

AI-ACT

Folgen und Chancen der ersten Regulierung künstlicher Intelligenz

Podiumsdiskussion, 26.11.2024

schafft **Wissen**
sichert **Werte**

Umsetzung



AI-Act – mit August 2024 in Kraft

Für **Kreditauskunfteien** in Österreich bedeutet der AI-Act, dass sie strengere Auflagen erfüllen müssen, wenn sie **KI-basierte Systeme** für die **Bonitätsbewertung** verwenden. Solche Systeme fallen unter die „**Hochrisiko-KI-Systeme**“ (laut Anhang III AI-Act).

Anwendbar ab 2. August 2026

Hochrisiko KI-Systeme [A3]

- ✓ Transparenz und Erklärbarkeit
- ✓ Regelmäßige Überprüfung und Risikomanagement
- ✓ Datenqualität

Anwendbar ab 2. Februar 2025

Verbotene KI-Praktiken

Anwendbar ab 2. August 2025

KI-Systeme mit allgemeinem Verwendungszweck

Anwendbar ab 2. August 2027

Hochrisiko KI-Systeme [A1]

Fallstricke des AI-Acts

- ⇒ Definitionen für Normadressaten nicht leicht verständlich
- ⇒ Praktische Umsetzungsprobleme bei Transparenz, Datenqualität und Protokollierung
- ⇒ Herausforderung KI im Datenschutz

Definition KI-System

[...] ein maschinengestütztes System, das für in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können.

Transparenz

Bereitstellung detaillierter Informationen über KI-Modelle **vs.** Geschäftsgeheimnis iSv. proprietären Algorithmen und/oder Datenstrategien.

ErwG 63 S 3. AI-Act

Diese Verordnung sollte nicht als Rechtsgrundlage für die Verarbeitung personenbezogener Daten, gegebenenfalls einschließlich besonderer Kategorien personenbezogener Daten, verstanden werden, es sei denn, dies ist in dieser Verordnung ausdrücklich anders vorgesehen.

Möglichkeiten durch den AI-Act

- ✓ **Präzisierung der Anforderungen an automatisierte Entscheidungen**
Erklärbarkeit, Robustheit, und Nachvollziehbarkeit der KI-Modelle
- ✓ **Klarstellung der Rolle menschlicher Überprüfungen**
Definierte Standards, wie und wann menschliche Eingriffe erforderlich sind
- ✓ **Harmonisierung von Transparenzanforderungen**
Dokumentation und Nachvollziehbarkeit
Technischen Erklärbarkeit der Modelle (zB. verständliche Darstellungen von KI-Ergebnissen)
- ✓ **Risikobasierte Regulierung und differenzierte Behandlung**
Klassifizierung nach Risiko – dadurch Ermöglichung differenzierter Behandlung

Grundrechte-Folgeabschätzung

Vor der Inbetriebnahme eines Hochrisiko-KI-Systems im Bereich Kredit- und Bonitätsscoring ist eine Abschätzung der Auswirkungen, die die Verwendung eines solchen Systems auf die Grundrechte haben kann, durchzuführen:

- Beschreibung der Verfahren des Betreibers, bei denen das Hochrisiko-KI-System im Einklang mit seiner Zweckbestimmung verwendet wird.
- Beschreibung von Zeitraum und Häufigkeit, innerhalb dessen bzw. mit der jedes Hochrisiko-KI-System verwendet werden soll.
- Kategorien der natürlichen Personen / Gruppen, die von der Verwendung im spezifischen Kontext betroffen sein könnten.
- Spezifische Schadensrisiken, die sich auf die ermittelten Kategorien natürlicher Personen / Gruppen auswirken könnten, unter Berücksichtigung der vom Anbieter bereitgestellten Informationen.
- Beschreibung der Umsetzung von Maßnahmen der menschlichen Aufsicht entsprechend den Betriebsanleitungen.
- Maßnahmen, die im Falle des Eintretens dieser Risiken zu ergreifen sind, inkl. der Regelungen für die interne Unternehmensführung und Beschwerdemechanismen.

Auszugsweise wichtig aus dem AI-Act für Kreditauskunfteien:

- ✓ Artikel 6 (Hochrisiko-Klassifikation), inkl. Artikel 7 mit den Änderungen des Anhang 3
- ✓ Artikel 9 (Risikomanagementsystem)
- ✓ Artikel 10 (Daten und Daten-Governance)
- ✓ Artikel 11 (Technische Dokumentation)
- ✓ Artikel 13 (Transparenzpflichten)
- ✓ Artikel 14 (Menschliche Aufsicht)
- ✓ Artikel 43 (Konformitätsbewertung)
- ✓ Artikel 71–74 (Sanktionen)

Kapitaladäquanzverordnung = Capital Requirements Regulation (CRR), EU-Verordnung

Digital Operational Resilience Act (DORA) (kritisch, wichtig)

EU-Verbrauchercredit-Richtlinie = Consumer Credit Directive II (CCD II); nationale Umsetzung Juni 2025 (Verbraucherkreditgesetz)
Vergabeverbot, Diskriminierungsverbot, Dokumentation der Prozesse

**Grundrechtfolgenabschätzung (AIA),
Datenschutzfolgenabschätzung (DSGVO)**

Datenschutz-Grundverordnung (DSGVO) inkl. Einzelfallentscheide
EUGH 7.12.2023 Scoring, ART 22

Artificial Intelligence Act
Kreditprüfung Hochrisiko

**Kreditinstitute-
Immobilienfinanzierungsmaßnahmen-
Verordnung (KIM-VO)**

the AI Office launched a targeted stakeholder consultation (13.11.24)

"...the use of statistical methods, such as logistic regression, has raised questions related to the conditions under which certain software systems should be considered outside the scope of the AI system definition. The Commission guidelines are expected to provide a methodology for distinguishing AI systems from simpler traditional software systems or programming approaches, thus helping to define systems that are outside the scope of the AI Act."

Parliamentary questions on the AI

MEPs Axel Voss (EPP, DE) and Svenja Hahn (Renew, DE) have recently announced that they are tabling a parliamentary question to the European Commission regarding the definition of AI. These MEPs seek to know how the Commission will ensure that the definition of AI systems in the EU aligns with the OECD definition, which excludes simple statistical techniques, such as logistic regression. They also ask whether the Commission will clarify, in its upcoming guidelines on the AI definition, the meaning of "basic data processing" in relation to the capacity of an AI system to infer.

A parliamentary question is a formal tool that Members of the European Parliament (MEPs) use to seek information or press for action from other EU institutions or bodies. These questions help MEPs fulfill their oversight and legislative roles. The Commission is expected to respond to these MEPs within the next six weeks.

Vielen Dank!

Gerhard Wagner

Geschäftsführer

KSV1870 Information GmbH

Wagenseilgasse 7, 1120 Wien

T +43 (0) 50 1870-8124

www.ksv.at