang mit neuen Technologien – hier mit KI-Systemen – fortlaufend reflektiert.

Angesichts der rasanten technischen Entwicklungen im Bereich der Künstlichen Intelligenz sowie sich wandelnder rechtlicher und gesellschaftlicher Rahmenbedingungen, wird diese Richtlinie regelmäßig überprüft und fortgeschrieben. Ihr Zweck ist es, allen Beschäftigten einen verlässlichen Rahmen zu geben, in dem sie KI-Systeme sicher, verantwortungsvoll, ethisch vertretbar, transparent und rechtskonform an der Universität Stuttgart einsetzen können.

**Anwendungsbereich:** Diese Richtlinie gilt für alle Beschäftigten der Universität Stuttgart, die KI-Systeme im Rahmen ihrer dienstlichen Tätigkeiten außerhalb von Forschung einsetzen, etwa für Projektmanagement, Drittmittelverwaltung, Prüfungsorganisation oder Gremienarbeit. Sie wird durch folgende Dokumente ergänzt:

- Vertraulichkeitsklassifikation für Informationen im Kontext des Einsatzes von KI-Systemen
- Whitelist für die unterschiedlichen Typen von KI-Systemen

Die letztinstanzliche Entscheidung darüber, ob und vor allem welche KI-Systeme für dienstliche Zwecke außerhalb der Forschung eingesetzt werden dürfen, obliegt der Universitätsleitung. Für die in der Wissenschaft tätigen Beschäftigten gilt diese Richtlinie auch, zuzüglich weiterer Regelungen.

## 1. Definition von KI-Systemen und Relevanz der Informationsklassifikation

KI-Systeme im Sinne dieser Richtlinie sind softwarebasierte Anwendungen, die daten- oder regelbasierte Verfahren nutzen, um eigenständig Informationen zu verarbeiten, zu erzeugen und menschliche Entscheidungs- oder Problemlösungsprozesse zu unterstützen.

Dazu zählen insbesondere Systeme, mit denen Nutzerinnen und Nutzer in Dialogform z.B. über Texteingaben interagieren und die in Echtzeit oder asynchron eine Ausgabe erzeugen. Beispiele hierfür sind Chatbots (z. B. ChatGPT), Schreibassistenten (z. B. Copilot, DeepL Write), Bild- oder Analysegeneratoren (z. B. Midjourney, KI-gestützte Dashboards) sowie Business-Intelligence-Systeme, die Daten automatisiert klassifizieren (z.B. Power BI).

Bereits die Eingabe von Informationen in solche Systeme – in Form strukturierter Daten (z.B. Tabellen, Datenbanken, Excel-Dateien) oder unstrukturierter Daten (z.B. Texte, Bilder, Audio- oder Videodateien) – ist datenschutz- und sicherheitsrelevant. Denn ein KI-System kann diese Informationen nicht nur speichern oder weiterverarbeiten, es kann sie fallweise auch zur eigenen Weiterentwicklung nutzen (z. B. zum Training der nächsten Version des Sprachmodells). **Deshalb ist bei jeder Nutzung eines KI-Systems entscheidend, welche Informationen dort eingegeben werden** - nicht nur, welches Ergebnis das KI-System liefert.

Die vorliegende KI-Richtlinie basiert auf einer Vertraulichkeitsklassifikation für Informationen im Kontext des Einsatzes von KI-Systemen. Diese steht als gesondertes Dokument zur Verfügung.

Vor der Eingabe von Informationen in ein KI-System ist von den Nutzenden sorgfältig zu prüfen, welcher Vertraulichkeitsklasse die betreffende Information angehört.

- Liegt bereits eine Einstufung in eine dieser Vertraulichkeitsklassen vor, ist diese verbindlich zu beachten.
- Liegt keine Einstufung vor, sind die Nutzenden verpflichtet, die Vertraulichkeitsklasse in eigenem pflichtgemäßen Ermessen festzulegen oder von einer übergeordneten Instanz (Vorgesetzte, Rektorat, ...) festlegen zu lassen.

