AI Act: Das gilt für KI in Hochschulen und Forschung

Künstliche Intelligenz (KI) bietet zahlreiche Chancen für Forschung, Lehre und Verwaltung, wirft aber zugleich komplexe rechtliche Fragen auf. Die KI-Verordnung der Europäischen Union (AI Act) hat auch für Hochschulen und den Wissenschaftsbereich erhebliche Auswirkungen. Die ersten Vorgaben des AI Acts gelten bereits seit dem 2. Februar 2025.

In diesen Bereichen nutzen Hochschulen KI

KI ist für Hochschulen und Forschungseinrichtungen insbesondere in vier Bereichen relevant:

Nutzung in der Hochschulverwaltung: Hochschulen können KI-gestützte Systeme zur Effizienzsteigerung in der Verwaltung nutzen, etwa für die automatisierte Analyse von Studienverläufen oder im HR-Bereich.

Nutzung durch Studierende: Studierende nutzen inzwischen Chatbots, Sprachmodelle oder Bildgenerierungssysteme bei der Erstellung von schriftlichen Arbeiten, teilweise auch bei Klausuren und anderen Prüfungsleistungen.

Nutzung in der Forschung: Im wissenschaftlichen Bereich wird KI oft für Datenanalysen, Mustererkennung oder Modellierung wissenschaftlicher Theorien eingesetzt.

Entwicklung oder Weiterentwicklung von KI: Hochschulen und Forschungseinrichtungen sind auch an der Entwicklung neuer KI-Systemen, KI-Modelle und Algorithmen beteiligt.

Das bedeutet der AI Act für Hochschulen und Wissenschaftseinrichtungen

Hochschulen und Wissenschaftseinrichtungen müssen nach dem AI Act sicherstellen, dass sie die gesetzlichen Anforderungen an Transparenz, Datenschutz und Sicherheit erfüllen. Gleichzeitig sollte die wissenschaftliche Freiheit und innovative Forschung nicht übermäßig eingeschränkt werden.

Hochschulen und Wissenschaftseinrichtungen sind verpflichtet, interne Richtlinien zur Nutzung von KI zu entwickeln, Mitarbeitende zu schulen und interdisziplinäre Expertengremien einzusetzen, die sich mit der verantwortungsvollen Implementierung von KI-Technologien befassen.

Die KI-Verordnung verfolgt einen risikobasierten Ansatz. Anwendungen werden je nach Risikostufe unterschiedlich reguliert:

- **Verbotene KI**: Bestimmte KI-Technologien, die mit hohen Risiken für Grundrechte verbunden sind (zum Beispiel biometrische Echtzeit-Identifikation im öffentlichen Raum), sind verboten.

- **Hochriskante KI**: Systeme, die in sensiblen Bereichen wie kritischer Infrastruktur, Bildungs-wesen oder Beschäftigung eingesetzt werden, unterliegen strengen Anforderungen hinsichtlich Transparenz, Datenschutz und Sicherheit.
- **Geringes Risiko**: KI-Anwendungen mit geringem Risiko müssen lediglich allgemeine Vorgaben erfüllen.

Hochschulen müssen damit rechnen, dass KI-gestützte Bewertungs- und Auswahlverfahren oder Systeme zur Entscheidungsfindung, zum Beispiel Zulassungsverfahren, als „hochriskant“ eingestuft werden und daher den umfassenden Compliance-Anforderungen des AI Acts unterliegen.

Privilegierung von Forschungseinrichtungen

Der AI Act gilt ausdrücklich nicht für KI-Systeme oder KI-Modelle, die eigens für den alleinigen Zweck der wissenschaftlichen Forschung und Entwicklung entwickelt werden, solange sie nicht in Verkehr gebracht oder in Betrieb genommen werden (Artikel 2 Abs. 8 des AI Acts). Hintergrund der Ausnahme ist, dass die EU Innovation fördern, die Freiheit der Wissenschaft achten und Forschungs- und Entwicklungstätigkeiten nicht untergraben möchte. Erwägungsgrund 25 des AI Acts betont, dass KI-Systeme, die im Rahmen von Grundlagenforschung, experimenteller Entwicklung oder wissenschaftlicher Erprobung entwickelt werden, nicht den regulären Vorgaben der Verordnung unterliegen. Auch wenn die Vorgaben des AI Act nicht gelten, sind ethische und wissenschaftliche Integritätsstandards zu wahren und sicherzustellen, dass Forschende KI verantwortungsbewusst einsetzen.

