

Pressemitteilung

Zentren für Kommunikation und Informationsverarbeitung in Lehre und Torsten Prill

01.02.2025

<http://idw-online.de/de/news846730>

Buntes aus der Wissenschaft, Wissenschaftliche Publikationen
Informationstechnik, Recht
überregional



KI-Verordnung / Artificial Intelligence Act: KI-Kompetenz wird Pflicht

Ab dem 2. Februar 2025 tritt eine zentrale Bestimmung der Verordnung in Kraft: Anbieter und Betreiber von KI-Systemen müssen sicherstellen, dass alle beteiligten Personen über die notwendige KI-Kompetenz verfügen. Für Hochschulen, die zunehmend auf KI-Technologien in Forschung, Lehre und Verwaltung setzen, bringt dies besondere Herausforderungen mit sich. Diese umfassen die Bewertung des Risikopotenzials eingesetzter KI-Systeme und die Etablierung zielgerichteter Schulungsmaßnahmen für Mitarbeitende. Der folgende Beitrag erläutert zentrale Aspekte der KI-VO und bietet praktische Handlungsempfehlungen, um die neuen Anforderungen rechtssicher und effizient umzusetzen.

Mit der Einführung der KI-Verordnung (KI-VO), die am 2. August 2024 in Kraft getreten ist, hat die Europäische Union einen rechtlichen Rahmen geschaffen, um den Einsatz Künstlicher Intelligenz (KI) zu regulieren und sicherer zu gestalten. Die Verordnung zielt darauf ab, die Grundrechte der EU-Bürger:innen zu schützen, Rechtssicherheit zu schaffen und verbindliche Standards für den Betrieb von KI-Systemen festzulegen.

Ein System der Künstlichen Intelligenz (KI-System) ist nach Artikel 3 Nr. 1 KI-Verordnung (KI-VO), englisch Artificial Intelligence Act (AI Act), definiert als „ein maschinengestütztes System, das so konzipiert ist, dass es mit unterschiedlichem Grad an Autonomie operieren kann und nach seiner Einführung Anpassungsfähigkeit zeigt, und das für explizite oder implizite Ziele aus den Eingaben, die es erhält, ableitet, wie es Ergebnisse wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erzeugen kann, die physische oder virtuelle Umgebungen beeinflussen können“.

Die KI-VO ist ein Rechtsakt der Europäischen Union, die den Einsatz von Künstlicher Intelligenz regulieren soll, und ist am 2. August 2024 in Kraft getreten. Ziel ist es, die Grundrechte der EU-Bürger:innen zu wahren, Rechtssicherheit herzustellen sowie Sicherheitsstandards für den Betrieb von KI-Systemen und den Umgang mit KI-Anwendungen festzulegen. Sie gilt für Anbieter, Importeure oder Händler von KI-Systemen, die in der EU in Verkehr gebracht werden, sowie für Betreiber von KI-Systemen, die ihren Sitz in der EU haben. Auch Anbieter, Betreiber und Produkthersteller mit Sitz in Drittländern sind betroffen, wenn die KI-Ausgabe in der EU verwendet wird.

☑ Als Anbieter gilt, wer aktiv an der Entwicklung beteiligt ist oder ein bereits bestehendes KI-Modell in ein eigenes Produkt integriert und dieses unter seiner Marke vertreibt.

☑ Als Betreiber wird eingestuft, wer ein KI-System für interne Zwecke einsetzt, ohne es weiterzuentwickeln oder als eigenes Produkt anzubieten.

Wenn an KI-Modellen oder -Systemen geforscht wird und sie zusätzlich nicht produktiv genutzt werden, sind diese vom Anwendungsbereich der KI-VO ausgenommen. Dieses Forschungsprivileg gilt nicht für KI-Modelle und -Systeme, die in der Forschung als Tool eingesetzt werden, wie z.B. Software zur Transkription von Interviews, die nicht eigens und für den alleinigen Zweck der wissenschaftlichen Forschung und Entwicklung entwickelt und in Betrieb genommen worden sind.

In der KI-VO wird ein risikobasierter Ansatz verfolgt. Mit diesem risikobasierten Ansatz wird die Regulierungsintensität an das Risiko angepasst, das von der konkreten Anwendung ausgeht. Sechs Monate nach Inkrafttreten der KI-VO sind

KI-Systeme mit inakzeptablem Risiko verboten, weil sie besonders tief in die Grundrechte eingreifen und potenziell erheblichen Schaden verursachen können. In der KI-VO werden vier Risikostufen für KI-Systeme definiert (siehe Originalpublikation <https://www.zki.de/>)

