

Gesellschaft für Informatik – Regionalgruppe Köln

Verwendung von KI-Modellen mit allgemeinem
Verwendungszweck – Rechtliche Pflichten für
die Beteiligten aus der KI-VO

Agenda

- I. Worum geht's?
- II. Überblick
- III. Pflichten für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck
- IV. Zusätzliche Pflichten bezüglich KI-Modellen maVwz mit systemischen Risiken
- V. (Allgemeine) Pflichten für Anbieter von KI-Systemen, die fremde Modelle verwenden
- VI. Durchsetzung der Pflichten und Haftung

Worum geht's?

- Foundation Models
 - = „KI-Modelle mit allgemeinem Verwendungszweck“ (Art. 3 Ziff. 63 KI-VO)
 - erhebliche allgemeine Verwendbarkeit
 - Eignung, ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen
 - Möglichkeit, sie in eine Vielzahl nachgelagerter Systeme oder Anwendungen zu integrieren
 - Training mit großer Datenmenge unter umfassender Selbstüberwachung
 - Verschiedene Akteure bei der Erstellung des Modells und seiner nachgelagerten konkreten Verwendung beteiligt

→ Erschwerte Zuordnung von Verantwortlichkeiten entlang der KI-Wertschöpfungskette.

II. Überblick

- **Ziel der KI-VO:**

„Zweck dieser Verordnung ist es, das Funktionieren des Binnenmarkts zu verbessern und die Einführung einer auf den Menschen ausgerichteten und vertrauenswürdigen KI zu fördern und gleichzeitig ein hohes Schutzniveau in Bezug auf Gesundheit, Sicherheit und die in der Charta verankerten Grundrechte, einschließlich Demokratie, Rechtsstaatlichkeit und Umweltschutz, vor schädlichen Auswirkungen von KI-Systemen in der Union zu gewährleisten und die Innovation zu unterstützen.“ (Art. 1 Abs. 1 KI-VO)

- Erst im Jahr 2023 sind generative KI und Foundation Models in den Fokus der Gesetzgebung gerückt (2021 erster Vorschlag KI-VO)
- „Neue“ **Risiken** in bestehende Systematik integrieren: z.B. hinsichtlich des demokratischen Diskurses und der öffentlichen Meinungsbildung, des Schutzes menschlichen Schaffens, Befürchtung mangelnder Zuverlässigkeit von KI-Systemen, insb. durch Halluzinationen

Pflichten für Anbieter von KI-Modellen maVwz

- Im Hinblick auf KI-Modelle maVwz nur **Anbieter** verpflichtet
- **Anbieter** (Art. 3 Nr. 3 KI-VO)
 - eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle,
 - die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt,
 - und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich

Pflichten für Anbieter von KI-Modellen maVwz

- **Erstellung und fortlaufende Aktualisierung einer technischen Dokumentation**, die auf Anfrage **Behörden** zur Verfügung gestellt werden muss (Art. 53 Abs. 1 lit. a i.V.m. Anhang XI KI-VO) 
- **Informationspflichten gegenüber den Anbietern von KI-Systemen**, die beabsichtigen, das KI-Modell mit allgemeinem Verwendungszweck in ihre KI-Systeme zu integrieren (Art. 53 Abs. 1 lit. b i.V.m. Anhang XII KI-VO) 
 - Soll dafür sorgen, dass Anbieter von KI-Systemen ihrerseits die Pflichten aus der KI-VO erfüllen können
 - Schaffung von Vertraulichkeit zum Schutz von Geistigem Eigentum und Geschäftsgeheimnissen
- **Ausnahme** für Open-Source-Modelle (Art. 53 Abs. 2 Satz 1 KI-VO)

Pflichten für Anbieter von KI-Modellen maVwz

- **Auf den Weg bringen einer „Urheberrechtsstrategie“** (Art. 53 Abs. 1 lit. c KI-VO)
 - Soll dafür sorgen, dass „Urheberrecht der Union“ eingehalten wird
 - Keine urheberrechtliche Einzelfallbewertung der Trainingsdaten
- **Veröffentlichung einer hinreichend detaillierten Zusammenfassung der für das Training des KI-Modells verwendeten Inhalte** (Art. 53 Abs. 1 lit. d KI-VO)
 - Hierfür soll es eine Vorlage geben.
- Keine Ausnahmen



