Leitfaden zur Nutzung von KI-Systemen (KI-Leitfaden)

(Version vom 28.04.2026)

Die Verwendung Künstlicher Intelligenz (KI) bietet Chancen, birgt aber auch Risiken. KI-Systeme müssen im Arbeitsalltag jederzeit bestimmungs- und verantwortungsvoll eingesetzt werden, um die damit verbundenen Risiken zu reduzieren und die geltenden Gesetze und UZH-Bestimmungen einzuhalten.

0. Definitionen

- KI (Künstliche Intelligenz): Eine Technologie, die es Computern und Maschinen ermöglicht, menschliches Lernen, Verständnis, Problemlösung, Entscheidungsfindung, Kreativität und Autonomie zu simulieren. (Definition von IBM[1])
- KI-System: Maschinengestütztes System, das so konzipiert ist, dass es mit unterschiedlichem Grad an Autonomie betrieben werden kann und nach seiner Einführung Anpassungsfähigkeit zeigt, und das für explizite oder implizite Ziele aus den Eingaben, die es erhält, ableitet, wie es Ausgaben wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen generieren kann, die physische oder virtuelle Umgebungen beeinflussen können. (Definition EU AIAct[2])

Für die Nutzung von KI-Systemen durch Universitätsangehörige gelten folgende Grundsätze:

1. Künstliche Intelligenz unterstützt, während Verantwortung und Kontrolle beim Menschen bleiben

Antworten und Ergebnisse der KI können fehlerhaft, unvollständig, veraltet oder diskriminierend sein.
KI kann Ergebnisse verzerren („KI-Bias“) oder frei erfinden („KI-Halluzinationen“).
Daher sind die Nutzenden:

- dazu verpflichtet den von KI-Systemen generierten Content auf inhaltliche Richtigkeit zu prüfen, bevor sie ihn verwenden
- und sind für den verwendeten Content verantwortlich.
- für die Herbeiführung von Entscheidungen und die Entscheidungen selbst verantwortlich.

Beim Erstellen und Trainieren von KI-Systemen muss darauf geachtet werden, dass diese soweit notwendig erklärbar, fair, robust, sicher und transparent sind.

2. KI-Systeme sind korrekt und sicher zu nutzen

- Es liegt in der Verantwortung der Nutzenden, dass KI-Systeme nur im Rahmen des geltenden Rechts und der UZH-Bestimmungen verwendet werden.
  - Geltende Gesetze sind jederzeit zu erfüllen, insbesondere Datenschutz, Urheberrecht und Vertragsrecht müssen eingehalten werden.
  - Die gültigen UZH-Bestimmungen sind zu befolgen. Insbesondere gelten das Reglement über den Einsatz von Informatikmitteln an der UZH (REIM[3]) sowie produktspezifische Merkblätter der Zentralen Informatik zu den verfügbaren KI-Systemen.
  - Bei der Nutzung von KI-Systemen über Skripte und API-Schnittstellen gelten die Vorgaben gemäss REIM und seinen Ausführungsbestimmungen (insb. Weisung über die Netzwerksicherheit und weitere IT-Sicherheitsregelungen)

- KI-Systeme dürfen nur mit den dafür erlaubten Daten und Informationen nach Ziff. 3.1 der Weisung zur Klassifizierung von Informationen[4] verwendet werden. Dies gilt für jegliche Art von Nutzung, insbesondere die Eingabe der Anfrage an das KI-System, und auch für die Berechtigung von Zugriffen auf Datenablagen.
  - KI-Systeme dürfen nicht mit Daten genutzt werden, die als „geheim“ zu qualifizieren sind. Ausnahmen bilden KI-Systeme, die ausdrücklich für die Verwendung mit geheimen Daten von den verantwortlichen Stellen (insbesondere Fachbereich Informationssicherheit, Fachbereich Datenschutz, Informatik (zentral oder dezentral), gegebenenfalls Ethik-Kommissionen) freigegeben sind.
  - Als „vertraulich“ oder „intern“ klassifizierte Daten und Informationen dürfen nur dann mit KI-Systemen genutzt werden, wenn das verwendete KI-System für diese Klassifizierungen freigegeben ist. Die von der Zentralen Informatik freigegebenen KI-Systeme sind im Software-Katalog[5] aufgeführt. Die freigegebene Vertraulichkeitsstufe ist dem Software-Katalog oder dem jeweiligen Merkblatt zu entnehmen.
  - „Öffentlich“ klassifizierte Daten und Informationen dürfen in KI-Systemen genutzt werden.