Ab dem 2. Februar 2025 tritt eine der zentralen Vorschriften der KI-VO (Art. 4 KI-VO) in Kraft. Anbieter und Betreiber von KI-Systemen müssen sicherstellen, dass ihre Mitarbeitenden und wahrscheinlich einzelfallabhängig auch Studierende, die KI-Systeme der Hochschule nutzen sollen, sowie alle weiteren in den Betrieb oder die Nutzung eingebundenen Personen über ein ausreichendes Maß an KI-Kompetenz verfügen. Die Gesetzgebung verlangt die Sicherstellung der KI-Kompetenz, definiert als Kombination von Fähigkeiten, Kenntnissen und Verständnis, um KI-Systeme sachkundig zu nutzen, einschließlich des Bewusstseins für Chancen, Risiken und mögliche Schäden. Ziel ist es, die Risiken im Umgang mit Künstlicher Intelligenz zu minimieren und einen verantwortungsvollen Einsatz von KI-Technologien gemäß Zeitplan seit Inkrafttreten des AI Act zu gewährleisten (siehe weiterführende Informationen)

Mittels einer KI-Inventur kann ermittelt werden, welche KI-Systeme zu welchem Einsatzzweck verwendet werden und wie diese funktionieren. Vorhandene moderne Software Asset Management Tools (SAM Tools) können dabei unterstützen.

Zum einen kann über eine KI-Inventur identifiziert werden, welche KI-Systeme ein inakzeptables Risiko haben und damit verboten wären. Für die KI-Inventur muss der Verwendungszweck jedes einzelnen Systems kurz umrissen werden. Auf dieser Grundlage gilt es zu prüfen, ob eine der Anwendungen in die Beschreibung eines der Absätze von Artikel 5 der KI-VO fällt. Solche Systeme müssen bis spätestens zum 2. Februar 2025 außer Betrieb genommen werden.

Zum anderen kann auf Grundlage einer KI-Inventur auch der Schulungsbedarf analysiert werden, um mögliche niederschwellige, auch kostenlose oder kostengünstige Möglichkeiten auszuloten, um Mitarbeitenden allgemeine Grundlagen von KI zu vermitteln (z.B. über Materialsammlungen für unterschiedliche Bedarfe wie Informationsmaterialien, Podcast, Kurse, Videos).

Damit könnten ggf. erste Mindestanforderungen an KI-kompetente Mitarbeitende erfüllt werden. Auf dieser Basis sollte dann – insbesondere beim Einsatz von KI-Systemen in höheren Risikokategorien – schrittweise, ggf. mit Partnern, ein zielgruppenspezifisches Angebot aufgebaut werden. Diese Vorgehensskizze lehnt sich an die Empfehlungen von „KI-Campus“ an. Der „KI-Campus“ ist eine Gemeinschaftsinitiative mit der Zielstellung, einzigartige Strukturen für Bildungsinnovationen auf regionaler, nationaler und europäischer Ebene zu schaffen (siehe Originalquelle <https://www.zki.de/>)

Werden in einem KI-System auch personenbezogene Daten verarbeitet, ist neben der KI-VO die DSGVO zu beachten. Die Verarbeitung personenbezogener Daten in KI-Systemen wird regelmäßig dazu führen, dass für die Verarbeitungstätigkeiten, in denen diese Systeme eingesetzt werden, eine Datenschutz-Folgenabschätzung durchgeführt werden muss. Dies gilt für den Einsatz von KI-Systemen in Forschung, Lehre und Hochschulverwaltung und ist bei der zeitlichen Planung von Projekten zu berücksichtigen.

wissenschaftliche Ansprechpartner:

Johannes Nehlsen, Universität Würzburg | Stabsstelle IT-Recht
Karola Möhring, TU Ilmenau | Hochschul-IT-Zentrum Thüringen | Stabsstelle IT-Recht
Stephan Rehfeld, TU Braunschweig | Datenschutz, Risikomanagement und Informationssicherheit

Originalpublikation:

ZKI-News zum Inkrafttreten AI Act am 02.02.2025:
<https://www.zki.de/aktuelles/ki-verordnung-artificial-intelligence-act-ki-kompetenz-ab-2-februar-2025-pflicht/>

ZKI-Publikationsliste:

<https://www.zki.de/publikationen/>

ZKI-Handlungsempfehlung AI Act:

https://www.zki.de/fileadmin/user_upload/Downloads/ZKI_KI-Verordnung_AI-Act_Handlungsempfehlung.pdf

ZKI-Merkblatt zur KI-VO:

https://www.zki.de/fileadmin/user_upload/Downloads/ZKI_KI-Verordnung-Anlage-Merkblatt.pdf

URL zur Pressemitteilung: <http://Quelle: https://www.digitalaustria.gv.at/Themen/KI/AI-Act.html>

URL zur Pressemitteilung: <http://Quelle: Dr. Till und weitere in „EU AI Act: Wie wird Deutschland KI-kompetent?“>

URL zur Pressemitteilung: <https://ki-campus.org/blog/ai-act-ki-kompetenzen>