Zusätzliche Pflichten bezüglich systemischer Risiken

- **Zusätzliche Pflichten für Anbieter bei KI-Modell maVwz mit systemischem Risiko** (Art. 55 KI-VO)
- **Systemisches Risiko** (Art. 3 Nr. 65 KI-VO):
 - erhebliche Auswirkungen auf den Unionsmarkt
 - aufgrund von großer Reichweite oder tatsächlicher oder vernünftigerweise vorhersehbarer negativer Auswirkungen für die öffentliche Gesundheit, die Sicherheit, die öffentliche Sicherheit, die Grundrechte oder die Gesellschaft
 - Einstufungsverfahren, das an Fähigkeiten mit hohem Wirkungsgrad anknüpft (Art. 51 Abs. 1 KI-VO)
 - Vermutung anhand des Trainingsaufwands, wenn $> 10^{25}$ Gleitkommaoperationen (Art. 51 Abs. 2 KI-VO)
 - ansonsten: Bewertung anhand von objektiven, vorwiegend technischen Kennzahlen (Art. 51 Abs. 1 lit. b KI-VO i.V.m. Annex XIII)



Zusätzliche Pflichten bezüglich systemischer Risiken

- **Risikomanagement- und Informationspflichten (Art. 55 Abs. 1 KI-VO):**
 - Durchführung einer Modellbewertung mit standardisierten Protokollen und Instrumenten (lit. a)
 - Bewertung und Minderung möglicher systemischer Risiken auf Unionsebene (lit. b)
 - Erfassung und Dokumentation von Informationen über etwaige schwerwiegende Vorfälle und mögliche Abhilfemaßnahmen, diesbezügliche Unterrichtung der Behörden
 - Gewährleistung eines „angemessenen Maßes“ an Cybersicherheit



(Allg.) Pflichten von Anbietern von KI-Systemen, die Modelle verwenden

Risikobasierter Ansatz

- Zuordnung je nach konkretem Verwendungszweck (ein KI-System kann unterschiedlichen Risikostufen zugeordnet sein)
- präventive Prüfung



Voraussetzungen:

Unannehmbares Risiko
= Verbotene KI-Systeme,
Art. 5 KI-VO

Hochrisiko-KI-Systeme,
Art. 6 und 7 KI-VO
= Hauptregulierung (bis Art. 49)

Geringes Risiko
= Transparenzpflichten,
Art. 50 KI-VO

Minimales Risiko
= keine Regulierung

(Allg.) Pflichten von Anbietern von KI-Systemen, die Modelle verwenden

Risikobasierter Ansatz

- Zuordnung je nach konkretem Verwendungszweck (ein KI-System kann unterschiedlichen Risikostufen zugeordnet sein)
- präventive Prüfung

Voraussetzungen:

Unannehmbares Risiko
= Verbotene KI-Systeme,
Art. 5 KI-VO



Hochrisiko-KI-Systeme,
Art. 6 und 7 KI-VO
= Hauptregulierung (bis Art. 49)

Geringes Risiko
= Transparenzpflichten,
Art. 50 KI-VO

Minimales Risiko
= keine Regulierung

(Allg.) Pflichten von Anbietern von KI-Systemen, die Modelle verwenden

Risikobasierter Ansatz

- Zuordnung je nach konkretem Verwendungszweck (ein KI-System kann unterschiedlichen Risikostufen zugeordnet sein)
- präventive Prüfung

Voraussetzungen:

Unannehmbares Risiko
= Verbotene KI-Systeme,
Art. 5 KI-VO

Hochrisiko-KI-Systeme,
Art. 6 und 7 KI-VO
= Hauptregulierung (bis Art. 49)



