

SHAPING EUROPE'S DIGITAL FUTURE

Ziele des AI Acts im Bereich der Hochrisiko-KI-Systeme

European AI Office – DG CNECT

Grundlagen der KI-Verordnung

Regeln für vertrauenswürdige KI



Produktsicherheitsgesetz: Sicherheit, Schutz von Gesundheit und Grundrechten



Fokus auf KI-System als Produkt und damit technologie-neutral



Proportionalität durch **risikobasierten Ansatz**



Vertrauen entlang der Wertschöpfungskette durch Regeln für general-purpose KI



Verantwortungsvolle Innovation

Wann ist ein KI-System „hochrisiko“?

Entscheidend ist der Verwendungszweck des KI-Systems:

1

KI-Systeme ist Teil eines regulierten Produkts oder gilt als reguliertes Produkt

Relevante Produktgesetze sind in Anhang I aufgelistet.

Zwei Voraussetzungen:

- KI-System soll als Sicherheitskomponent verwendet werden oder gilt selbst als Produkt nach dem Produktgesetz
- Betroffenes Produkt unterliegt einer Konformitätsprüfung durch Dritte

2

KI-Systeme soll in einem “Hochrisiko”- Anwendungsfall eingesetzt werden

8 Bereiche mit hoher Grundrechtsrelevanz, gelistet in Anhang III (z.B. Bildung, Strafverfolgung).

Pro Bereich konkrete Anwendungsfälle.

KI-System wird als „hochrisiko“ eingestuft, wenn es für einen dieser Anwendungsfälle verwendet werden soll.



„Filter“: KI-Systeme nach bestimmen Kriterien ausgenommen werden (z.B. wenn sie nur eng gefasste Verfahrensaufgaben übernehmen)

Anforderungen und Pflichten

Anbieter



Anforderungen an KI-System, Datenqualität, menschliche Aufsicht, Akkuratheit, Robustheit



Konformitätsprüfung bevor das KI-System in den Verkehr gebracht wird



Qualitäts- und Risikomanagement, um Risiken für Betreiber und betroffene Personen zu minimieren



Registrierung in einer EU-Datenbank

Betreiber



Korrektur Betrieb nach Gebrauchsanweisung und Training von Mitarbeiter/innen



Verwendung **repräsentativer Daten** und Aufbewahrung von **Protokollen**



Ggbf. **Informationspflichten** gegenüber betroffenen Personen



Ggbf. **Grundrechtsfolgenabschätzung** (gilt nur für bestimmte Arten von Betreibern)

Möglichkeit zur Ausnahme

Ein KI-System, das für einen „Hochrisiko“-Anwendungsfall verwendet werden soll, kann ausnahmsweise als nicht-hochriskant eingestuft werden

Vier Fälle:

- KI-System soll eng gefasste Verfahrensaufgabe durchführen
- KI-System soll zuvor abgeschlossene menschliche Tätigkeit verbessern
- KI-System soll Entscheidungsmuster erkennen, ohne menschliche Entscheidung zu ersetzen
- KI-System soll vorbereitende Aufgabe für eine Bewertung durchführen

Keine Ausnahme wenn KI-System **Profiling** vornimmt.

Um Umgehungen zu vermeiden und Rückverfolgbarkeit zu gewährleisten müssen diese KI-Systeme dennoch in EU-Datenbank registriert werden

Wie geht es weiter?

Umsetzungsprioritäten der Kommission:

Aufbau der Governance-Struktur

Einrichtung des AI Office (KI-Büro), Einrichtung der Beratungsgremien, Unterstützung der Mitgliedsstaaten im Aufbau der Behörden

Koordinierung des „Code of Practice“ für general-purpose KI

Kommission koordiniert den Prozess, in dem Anbieter von general-purpose KI und andere Stakeholder einen „Code of Practice“ zu den neuen Regeln entwickeln

Vorbereitung von Normen für die „Hochrisiko“-Anforderungen

Kommission hat den europäischen Normungsorganisationen CEN und CENELEC ein Mandat erteilt und verfolgt die Entwicklung der technischen Spezifikationen

Vorbereitung von Leitlinien, Durchführungs- und delegierten Rechtsakten

Priorität haben dabei Leitlinien für die praktische Anwendung der KI-System-Definition und der Verbotsvorschriften (Veröffentlichung vor/mit Geltung der Vorschriften)

Inkrafttreten:
August 2024

Verbote

6 Monate

Governance und General-purpose AI

12 Monate

Alle anderen Vorschriften

24 Monate

Hochrisiko KI nach anderen Produktgesetzen

36 Monate



Vielen Dank