fieldfisher

# ARIC Brown Bag
# Update zur KI Verordnung

2. April 2024

Martin Lose

# Wann kommt der AI Act?

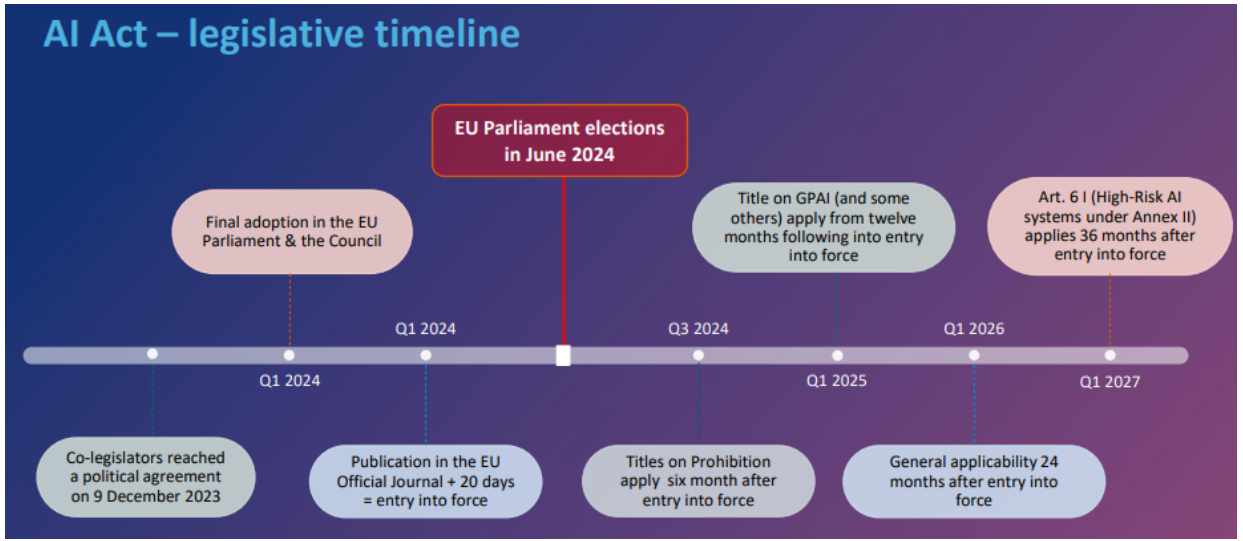
**Wegmarken des Gesetzgebungsverfahrens**

- Gesetzgebungsverfahren „auf den letzten Metern“:
  - 1. Entwurf der Kommission (April 2021)
  - Standpunkt des Rates zum Gesetz über künstliche Intelligenz festgelegt (Dezember 2022)
  - Monatelange Trilogverhandlung zwischen Parlament, Kommission und Rat münden im Dezember 2023 in politischer Einigung
  - Formelle Zustimmung der Mitgliedsstaaten (Februar 2024) und des Parlaments (März 2024)

# Wann kommt der AI Act?

## Inkrafttreten

- 20 Tage nach Veröffentlichung im Amtsblatt, anschließend stufenweise Geltung verschiedener Regelungsbereiche




# Was ist KI?

**Definition von "Systemen der künstlichen Intelligenz" in Artikel 3 Nr. 1 EU-KI-Verordnung in Anlehnung an OECD-Definition:**

„ein ***maschinengestütztes System***, das so konzipiert ist, dass es mit unterschiedlichem ***Grad an Autonomie*** operieren kann und das für explizite oder implizite Ziele Ergebnisse wie ***Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann***, die das ***physische oder virtuelle Umfeld beeinflussen***"

# Single Purpose KI – KI mit spezifischem Verwendungszweck


→ **Verbotene KI**

→ **Hochrisiko-KI** → **Umfangreiche Pflichten für Anbieter, Einführer und Nutzer!**

