

Das KI-Forschungsprivileg

Das sogenannte KI-Forschungsprivileg im EU AI Act bedeutet, dass bestimmte Forschungs-, Test- und Entwicklungstätigkeiten an KI-Systemen oder KI-Modellen nicht unter die regulären Pflichten der KI-Verordnung fallen, solange das betreffende System noch nicht in Verkehr gebracht oder in Betrieb genommen wurde.

Erfasst ist damit ausschließlich die **Entwicklung, Erprobung oder wesentliche Veränderung eines KI-Systems oder KI-Modells** im Forschungs- und Entwicklungsstadium. Ebenfalls ausgenommen sind KI-Systeme, die ausschließlich für wissenschaftliche Forschung und Entwicklung entwickelt und eingesetzt werden.

Wichtig ist die klare Abgrenzung:

Dieses Forschungsprivileg gilt **nicht** für den normalen Einsatz bereits fertiger KI-Systeme, etwa wenn Forschende, Lehrende oder Studierende ChatGPT, Gemini, Claude, NotebookLM, Elicit oder andere verfügbare Tools zur Recherche, Textbearbeitung, Datenanalyse, Lehre oder Verwaltung verwenden. In diesen Fällen wird kein eigenes KI-System entwickelt oder verändert, sondern ein bestehendes KI-System genutzt. Dafür gelten weiterhin die allgemeinen Vorgaben der PMU-KI-Richtlinie, insbesondere zu Verantwortung, Transparenz, Datenschutz, Vertraulichkeit, Kennzeichnung und wissenschaftlicher Integrität.

Wird ein im Forschungsprivileg entwickeltes oder erprobtes KI-System später in den regulären Betrieb überführt, etwa in Lehre, Klinik, Verwaltung, Prüfung oder Studienorganisation, endet die bloße Forschungssituation. Vor einer solchen Nutzung ist eine Prüfung nach den einschlägigen Governance-, Datenschutz-, Risiko- und Freigabeverfahren erforderlich.

(Text KI-gereiert)

- [Rechtlicher Rahmen: KI-Forschungsprivileg](#)

Rechtlicher Rahmen: KI-Forschungsprivileg

(Text KI-generiert)

Das KI-Forschungsprivileg nach dem AI Act betrifft KI-Systeme, die tatsächlich ausschließlich für wissenschaftliche Forschung und Entwicklung gebaut, trainiert, validiert oder technisch erprobt werden.

Nach Art. 2 Abs. 6 AI Act fallen solche KI-Systeme grundsätzlich nicht unter die operativen Pflichten des AI Act, solange sie ausschließlich für wissenschaftliche Forschungs- und Entwicklungszwecke entwickelt und genutzt werden. Ergänzend privilegiert Art. 2 Abs. 8 AI Act insbesondere Laborforschung, interne Entwicklung, Modelltraining, Validierung und technische Erprobung vor einer Markteinführung oder vor dem Regelbetrieb.

Wichtig ist dabei die Abgrenzung: Das Forschungsprivileg betrifft die Entwicklung, Veränderung oder Erprobung eines KI-Systems, nicht den normalen Einsatz bereits fertiger KI-Systeme wie ChatGPT, Claude, Gemini oder anderer verfügbarer Tools in Forschung, Lehre, Verwaltung oder Klinik.

Die Ausnahme gilt nicht grenzenlos. Sobald ein entwickeltes KI-System unter realen Bedingungen außerhalb eines Labors oder einer simulierten Umgebung getestet wird, um belastbare Daten zu sammeln oder seine Konformität zu prüfen, greift das Forschungsprivileg nicht mehr automatisch. Ein solcher Test fällt nur dann nicht als „Inverkehrbringen“ oder „Inbetriebnahme“ ins Gewicht, wenn er entweder als behördlich begleitetes KI-Reallabor nach Art. 57 AI Act oder als regulierter Realwelttest außerhalb eines Reallabors nach Art. 60 AI Act durchgeführt wird. Für Tests unter Realbedingungen sind daher die Schutzvorgaben der Art. 60 und 61 AI Act besonders relevant.

Das Forschungsprivileg hebt andere rechtliche Anforderungen nicht auf. Art. 2 Abs. 7 AI Act stellt klar, dass andere Rechtsvorschriften weiterhin anwendbar bleiben. Dazu gehören insbesondere die DSGVO, mögliche Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO, der Schutz besonderer Kategorien personenbezogener Daten, insbesondere Gesundheitsdaten nach Art. 9 DSGVO, Forschungsethik, Urheberrecht, Vertraulichkeits- und Geheimhaltungspflichten sowie Patient*innenrechte und Proband*innenschutz.

Das Forschungsprivileg endet insbesondere dann, wenn das KI-System auf den Markt gebracht oder in Betrieb genommen wird, nicht mehr ausschließlich wissenschaftlicher Forschung und Entwicklung dient, gegenüber Studierenden, Mitarbeitenden, Patient*innen, Proband*innen oder Dritten eingesetzt wird oder für reale Bewertungen, Auswahlentscheidungen, Überwachung, Diagnose, Behandlung, Verwaltung oder sonstige Entscheidungen genutzt wird. Nach Ende des Privilegs sind insbesondere eine Rollenprüfung der PMU als mögliche Anbieterin oder Betreiberin, eine Risikoklassifizierung einschließlich der Prüfung auf Hochrisiko-KI nach Art. 6 AI Act in

Verbindung mit Anhang III, eine Datenschutzprüfung, gegebenenfalls eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO, sowie bei sensiblen oder hochriskanten Anwendungen eine Grundrechteprüfung erforderlich.

Für die weitere Nutzung sind außerdem die besonders relevanten AI-Act-Pflichten zu beachten: Art. 4 AI Act verpflichtet zur Sicherstellung von KI-Kompetenz; Art. 5 AI Act verlangt den Ausschluss verbotener KI-Praktiken; Art. 26 AI Act enthält Betreiberpflichten bei Hochrisiko-KI; Art. 27 AI Act betrifft die Grundrechte-Folgenabschätzung; Art. 50 AI Act regelt Transparenzpflichten bei KI-Interaktion, synthetischen Inhalten und Deepfakes. Zusätzlich sind menschliche Aufsicht, Transparenz, Dokumentation, Informationssicherheit und eine Freigabe durch das KI- und Digitalisierungsboard, gegebenenfalls auch durch Rektorat oder Vorstand, zu prüfen.

Als praktische Entscheidungsregel gilt: Wird KI ausschließlich für Forschung oder technische Erprobung entwickelt, kann ein möglicher Anwendungsfall des Forschungsprivilegs vorliegen. Hat die Nutzung jedoch Auswirkungen auf Studierende, Mitarbeitende, Patient*innen, Proband*innen oder Dritte, oder soll das System unter Realbedingungen in Lehre, Klinik, Verwaltung, Personalverfahren oder sonstigen PMU-Prozessen eingesetzt werden, muss vor einer weiteren Ausrollung das KI & Digitalisierungsboard kontaktiert werden.