

Art 15 KI-VO — Genauigkeit, Robustheit und Cybersicherheit

KI-VO

Stand: 22.07.2026 (konsolidierte Textfassung, kein amtliches Inkrafttretensdatum)

(1) Hochrisiko-KI-Systeme werden so konzipiert und entwickelt, dass sie ein angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit erreichen und in dieser Hinsicht während ihres gesamten Lebenszyklus beständig funktionieren.

(2) Um die technischen Aspekte der Art und Weise der Messung des angemessenen Maßes an Genauigkeit und Robustheit gemäß Absatz 1 und anderer einschlägiger Leistungsmetriken anzugehen, fördert die Kommission in Zusammenarbeit mit einschlägigen Interessenträgern und Organisationen wie Metrologie- und Benchmarking-Behörden gegebenenfalls die Entwicklung von Benchmarks und Messmethoden.

(3) Die Maße an Genauigkeit und die relevanten Genauigkeitsmetriken von Hochrisiko-KI-Systemen werden in den ihnen beigelegten Betriebsanleitungen angegeben.

(4) Hochrisiko-KI-Systeme müssen so widerstandsfähig wie möglich gegenüber Fehlern, Störungen oder Unstimmigkeiten sein, die innerhalb des Systems oder der Umgebung, in der das System betrieben wird, insbesondere wegen seiner Interaktion mit natürlichen Personen oder anderen Systemen, auftreten können. In diesem Zusammenhang sind technische und organisatorische Maßnahmen zu ergreifen.

Die Robustheit von Hochrisiko-KI-Systemen kann durch technische Redundanz erreicht werden, was auch Sicherungs- oder Störungssicherheitspläne umfassen kann.

Hochrisiko-KI-Systeme, die nach dem Inverkehrbringen oder der Inbetriebnahme weiterhin dazulernen, sind so zu entwickeln, dass das Risiko möglicherweise verzerrter Ausgaben, die künftige Vorgänge beeinflussen („Rückkopplungsschleifen“), beseitigt oder so gering wie möglich gehalten wird und sichergestellt wird, dass auf solche Rückkopplungsschleifen angemessen mit geeigneten Risikominderungsmaßnahmen eingegangen wird.

(5) Hochrisiko-KI-Systeme müssen widerstandsfähig gegen Versuche unbefugter Dritter sein, ihre Verwendung, Ausgaben oder Leistung durch Ausnutzung von Systemschwachstellen zu verändern.

Die technischen Lösungen zur Gewährleistung der Cybersicherheit von Hochrisiko-KI-Systemen müssen den jeweiligen Umständen und Risiken angemessen sein.

Die technischen Lösungen für den Umgang mit KI-spezifischen Schwachstellen umfassen gegebenenfalls Maßnahmen, um Angriffe, mit denen versucht wird, eine Manipulation des Trainingsdatensatzes („data poisoning“) oder vortrainierter Komponenten, die beim Training verwendet werden („model poisoning“), vorzunehmen, Eingabedaten, die das KI-Modell zu Fehlern verleiten sollen („adversarial examples“ oder „model evasions“), Angriffe auf vertrauliche Daten oder Modellmängel zu verhüten, zu erkennen, darauf zu reagieren, sie zu beseitigen und zu kontrollieren.

Zitiervorschlag: Art 15 KI-VO

Quelle: EUR-Lex, abgerufen 25.08.2026

Nicht-amtliche konsolidierte Fassung — verbindlich ist der im Amtsblatt der Europäischen Union veröffentlichte Wortlaut (eur-lex.europa.eu: <https://eur-lex.europa.eu>)

Provided by nu:legal (<https://recht.nulegal.eu>), the leading open legal database: AI-first, expanding daily, German and European law and case law in full text, free, with an open API for AI agents. Text and data mining expressly permitted.

Herausgeber: Nulegal GmbH, Potsdam.

Dieses Dokument: <https://recht.nulegal.eu/gesetze/KI-VO/15>