## 2. Grundsätze der KI-Nutzung

- KI-Systeme **sollen als Hilfsmittel verwendet werden**. Sie können und dürfen menschliches Urteilsvermögen und die Entscheidungsverantwortung des Einzelnen nicht ersetzen.
- **Der Schutz von Persönlichkeitsrechten und von vertraulichen Informationen hat oberste Priorität**. Vor der dienstlichen Nutzung eines KI-Systems prüfen die Nutzenden, welche Informationen gemäß dieser Richtlinie in welches System eingegeben werden dürfen. Für die Verarbeitung personenbezogener Daten braucht es eine Rechtsgrundlage.
- **Der Einsatz von KI-Systemen ist so transparent wie möglich zu gestalten**. Das bedeutet, dass Funktionsweise, Entscheidungsgrundlagen und Verantwortlichkeiten für alle betroffenen Personen nachvollziehbar sind.
- **Die Verantwortung für die Qualität und die Richtigkeit von Inhalten**, in die Ergebnisse aus KI-Systemen einfließen, **liegt bei den Nutzenden**. Diesen obliegt es, KI-generierte Inhalte vor der Verwendung sorgfältig zu prüfen.

Die Universität stellt ihren Beschäftigten die erforderlichen Informationen für eine sichere, verantwortungsvolle, ethisch vertretbare und rechtskonforme Nutzung von KI-Systemen einfach zugänglich bereit. Sie bietet als unterstützende Maßnahmen Schulungen an und benennt eine zentrale Ansprechperson für Nachfragen hinsichtlich einer KI-Nutzung.

---

## 3. Typisierung von KI-Systemen zur dienstlichen Nutzung

Diese Richtlinie unterscheidet folgende Typen von KI-Systemen und schränkt zulässige Eingaben entsprechend ein:

- **Universitätseigene KI-Systeme (Typ 1):**  
KI-Systeme, die vollständig von und innerhalb der Universität Stuttgart betrieben werden und bei denen ausgeschlossen ist, dass Daten in externe Systeme abfließen. Diese KI-Systeme verarbeiten Daten ausschließlich innerhalb universitärer Infrastruktur und dürfen nach Freigabe des Systems durch das Rektorat für die Eingabe von Informationen aller Vertraulichkeitsklassen einschließlich streng vertraulicher Informationen (C4) verwendet werden. Beschäftigte dürfen Informationen der Vertraulichkeitsklassen C1 bis C4 in diese Systeme eingeben, bei C3 und C4 allerdings nur nach Prüfung und dokumentierter Freigabe durch den Vorgesetzten/die Vorgesetzte oder eine höhere Instanz.

- **Von der Universität Stuttgart betriebene KI-Systeme mit Zugriff auf ein Modell bei einem wissenschaftsnahen Partner (z. B. GWDG) (Typ 2):**  
KI-Systeme, deren Oberfläche die Universität Stuttgart betreibt, mit Zugriff auf Modelle, die von vertrauenswürdigen, wissenschaftsnahen Einrichtungen wie der Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG) gehostet werden, ohne dass Daten an Dritte weitergegeben werden. Beschäftigte dürfen Informationen der Vertraulichkeitsklassen C1 bis C3 in diese Systeme eingeben, bei C3 allerdings nur nach Prüfung und dokumentierter Freigabe durch den Vorgesetzten/die Vorgesetzte oder eine höhere Instanz.
- **Von der Universität Stuttgart betriebene KI-Systeme mit Zugriff auf ein Modell bei einem kommerziellen Anbieter (z. B. Azure OpenAI) (Typ 3):**  
KI-Systeme, deren Oberfläche die Universität Stuttgart betreibt, mit Zugriff auf Modelle in externen Cloud-Infrastrukturen innerhalb der EU. Beschäftigte dürfen Informationen der Vertraulichkeitsklassen C1 und C2 in diese Systeme eingeben. Eine Eingabe von Informationen der Vertraulichkeitsklassen C3 und C4 ist nicht erlaubt.
- **Externe Dienste mit datenschutzfreundlichen Einstellungen und Enterprise-Verträgen (z. B. ChatGPT Team) (Typ 4):**  
KI-Systeme großer Anbieter, die über Hochschulverträge genutzt werden und nach Anmeldung mit dem Universitätsaccount datenschutzfreundliche Voreinstellungen bieten. Beschäftigte dürfen Informationen der Vertraulichkeitsklassen C1 und C2 in diese Systeme eingeben. Eine Eingabe von Informationen der Vertraulichkeitsklassen C3 und C4 ist nicht erlaubt.
- **Nicht geprüfte öffentliche KI-Systeme (z.B. Chat GPT Free) (Typ 5):**  
Beschäftigte dürfen nur Informationen der Vertraulichkeitsklasse C1 in diese Systeme eingeben. Eine Eingabe von Informationen der Vertraulichkeitsklassen C2, C3 und C4 ist nicht erlaubt. Eine Eingabe von personenbezogenen oder vertraulichen Informationen ist strikt untersagt.