- KI-Systeme dürfen nur mit urheberrechtlich geschützten Inhalten Dritter genutzt werden, soweit eine entsprechende Lizenz für die Nutzung besteht.

- Bei der Verwendung von KI-Systemen ist insbesondere darauf zu achten, dass:
  - Prompts so formuliert werden, dass sie keine Informationen enthalten, die gemäss KI-Leitfaden und produktspezifischem Merkblatt nicht in ein KI-System eingegeben werden dürfen
  - Keine Dokumente hochgeladen werden, die Informationen enthalten, die gemäss KI-Leitfaden und produktspezifischem Merkblatt nicht in ein KI-System eingegeben werden dürfen

3. Bearbeitung von Personendaten in KI-Systemen

- Personendaten dürfen nur mit KI-Systemen bearbeitet werden, soweit dies zur Erfüllung der gesetzlich umschriebenen Aufgaben der jeweiligen Organisationseinheit geeignet und erforderlich ist. *Gesetzmässigkeit §8 IDG*
  - Personendaten dürfen nur für einen der Zwecke verwendet werden, für welchen sie ursprünglich beschafft worden sind oder wenn die betroffenen Personen den neuen Zweck explizit genehmigen. *Zweckbindung §9 IDG*
  - Der Gebrauch von Personendaten ist auf das für den verfolgten Zweck notwendige Minimum zu beschränken.
- Insbesondere dürfen KI-Systeme nicht genutzt werden:
  - Zur Zusammenstellung von Informationen, welche der Beurteilung wesentlicher Aspekte der Persönlichkeit einer anderen Person dienen, wie beispielsweise zur Erstellung von Arbeitszeugnissen oder Mitarbeitenden-beurteilungen. *Auswertung von Personendaten*
  - Zur automatisierten Auswertung von Informationen, um wesentliche persönliche Merkmale einer anderen Person zu analysieren oder ihre persönliche Entwicklung vorherzusagen (Profiling). *Profiling §3 Abs.4 lit. c IDG*
- Personendaten dürfen nur so lange aufbewahrt werden, wie es zur Erfüllung des jeweiligen Verarbeitungszwecks notwendig ist. *Löschung §11 IDG*
  - Mit KI-Systemen generierter Content, der Personendaten enthält, ist zu löschen, wenn er nicht weiter benötigt wird.
  - Dies betrifft auch einen allfälligen Chat-Verlauf (History).

4. Die Verwendung von KI ist offenzulegen

- Falls KI-Content ohne wesentliche Überarbeitung weiterverwendet oder publiziert wird, ist dies entsprechend zu deklarieren. Bild- oder Toninhalte, die mit KI erzeugt oder verändert worden sind, müssen gekennzeichnet werden. Weitere Informationen, wie mit der Deklaration vorzugehen ist, sind der Webseite Künstliche Intelligenz | Universität Zürich | UZH zu entnehmen.
- Wenn die Nutzung eines KI-Systems wesentlich zu einem Einzelentscheid betreffend eine Person beigetragen hat, ist dies gegenüber der betroffenen Person transparent auszuweisen.

Dieser KI-Leitfaden wurde am 28.04.2026 vom CISO der UZH erlassen und bleibt gültig, bis vernehmlasste Vorgaben für KI von der Universitätsleitung veröffentlicht werden.

[1]: Was ist künstliche Intelligenz (KI)? | IBM
[2]: Definition Künstliche Intelligenz (KI) durch EU Artificial Intelligence Act | EU AI Act
[3]: Rechtssammlung UZH | Recht und Datenschutz | UZH
[4]: Weisung zur Klassifizierung von Informationen (PDF) | Recht und Datenschutz | UZH
[5]: Software-Katalog | Zentrale Informatik | UZH