

KI-Verordnung – was nun? Herausforderungen des AI Acts für Hochschulen

DLHN-Veranstaltungsreihe KI in Lehre und
Prüfungen

Dr. Janine Horn, 05.05.2025

KI-VO (AI-Act) EU/2024/1689

- 180 Erwägungsgründe (EWG) als Erörterungen der Artikel
- 113 Artikel (Art.)
- 13 Anhänge
- Leitlinien der Europäischen Kommission, Art. 56 KI-VO

„These Guidelines are non-binding. Any authoritative interpretation of the AI Act may ultimately only be given by the Court of Justice of the European Union.“

- Gestaffeltem Geltungsbeginn, Art. 113 KI-VO

2. Februar 2025 Verbotene KI-Systeme und **KI-Kompetenz**

2. August 2025 **GPAI**-Modelle und -Systeme

2. August 2026 Transparenzpflicht **GPAI**- und **GKI**-Systeme

2. August 2027 **HRKI**-Systeme

Prüfungsschritte

1. Liegt ein KI-Modell bzw. KI-System i.S.d. KI-VO vor?
2. Welche Art von KI-System i.S.d. KI-VO handelt es sich?
3. Welche Rolle nimmt die Hochschule bzw. der/die Lehrende ein?
4. Welche Personen sind vom Einsatz des KI-Systems betroffen?
5. Welche Pflichten resultieren daraus?
6. Wie sind diese konkret umzusetzen (Umsetzungshilfen)?

KI-System

- Alle maschinengestützten Systeme, die für einen in wechselndem Maße **autonomen Betrieb** ausgelegt sind, die nach seiner Einführung anpassungsfähig sein können und die aus den **erhaltenen Eingaben explizite oder implizite Ziele ableiten**, wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen hervorbringen können, die physische oder virtuelle Umgebungen beeinflussen können, Art. 3 Abs. 1 Nr. 1 KI-VO, EWG 12
- Ausgenommen KI-Systeme zum alleinigen Zweck wissenschaftlicher Forschung und Entwicklung, Art. 2 Abs. 6 KI-VO
- Ausgenommen KI-Systeme, die unter freien und quelloffenen Lizenzen bereitgestellt werden, Art. 2 Abs. 12 KI-VO, es sei denn Hochrisiko-KI-Systeme, Verbotene KI-Systeme, GPAI-Systeme

Definition von KI-Systemen, <https://s.gwdg.de/twjJhQ>

Risikobasierter Ansatz

Verbotene KI-Systeme, Art. 5 KI-VO

z.B. Ableitung von Emotionen einer natürlichen Person in Bildungseinrichtungen, Art. 5 Abs. 1 lit. f KI-VO, EWG 44

Verbotenen Praktiken, <https://s.gwdg.de/UV8VFH>

Hochrisiko-KI-Systeme, Art. 6 KI-VO

HRKI-Systeme im Bildungsbereich, Art. 6 Abs. 2 KI-VO, Anhang III Nr. 3 lit. a-d

KI-Systeme/KI-Modelle mit allgemeinem Verwendungszweck mit/ohne systemisches Risiko, Art. 50, 51, 52 KI-VO

z.B. LLM

KI-Systeme die mit natürlichen Personen interagieren, Art. 50 KI-VO

z.B. Chatbots für Studierende zum Selbstlernen

Beteiligte beim KI-Einsatz

- Entwickler – Trainer – Anbieter – Nutzer
- Vollständige Eigenentwicklung und -nutzung, dann alle Rollen in einer Person
- Häufig Entwickler-Trainer-Anbieter in einer Person, z.B. OpenAI
- AI Training as a Service: Trainer solo
- AI as a Service: Anbieter und Nutzer getrennt
- AI on premise: Anbieter und Nutzer eine Person