#### 4. Zulässige Anwendungsfälle

Die folgende Matrix zeigt, welche Informationen welcher Vertraulichkeitsklasse in welche Typen von KI-Systemen eingegeben werden dürfen und in welchen Fällen zuvor eine zusätzliche Prüfung erforderlich ist. Der konkrete Anwendungsfall (z. B. Textentwurf, Planung, Auswertung unter Zuhilfenahme eines KI-Systems) ist jeweils zulässig, wenn die gewählte Kombination von Systemtyp und Vertraulichkeitsklasse dies erlaubt (ggf. nach zusätzlicher Prüfung).

Solange unklar ist, welchem Typ ein KI-System zuzuordnen ist, dürfen nur öffentliche Daten (C1) in dieses KI-System eingegeben werden (Restriktivfall).

	TYP 1	TYP 2	TYP 3	TYP 4	TYP 5
<b>KI-Systemtyp/ Vertraulichkeitsklasse</b>	<b>Universitäts-eigene KI-Systeme</b>	<b>Von der Uni Stgt betriebene KI-Systeme mit Modellen bei wiss.-nahen Partnern (z. B. GWDG)</b>	<b>Von der Uni Stgt betriebene KI-Systeme mit Modellen bei kommerziellen Anbietern (z.B. Azure/OpenAI)</b>	<b>Externe Enterprise-KI-Systeme (z. B. ChatGPT Teams)</b>	<b>Nicht-geprüfte öffentliche KI-Systeme (z. B. ChatGPT Free)</b>
<b>C1 – Öffentlich</b>	✔ erlaubt	✔ erlaubt	✔ erlaubt	✔ erlaubt	✔ erlaubt
<b>C2 – Intern</b>	✔ erlaubt	✔ erlaubt	✔ erlaubt	✔ erlaubt	❌ nicht erlaubt
<b>C3 Vertraulich</b>	✔ erlaubt (nach Prüfung)	✔ erlaubt (nach Prüfung)	❌ nicht erlaubt	❌ nicht erlaubt	❌ nicht erlaubt
<b>C4 – Streng vertraulich</b>	✔ erlaubt (nach Prüfung)	❌ nicht erlaubt	❌ nicht erlaubt	❌ nicht erlaubt	❌ nicht erlaubt

#### 5. Transparenz & Dokumentation

- Wird ein KI-System in größerem Umfang z. B. beim Erstellen eines Textes eingesetzt, soll dies durch eine Notiz (z. B. "erstellt mit Hilfe von GPT-4 am 20.6.2025") im Dokument kenntlich gemacht werden.
- Wird ein KI-System nur in geringem Umfang genutzt (z. B. zur Einholung von Formulierungsvorschlägen), ist keine Kennzeichnung erforderlich.
- Eine Kennzeichnung muss erfolgen, wenn KI-generierte Inhalte direkt weiterverwendet werden, etwa für Webseiten, offizielle Schreiben oder andere Veröffentlichungen.

- Wenn KI-Systeme zur Beantwortung von Anfragen eingesetzt werden – etwa im Kontakt mit Studierenden oder mit externen Personen – muss dies klar zu erkennen sein. Das gleiche gilt für den Einsatz von KI-Systemen in Lern-Management-Systemen.
- 

