Herausforderungen des EU Artificial Intelligence Act

Workshop „Herausforderungen Low-Code orientierter KI-Ansätze“

Prof. Dr. Ralf Schnieders

12.11.2024

in Kaiserslautern

Hochschule für Technik
und Wirtschaft Berlin

University of Applied Sciences

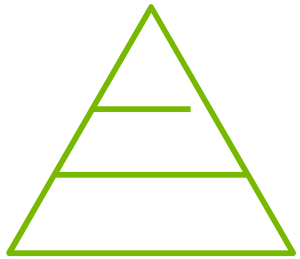
Agenda

1. Aufbau und Grundgedanke der KI-VO (AI Act)
2. Anwendungsbereich und Inkrafttreten
3. Anforderungen für Hochrisiko-KI
4. Transparenzanforderungen
5. Überwachung – Durchsetzung - Betroffenenrechte

Agenda

1. **Aufbau und Grundgedanke der KI-VO (AI Act)**
2. Anwendungsbereich und Inkrafttreten
3. Anforderungen für Hochrisiko-KI
4. Transparenzanforderungen
5. Überwachung – Durchsetzung - Betroffenenrechte

Aufbau und Grundgedanke



Der risikobasierte Ansatz der KI-VO:

- Unannehmbares Risiko → Verbot
  - Z.B. biometrische Echtzeit-Fernidentifikation zu Strafverfolgugszwecken
- Hochrisiko-KI-System → Spezielle Anforderungen und Bewertung (als spezielles Produktsicherheitsrecht)
  - KI-Systeme, die in Produkten verwendet werden, die nach den Produktsicherheitsregeln der EU durch Dritte zertifiziert werden müssen, z.B. für bestimmte Medizinprodukte
  - KI-Systeme, die in „Hochrisiko“-Bereichen für Persönlichkeitsrechte, z.B. Strafverfolgung, Asyl, Arbeitsplatz eingesetzt werden
- Sonstige KI → Transparenzanforderungen
  - Z.B. für generative KI-Systeme mit allgemeinem Verwendungszweck wie ChatGPT

Agenda

1. Aufbau und Grundgedanke der KI-VO (AI Act)
2. **Anwendungsbereich und Inkrafttreten**
3. Anforderungen für Hochrisiko-KI
4. Transparenzanforderungen
5. Überwachung – Durchsetzung - Betroffenenrechte

Anwendungsbereich

- **Anbieter**: wer KI entwickelt und in Verkehr bringt (sozusagen der „Hersteller“)
- **Betreiber**: wer ein KI-System in eigener Verantwortung verwendet.

→ unabhängig vom Sitz in der EU!

- **Ausnahme** für **Forschung**: Entwicklung bis zum „Prototyp“. Geltung der KI-VO sobald Absicht operativer Nutzung oder Vertriebs (Art. 2 Abs. 6, 8)

Inkrafttreten

- Zeitlich gestufter **Anwendungsbeginn**:
  - 1.8.2024 Inkrafttreten
  - Verbote ab 2.2.2025
  - 2.8.2025 Regeln über Behördeneinrichtungen, Sanktionen, KI-Modelle mit allg. Verwendungszweck
  - 2.8.2026 Sonstige Regeln, bis auf:
  - 2.8.2027 Regeln über produktbezogene KI-Hochrisiko-Systeme (Art. 113)
  - Längere Übergangsfristen für KI-Modelle, die vor dem 2.8.2025 in Verkehr gebracht wurden (Art. 111)

Agenda

1. Aufbau und Grundgedanke der KI-VO (AI Act)
2. Anwendungsbereich und Inkrafttreten
3. **Anforderungen für Hochrisiko-KI**
4. Transparenzanforderungen
5. Überwachung – Durchsetzung - Betroffenenrechte

Anforderungen an Hochrisiko-KI-Systeme (1)

- Grundanforderung: Risikomanagement als iterativer Prozess über den gesamten Lebenszyklus (Art. 9):
  - Ermittlung der Risiken für Gesundheit, Sicherheit und Grundrechte,
  - Bewertung der Verwendungsrisiken,
  - Risikomanagementmaßnahmen zur Bewältigung der Risiken.

Anforderungen an Hochrisiko-KI-Systeme (2)

- Qualitätsanforderungen an die Trainingsdaten (Art. 10)
- Dokumentation des Erfüllens der Anforderungen (Art. 11)
- Transparenz: Betriebsanleitung u.a. (Art. 13)
- Robustheit und IT-Sicherheit (Art. 15)
- Konformitätsbewertung durch den Anbieter und Anbringung einer CE-Zertifizierung (Art. 40-48)
- Registrierung in der EU-Datenbank (Art. 49)
- Meldung von Vorfällen an die Überwachungsbehörden (Art. 73)

Agenda

1. Aufbau und Grundgedanke der KI-VO (AI Act)
2. Anwendungsbereich und Inkrafttreten
3. Anforderungen für Hochrisiko-KI
4. **Transparenzanforderungen**
5. Überwachung – Durchsetzung - Betroffenenrechte

Transparenzanforderungen (Art. 50)

- Besondere Anforderungen gelten für bestimmte KI-Systeme
- Pflichten für den Anbieter (als technische Anforderung):
  - Bei direkter Interaktion mit Personen: Pflicht zur Offenlegung der Interaktion mit einem KI-System
  - Für generative KI: Pflicht zur maschinenlesbaren Kennzeichnung KI-generierter Inhalte
- Pflichten für den Betreiber:
  - Für Emotionserkennungssysteme oder Systeme zur biometrischen Kategorisierung (unbestimmt?): Pflicht zur Offenlegung
  - Deepfakes und Nachrichten von öffentlichem Interesse: Pflicht zur Kennzeichnung

Agenda

1. Aufbau und Grundgedanke der KI-VO (AI Act)
2. Anwendungsbereich und Inkrafttreten
3. Anforderungen für Hochrisiko-KI
4. Transparenzanforderungen
5. **Überwachung – Durchsetzung - Betroffenenrechte**

Überwachung – Durchsetzung - Betroffenenrechte

- **Überwachung** der Vorschriften über Hochrisiko-KI durch **nationale Behörden**, in D wohl überwiegend die Länder (Art. 74)
- **Überwachung** von KI-Modellen mit allgemeinem Verwendungszweck durch die **Europäische Kommission** und ihr **Büro für Künstliche Intelligenz** (Art. 88)
- **Bußgelder** (Art. 99)
- **Betroffenenrechte**: Beschwerderecht auch für nicht selbst Betroffene (Art. 85), Recht auf Erläuterung (Art. 86)
- **Ausführungsrechtsakte** und **Leitlinien** der Kommission sowie **Praxisleitfäden** des Büros für Künstliche Intelligenz (Art. 56) zur Konkretisierung

Danke für die Aufmerksamkeit!