Rollen nach KI-VO

- **Anbieter:** eine natürliche oder juristische Person, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck **entwickelt oder entwickeln lässt** und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem **eigenen Namen** oder ihrer Handelsmarke **in Betrieb nimmt**, sei es entgeltlich oder unentgeltlich, Art. 3 Nr. 3 KI-VO
- **Betreiber:** eine natürliche oder juristische Person, die ein **KI-System in eigener Verantwortung verwendet**, es sei denn, das KI-System wird im Rahmen einer persönlichen und **nicht beruflichen Tätigkeit** verwendet, Art. 3 Nr. 4 KI-VO, Art. 2 Abs.10 KI-VO
- **Rollenwechsel** von Betreiber zu Quasi-Anbieter, Art. 25 KI-VO
 - Bestehendes Hochrisiko-KI-System mit eigenen Namen versehen oder eine wesentliche Änderung vornehmen
 - Zweckbestimmung von GPAI-System so verändern, dass es HRKI-System wird

Rollen als Anbieter und/oder Betreiber

Natürliche oder juristische Person	Rolle
Hochschule ermöglicht Hochschulmitgliedern Nutzung von GPAI-Modellen über eine API / bietet diese im eigenen Namen an	Betreiber/ Anbieter?
Hochschule stellt selbst entwickeltes oder im Auftrag entwickeltes System zur Verfügung	Anbieter und Betreiber
Hochschule setzt von anderer Stelle bereitgestellte KI-Detektoren zur Überprüfung von Prüfungsleistungen ein	Betreiber
Hochschule nimmt wesentliche Änderungen an einem HRKI-System vor oder betreibt dies unter eigenen Namen	Quasi- Anbieter
Lehrende verwenden eigenmächtig von anderer Stelle bereitgestellte GPAI-Systeme zur Prüfungsbewertung	Quasi- Anbieter
Lehrende schreiben Verwendung von anderer Stelle bereitgestellte KI-Tools zur Erbringung der Studien- oder Prüfungsleistungen vor	Betreiber

Hochrisiko-KI-Systeme im Bildungsbereich

- hohes Risiko der Beeinträchtigung für die Gesundheit, Sicherheit oder Grundrechte der betroffenen Personen (Art. 3 I GG und Art. 12 I GG)
- Art. 6 Abs. 2 KI-VO, Anhang III Nr. 3
 - a. System zur **Zulassung** und **Zuweisung** zu Bildungsangeboten
 - b. System zur **Bewertung** und **Steuerung** von Lernergebnissen
 - c. System zur **Bewertung** des angemessenen Bildungsniveaus
 - d. System zur **Überwachung** und **Erkennung** von verbotenen Prüfungsverhalten
- Die in Anhang III genannten KI-Systeme, sollten als HRKI-Systeme eingestuft werden, da sie über den Verlauf der Bildung und des Berufslebens einer Person entscheiden und daher ihre Fähigkeit beeinträchtigen können, ihren Lebensunterhalt zu sichern, EWG 56

DLHN-Stellungnahme zum Einsatz von KI-Detektoren <https://doi.org/10.57961/fjg9-jr89>

Rückausnahme: Nachweis kein erhebliches Risiko

- Art. 6 Abs. 3 KI-VO: System darf Entscheidung nicht wesentlich beeinflussen
 1. das Ergebnis einer zuvor abgeschlossenen menschlichen Tätigkeit zu verbessern
 2. Entscheidungsmuster oder Abweichungen von früheren Entscheidungsmustern zu erkennen, ohne die zuvor abgeschlossene menschliche Bewertung durch eine angemessene menschliche Überprüfung zu ersetzen oder zu beeinflussen
 3. eine eng gefasste Verfahrensaufgabe durchzuführen
 4. vorbereitende Aufgabe für eine Bewertung durchzuführen
- **Entscheidungsassistenten vs. maschinelle Entscheidungsfindung**
- Dokumentation und Registrierung des Nachweises in öffentlicher EU-Datenbank erforderlich
- Nur Anbieter zum entlastenden Nachweis befugt, nicht Betreiber