Geringes Risiko
= Transparenzpflichten,
Art. 50 KI-VO

Minimales Risiko
= keine Regulierung

(Allg.) Pflichten von Anbietern von KI-Systemen, die Modelle verwenden

Risikobasierter Ansatz

- Zuordnung je nach konkretem Verwendungszweck (ein KI-System kann unterschiedlichen Risikostufen zugeordnet sein)
- präventive Prüfung

Voraussetzungen:

Unannehmbares Risiko
= Verbotene KI-Systeme,
Art. 5 KI-VO

Hochrisiko-KI-Systeme,
Art. 6 und 7 KI-VO
= Hauptregulierung (bis Art. 49)

Geringes Risiko
= Transparenzpflichten,
Art. 50 KI-VO

Minimales Risiko
= keine Regulierung

Adressaten:

1. Anbieter
2. auch: Betreiber



Durchsetzung der Pflichten und Haftung

- **Durchsetzung der Pflichten:**

- primär: präventiv orientierte Vorgaben
- Geldbußen für Anbieter der Modelle: 3% des gesamten weltweiten Jahresumsatzes im vorangegangenen Geschäftsjahr oder 15 Mio. EUR (Art. 101 KI-VO)
- daneben Beschwerderecht nachgelagerter Anbieter von KI-Systemen:

„Nachgelagerte Anbieter haben das Recht, eine Beschwerde wegen eines Verstoßes gegen diese Verordnung einzureichen.“ (Art. 89 Abs. 2 KI-VO)

Durchsetzung der Pflichten und Haftung

- **Haftung:**

- Vertraglicher Anknüpfungspunkt:
 - Der Anbieter eines Hochrisiko-KI-Systems und Dritte, die Komponenten bereitstellen, die in einem Hochrisiko-KI-System verwendet oder integriert werden, treffen eine schriftliche Vereinbarung über ihre Zusammenarbeit und den Zugang zu Informationen (Art. 25 Abs. 4 KI-VO)
 - freiwillige Musterbedingungen sollen bereitgestellt werden
- KI-VO trifft keine Haftungsregelungen, auch Entwurf der KI-Haftungs-RL wurde jüngst von der Kommission zurückgezogen
- Stattdessen: Geltung mitgliedstaatlichen Zivilrechts
 - Sektorspezifische Regelungen, z.B. aus dem Urheberrecht
 - Regelung zur Produkthaftung (neue Produkthaftungs-RL vom 10.10.2024)
 - § 823 Abs. 1 und 2 BGB

Vielen Dank für Ihre Aufmerksamkeit

Ihre Ansprechpartnerin

Dr. Stefanie Schulz-Große

Leipziger Platz 3, 10117 Berlin

Tel: +49 30 88 56 65-248

schulz-grosse@redeker.de

Rechtsanwälte, Partnerschaftsgesellschaft mbB, Sitz Bonn, Essen PR 1947



Berlin · Bonn · Brüssel · Leipzig · London · München

www.redeker.de

REDEKER | SELLNER | DAHS

Berlin

Leipziger Platz 3
10117 Berlin
Tel +49 30 885665-0
Fax +49 30 885665-99
berlin@redeker.de

Bonn

Willy-Brandt-Allee 11
53113 Bonn
Tel +49 228 72625-0
Fax +49 228 72625-99
bonn@redeker.de

Brüssel

172, Av. de Cortenberg
1000 Brüssel
Tel +32 2 74003-20
Fax +32 2 74003-29
bruessel@redeker.de

Leipzig

Stentzlers Hof
Petersstraße 39-41
04109 Leipzig
Tel +49 341 21378-0
Fax +49 341 21378-30
leipzig@redeker.de

London

4 More London Riverside
London SE1 2AU
Tel +44 20 740748-14
Fax +44 20 743003-06
london@redeker.de

München

Maffeistraße 4
80333 München
Tel +49 89 2420678-0
Fax +49 89 2420678-69
muenchen@redeker.de

Rechtsanwälte, Partnerschaftsgesellschaft mbB, Sitz Bonn, Essen PR 1947



Berlin · Bonn · Brüssel · Leipzig · London · München

www.redeker.de

REDEKER | SELLNER | DAHS