Die Forschungsprivilegierung gilt nur für den Zeitraum, in dem ein KI-System oder KI-Modell ausschließlich für Forschungs-, Test- oder Entwicklungszwecke genutzt wird. Sobald eine dieser Bedingungen nicht mehr erfüllt ist, gelten die regulären Vorschriften des AI Acts. Ein KI-System oder -Modell gilt als „in Verkehr gebracht“, sobald es erstmals auf dem Markt bereitgestellt wird (vgl. hierzu auch die Definition des Art 3 Abs. 9 AI Act). Kommerziell nutzbare KI-Produkte oder -Dienste, die an externe Nutzende verkauft, lizenziert oder weitergegeben werden, fallen unter die regulären Anforderungen des AI Acts. Forschungseinrichtungen, die ein KI-Modell als fertiges Produkt weitergeben oder veröffentlichen, müssen dann sicherstellen, dass es den Vorgaben der Verordnung entspricht.

Ein KI-System oder -Modell wird „in Betrieb genommen“, wenn es über den reinen Forschungs- und Testzweck hinaus tatsächlich angewendet wird (vgl. hierzu auch die Definition des Art 3 Abs. 10 AI Act). Ein KI-System oder -Modell, das in einer realen Umgebung mit echten Nutzerdaten getestet oder genutzt wird, ist dann nicht mehr von der Forschungsprivilegierung erfasst.

Hierzu ein Beispiel: Eine Hochschule entwickelt eine KI zur automatisierten Bewertung von Prüfungen. Solange diese KI in einer Testumgebung erprobt wird, greift die Forschungsprivilegierung. Wird sie jedoch in einer echten Prüfungsbewertung eingesetzt, gilt sie als „in Betrieb genommen“ und unterliegt dem AI Act.

Anforderungen an Transparenz, Sicherheit und Datenschutz

Der AI Act setzt verbindliche Regelungen für den Einsatz von KI-Anwendungen und definiert spezifische Anforderungen hinsichtlich Transparenz, Sicherheit und Datenschutz. Die genannten Anforderungen betreffen primär KI-Systeme, nicht generell alle KI-Modelle.

- **Transparenz**: Hochschulen und Wissenschaftseinrichtungen müssen sicherstellen, dass Nutze-rinnen und Nutzer klar über den Einsatz von KI informiert werden. Das gilt für KI-Systeme, die in Entscheidungsprozesse eingebunden sind, zum Beispiel automatische Bewerberauswahl, KI-gestützte Prüfungsbewertungen. KI-Modelle als solche, zum Beispiel ein trainiertes Modell, das intern für Forschung genutzt wird, unterliegen diesen Transparenzpflichten nicht direkt, es sei denn, sie sind Teil eines KI-Systems.
- **Sicherheit**: KI-Anwendungen müssen so entwickelt und betrieben werden, dass sie keine Risiken für Personen oder Daten darstellen. Dies erfordert regelmäßige Sicherheitsprüfungen und Risikoanalysen. Dies betrifft KI-Systeme, die aktiv eingesetzt werden, insbesondere Hochrisiko-Systeme, zum Beispiel medizinische Diagnosetools. Für KI-Modelle gibt es nur Sicherheitsanforderungen, wenn es sich um allgemeine KI-Modelle (GPAI) mit systemischem Risiko handelt. In diesen Fällen gelten Verpflichtungen zur Risikoprüfung.
- **Datenschutz**: Die DSGVO gilt für alle KI-Anwendungen, die personenbezogene Daten verarbeiten, also sowohl für KI-Systeme als auch für KI-Modelle, wenn sie mit solchen Daten trainiert oder eingesetzt werden. Hochschulen müssen Maßnahmen zur Anonymisierung oder Pseudonymisierung ergreifen, wenn KI-Modelle oder KI-Systeme mit sensiblen Daten arbeiten.