Exkurs: Automatisierte Einzelfallentscheidung Art. 22 DSGVO

- Verbot **vollautomatisierter** Einzelfallentscheidung mit rechtlicher Wirkung bzw. erheblicher Beeinträchtigung, es sei denn eine Einwilligung oder RGL im LHG liegt vor
- Nichtbestehen einer Prüfung, Wiederholungsprüfung, Studiengangsfortschritt
- Eigenständige Stellungnahme und Entscheidung eines Prüfenden/ Lehrenden erforderlich
- EUGH - C 634/21: auch automatisierte Erstellung der Entscheidungsgrundlage unterfällt Verbot, sofern diese **maßgeblich Einfluss** auf spätere menschliche Entscheidung hat
- **Entscheidungsassistenz vs. maschinelle Entscheidungsfindung**
- Datenschutzbehörden: Autonome KI-Entscheidung muss durch natürliche Person überprüft und freigegeben werden (**Mensch-Maschine-Schnittstelle**)

Pflichten Anbieter und Betreiber bei HRKI

Anbieter, Art. 16 KI-VO

Transparenz (erklärbare KI)

Angemessenes Maß an Genauigkeit, Robustheit, Cybersicherheit

Durchführung Risiko- und Qualitätsmanagement vor und nach Inverkehrbringen

System zur Überwachung und Meldung schwerwiegender Vorfälle, Art. 72 KI-VO

Bereitstellung Betriebsanleitung

Bereitstellung technische Dokumentation

Automatische Protokollierungsfunktion

Schnittstelle für menschliche Aufsicht

Konformitätsbewertung, Art. 43 und Art. 20 KI-VO

Betreiber, Art. 26 KI-VO

Information von Personalrat und betroffene MA

Information der Betroffenen bei KI-gestützter Entscheidungsfindung

Eingabedaten Entsprechen Zweckbestimmung des Systems und sind hinreichend repräsentativ

→ Überwachung des Systems und Meldung schwerwiegender Vorfälle und Risiken

→ Verwendung gemäß Betriebsanleitung

→ Information zur Integration in eigenes System

→ Protokollierung und 6 Monate Aufbewahrung

→ Aufsichtsperson mit entsprechender KI-Kompetenz

Grundrechte-Folgenabschätzung, Art. 27 KI-VO

Pflichten Anbieter von GPAI-Modellen

- GPAI allgemein, Art. 53 KI-VO
 - Aktuelle technische Dokumentation
 - Zugang zu relevanten **Informationen und Dokumenten zum Zweck der Integration in eigenes System**, ausgenommen GPAI unter freier und quelloffener Lizenz, EWG 102, EWG 104
 - **Einhaltung des EU-Urheberrechts** und Beachtung von Urheberinnen vorgebrachten Vorbehalte, z.B. Opt-out für Text- und Data-Mining § 44b UrhG
 - Veröffentlichung einer **Zusammenfassung der Trainingsdaten**
- GPAI mit systemischem Risiko zusätzlich, Art. 55 KI-VO
 - Modellbewertung, Minderung möglicher systemischer Risiken
 - Erhöhtes Maß an Cybersicherheit, Information über schwerwiegende Vorfälle

General-Purpose AI Code of Practice, <https://s.gwdg.de/azpijc>

Transparenzpflichten Anbieter, Art. 50 Abs. 2 KI-VO

- **KI zur Interaktion mit Menschen (Chatbots)**
 - Hinweis auf Mensch-Maschine-Interaktion, es sei denn dies ist offensichtlich
- **GPAI und GKI**
 - Kennzeichnung des Outputs in maschinenlesbarem Format und als künstlich erzeugt oder manipuliert erkennbar
 - Keine Kennzeichnungspflicht bei unterstützender Funktion für die Standardbearbeitung
 - Keine Kennzeichnungspflicht sofern vom Betreiber bereitgestellten Eingabedaten oder deren Semantik nicht wesentlich verändert werden
- Information zum Zeitpunkt der ersten Interaktion oder Veröffentlichung in klarer und eindeutiger Weise unter Einhaltung der geltenden Barrierefreiheitsanforderungen