## **6. Schulung & Kompetenzentwicklung**

- Die Universität bietet kontinuierlich Weiterbildungen zur sicheren und vertrauensvollen Nutzung von KI-Systemen an und hält dafür Schulungen in einem asynchron nutzbaren Format bereit.
  - Die Sensibilisierung für potenzielle Verzerrungen („Bias“), Diskriminierungen und sogenannte Halluzinationen bei KI-generierten Inhalten ist fester Bestandteil dieser Schulungen.
  - Die Schulungen beinhalten auch Hinweise auf nachhaltige und digital-souveräne Nutzung von KI-Systemen, z. B. durch bevorzugte Verwendung europäischer Anbieter oder ressourcenschonender Systeme.
  - Beschäftigte sind verpflichtet, sich vor der dienstlichen Nutzung eines KI-Systems über die sichere und vertrauensvolle Nutzung, die rechtlichen Rahmenbedingungen sowie die Risiken beim Einsatz von KI-Systemen zu informieren.
- 

## **7. Governance & Verantwortung**

- Die Letztverantwortung für die richtlinienkonforme Nutzung von KI liegt bei den jeweils nutzenden Beschäftigten bzw. deren Vorgesetzten oder übergeordneten Stellen, wenn diese die Nutzung angewiesen haben.
- Das Rektorat benennt eine Ansprechperson im Prorektorat IT („KI-Referent\*in“) für Richtlinien, Schulungen der Beschäftigten zu ethischen Standards und Compliance-Anforderungen sowie die Durchführung von Audits und Risikobewertungen im Zusammenhang mit der Nutzung von KI-Systemen.
- In der „Whitelist für die unterschiedlichen Typen von KI-Systemen“, einem zusätzlichen Dokument, welches laufend aktualisiert wird, werden die vom Rektorat freigegebenen KI-Systeme aufgeführt.
- Die Freigabe eines neuen KI-Systems erfordert die Einbeziehung des KI-Referenten/der KI-Referentin, der Datenschutzstelle, dem Datenschutzbeauftragten/der Datenschutzbeauftragten und der Stabsstelle Informationssicherheit.

- Vor der dienstlichen Nutzung neuer KI-Systeme, d. h. KI-Systeme, die nicht bereits vom Rektorat freigegeben wurden, ist für Informationen der Vertraulichkeitsklasse C2 und höher eine Prüfung durch den KI-Referenten/die KI-Referentin erforderlich.
- Die Leitungen von Verwaltungseinheiten, zentralen Einrichtungen sowie von wissenschaftlichen Organisationseinheiten (z. B. Institutsleitungen, Projektleitungen) tragen die Verantwortung für die Einhaltung dieser Richtlinie innerhalb ihres jeweiligen Zuständigkeitsbereichs. Sie vergeben außerdem Freigaben für die Eingabe von Informationen ab Vertraulichkeitsklasse C3 in KI-Systeme.

### **Ergänzende Hinweise zur EU-KI-Verordnung (EU-AI Act)**

- Im Rahmen der EU-Verordnung über Künstliche Intelligenz (EU-AI Act) ist insbesondere auf Hochrisiko-KI-Systeme zu achten. Das sind Systeme, die etwa zur automatisierten Bewertung von Bewerbungen und Prüfungsleistungen oder zur Entscheidung über die Vergabe eines Studienplatzes eingesetzt werden. Sie unterliegen strengen rechtlichen Anforderungen.
- Die Universität Stuttgart setzt aktuell keine Hochrisiko-KI-Systeme ein. Sollte ein solches System eingeführt werden, ist vor der Nutzung eine Prüfung durch das Rektorat erforderlich, eingesteuert durch den/die Chief Information Officer und beraten durch den KI-Referenten/die KI-Referentin, die Datenschutzstelle, den Datenschutzbeauftragten/die Datenschutzbeauftragte, die Stabsstelle Informationssicherheit und ggf. die Ethikkommission.
- Für generative KI-Systeme (z. B. Chatbots, Bildgeneratoren) gelten die Transparenzpflichten der EU-KI-Verordnung – diese sind durch die Kennzeichnungspflichten in dieser Richtlinie abgedeckt.

---

## **8. Weiterentwicklung & Feedback**

- Das Rektorat wird diese Richtlinie mindestens einmal im Jahr überprüfen und bei Bedarf anpassen.
- Vorschläge, Anwendungsbeispiele oder Fragen zur Weiterentwicklung der Richtlinie können an die E-Mail-Adresse [ki@uni-stuttgart.de](mailto:ki@uni-stuttgart.de) gerichtet werden.

**Gültigkeit:** Version 1.0, Stand Oktober 2025

**Verantwortlich:** KI-Referent/in, Prorektorat Informationstechnologie