Anforderungen für hochriskante KI

Hochriskante KI-Systeme unterliegen besonders strengen Anforderungen, darunter:

- **Risikomanagement**: Ein systematisches Risikomanagement muss etabliert werden, um potenzielle Gefahren frühzeitig zu erkennen und zu minimieren.
- **Datenqualität und Fairness**: Hochschulen und Wissenschaftseinrichtungen müssen sicherstellen, dass Trainings- und Testdaten von hoher Qualität sind und keine Verzerrungen oder Diskriminierung fördern.
- **Menschliche Überwachung**: Es muss sichergestellt werden, dass kritische Entscheidungen nicht vollständig automatisiert erfolgen und dass Menschen in den Entscheidungsprozess eingreifen können.
- **Robustheit und Sicherheit**: KI-Systeme müssen vor externen Angriffen und Manipulationen geschützt werden, und es sind regelmäßige Sicherheitsüberprüfungen erforderlich.
- **Dokumentationspflichten**: Hochschulen und Wissenschaftseinrichtungen müssen detaillierte Aufzeichnungen über die Funktionsweise und Entscheidungen von KI-Systemen führen, um im Falle von regulatorischen Prüfungen Transparenz nachweisen zu können.

Hochschulen sollten das Prüfungsrecht anpassen

Ein weiterer wichtiger Punkt, der vor allem Hochschulen betrifft, ist die Anpassung des Prüfungsrechts. Angesichts der Anforderung an Transparenz ist es unerlässlich, dass Hochschulen klar festlegen, wo und unter welchen Bedingungen der Einsatz von KI erlaubt ist. Dies betrifft insbesondere Prüfungsleistungen, bei denen der Einsatz von KI-Technologien möglicherweise nicht immer nachweisbar ist. Hochschulen sollten Regelungen erlassen, die für Studierende eindeutig nachvollziehbar sind und für Prüfende eine klare Handhabung ermöglichen.
Um die Integrität von Prüfungen zu gewährleisten, sollten bestehende Prüfungsordnungen überarbeitet werden. Eine Möglichkeit ist die Einführung mündlicher Erläuterungen oder Disputationen für nicht beaufsichtigte Prüfungsformate, insbesondere für Abschlussarbeiten.

Diese Personen sind verantwortlich

Hochschulleitungen, Fachabteilungen, Nutzerinnen und Nutzer von KI-Anwendungen tragen gemeinsam die Pflicht, die Einhaltung gesetzlicher Vorgaben sicherzustellen. Dies umfasst:

- **Institutionelle Verantwortung**: Hochschulen müssen sicherstellen, dass KI-Anwendungen den geltenden gesetzlichen Rahmenbedingungen entsprechen und regelmäßig überprüft werden.
- **Individuelle Verantwortung**: Mitarbeitende, Forschende und Studierende, die KI-Anwendungen nutzen oder entwickeln, sollten über ein ausreichendes Maß an Wissen und Kompetenz verfügen, um mögliche Risiken zu erkennen und zu minimieren.
- **Haftungsfragen**: Im Falle von Fehlentscheidungen durch KI-Systeme müssen Verantwortlichkeiten rechtlich analysiert und klar geregelt sein, insbesondere in Bezug auf Datenschutzverstöße oder diskriminierende Entscheidungen.

Handlungsempfehlungen für Hochschulen und Wissenschaftseinrichtungen

- Hochschulen und Wissenschaftseinrichtungen sollten prüfen, welche KI-Anwendungen unter die Regelungen des AI Acts fallen, und entsprechende Compliance-Maßnahmen ergreifen.
- Es ist wichtig, sich aktiv in die Diskussion über regulatorische Rahmenbedingungen einzubringen, um eine Balance zwischen Schutzmechanismen und Forschungsfreiheit zu gewährleisten.
- Rechtliche, ethische und technische Expertinnen und Experten sollten gemeinsam an nachhaltigen KI-Lösungen für den Hochschul- und Forschungsbereich arbeiten.
- Lehrende, Forschende und Verwaltungspersonal sollten über die rechtlichen Implikationen von KI informiert werden.

Ansprechpartner:

Dr. Jannike Ehlers
Tel: +49 (0)40 360994-5021
jannikeluiseehlers@kpmg-law.com