Transparenzpflichten Betreiber, Art. 50 Abs. 4 KI-VO

- **Generierte oder manipulierte Bild-, Ton- oder Videoinhalt (Deepfakes)**
 - Offenlegung, dass die Inhalte künstlich erzeugt oder manipuliert wurden
 - Sofern Inhalt Teil eines künstlerischen, kreativen, satirischen, fiktionalen oder analogen Werks oder Programms ist, Offenlegung nur soweit wie die Darstellung oder der Genuss des Werks nicht beeinträchtigt wird
- **Generierter oder manipulierter Text** zur Veröffentlichung zur Information über Angelegenheiten von öffentlichem Interesse (Artikel, Blogs, Posts, Newsletter)
 - Offenlegung, dass der Text künstlich erzeugt oder manipuliert wurde
 - Ausnahme: menschliche Überprüfung und Übernahme der redaktionellen Verantwortung durch natürliche oder juristische Person
- Information zum Zeitpunkt der ersten Interaktion oder Veröffentlichung in klarer und eindeutiger Weise unter Einhaltung der geltenden Barrierefreiheitsanforderungen

KI-Kompetenz als Rechtsbegriff

- Kompetenzbildende Maßnahmen für **Personal und andere Personen**, die **in ihrem Auftrag** mit dem **Betrieb und der Nutzung** von KI-Systemen befasst sind, Art. 4 KI-VO
- Berücksichtigung ihrer technischen Kenntnisse, Erfahrung, Ausbildung und Schulung, dem **Kontext des KI-Einsatzes**, der von **KI betroffenen Personen**, Art. 4 KI-VO
- Keine konkrete Pflicht, kein Bußgeld, aber Verstoß gegen die allgemeine Sorgfaltspflicht des Betreibers oder Anbieters im Schadensfall bei fehlerhafter Bedienung eines KI-Systems oder unzureichende Risikobewertung
- Die Fähigkeiten, die Kenntnisse und das Verständnis, die es Anbietern, Betreibern (Nutzern) und Betroffenen unter **Berücksichtigung ihrer jeweiligen Rechte und Pflichten** im Rahmen dieser Verordnung ermöglichen, **KI-Systeme sachkundig einzusetzen** sowie sich der **Chancen und Risiken von KI und möglicher Schäden**, die sie verursachen kann, bewusst zu werden, vgl. Art. 3 Nr. 56 KI-VO, EWG 20

Kompetenzdimensionen – Technik, Ethik, Recht

- KI erkennen und identifizieren können. Sie sollten verschiedene Formen der KI unterscheiden und ihre Funktionsweise zumindest in ihren Grundzügen verstehen.
- Ethische Prinzipien kennen und befolgen, die eine verantwortungsbewusste Integration von KI-Systemen ermöglichen. Sie sollten Gefahrenpotenziale der KI reflektieren und ggf. Gegenmaßnahmen einleiten können.
- Rechtskompetent sein. Sie sollten mit den Gesetzen für die Nutzung mit KI vertraut sein und über allgemeine Datenschutzkenntnisse verfügen.

Wienrich,/Carolus/Markus/Augustin, AI Literacy: Kompetenzdimensionen und Einflussfaktoren im Kontext von Arbeit, 03/2022, www.denkfabrik-bmas.de

Zusammenfassung

- Sollen KI-Systeme von Hochschulen angeboten oder betrieben werden, so macht die KI-VO dafür detaillierte Vorgaben (von Transparenz bis zu menschlicher Aufsicht)
- Pflichten nehmen mit Risiko und Rolle (Anbieter oder Betreiber) zu
- Wechsel der Risikostufe und Rollenwechsel bei Nutzung möglich
- Wechsel der Verantwortlichkeit von Hochschule zu Lehrenden möglich
- Wenn sie KI in Studium und Lehre anbieten oder betreiben, müssen sie genau hinsehen, welcher Risikoklasse ein System zuzuordnen ist, und die entsprechenden Vorgaben beachten
- KI-Kompetenz ist an die mit KI befassten Hochschulmitglieder zu vermitteln, dabei sind unterschiedliche Kompetenz-Profile zu berücksichtigen

Weiterer Vorträge

- | | |
|------------|---|
| 19.05.2025 | Nutzung generativer KI - Urheberrechte, Datenschutz und Persönlichkeitsrechte |
| 02.06.2025 | Generative KI in Prüfungen – Eine prüfungsrechtliche Herausforderung |