→ **KI mit minimalem Risiko** → **Transparenzpflichten**

# Einteilung der Risikoklassen

## Verbotene KI

- Systeme zur **biometrischen Kategorisierung**, die auf sensiblen Merkmalen basieren (politische Meinung, Religion und Weltanschauung, sexuelle Ausrichtung und ethnische Herkunft)
- **Ungezielte Erfassung von Gesichtsbildern** aus dem Internet oder von Überwachungskameras **zur Erstellung einer Datenbank zur Gesichtserkennung**
- **Emotionserkennung** am Arbeitsplatz und in Bildungseinrichtungen
- Systeme, die das ***Verhalten von Personen manipulieren*** und deren freien Willen beeinträchtigen
- KI-Systeme, die **Schwächen einer Gruppe von Personen** (Alter, körperliche oder geistige Behinderung) ***in Schädigungsabsicht ausnutzen***
- **Social-Scoring-Systeme**, die Personen anhand ihres Sozialverhaltens oder ihrer persönlichen Merkmale bewerten

## Hochrisiko-KI

- **KI-Systeme, die speziellen EU –Sicherheitsvorschriften unterliegen** (Maschinen, Spielzeug, Luftfahrt- und Fahrzeugtechnik, Medizinprodukte, Aufzüge)
- **Kritische Infrastrukturen**
- **Schul- oder Berufsausbildung**, wenn der Zugang einer Person zur Bildung und zum Berufsleben beeinträchtigt werden könnte (z.B. Bewertung von Prüfungen);
- **Beschäftigung, Personalmanagement und Zugang zu selbständiger Tätigkeit** (z.B. Software zur Auswertung von Lebensläufen für Einstellungsverfahren);
- **Grundlegende private und öffentliche Dienstleistungen** (z.B. Bewertung der Kreditwürdigkeit, wodurch Bürgern die Möglichkeit verwehrt wird, ein Darlehen zu erhalten);
- **Strafverfolgung**, die in die Grundrechte der Menschen eingreifen könnte (z.B. Bewertung der Verlässlichkeit von Beweismitteln);
- **Migration, Asyl und Grenzkontrolle** (z.B. Überprüfung der Echtheit von Reisedokumenten);
- **Justiz** und **demokratische Prozesse** (z.B. Anwendung der Rechtsvorschriften auf konkrete Sachverhalte).

***Sonderfall:*** *Besondere Regelungen im Bereich* ***biometrischer Fernidentifizierung, zum Beispiel zur Bekämpfung bestimmter Katalogstraftaten*** *(Richtervorbehalt)*

## KI mit minimalem Risiko

- Für die **Interaktion** mit natürlichen Personen bestimmt (insb. Chatbots und Empfehlungssysteme)
- Visuelle und akustische Manipulation ("**deep fake**")

# Hohe Anforderungen für Hochrisiko-KI

## Hochrisiko-KI

- **Folgenabschätzung (Grundrechte)**
- **Risikomanagementsystem**
- **Daten-Governance** (konzeptionelle Entscheidungen, Datenerfassung und -aufbereitung, Annahmen; Eignungsbewertung, Bias-Bewertung, Gap-Analyse)
- Verwendete Daten müssen **relevant, repräsentativ, fehlerfrei und vollständig** sein
- **Technische Dokumentation** (Nachweisfunktion)
- **Aufzeichnungspflicht**: Protokollierung nach anerkannten Normen und Spezifikationen
- **Transparenzpflichten** u.a. Merkmale, Leistungsgrenzen, Risiken, Informationen über verwendete Trainings- oder Testdaten
- **Menschliche Aufsicht** muss „vollständiges Verständnis und ordnungsgemäße Überwachung“ ermöglichen
- **Konzeptionelle Anforderungen** – angemessenes Maß an Robustheit, Genauigkeit, Cybersicherheit; Widerstandsfähigkeit gegenüber Fehlern, Störungen, Unstimmigkeiten, Hacking etc.
- **Qualitätsmanagementsystem**
- Durchführung des **Konformitätsbewertungsverfahrens** und Erstellen der Konformitätserklärung
- **CE-Kennzeichnung**
- Bei Nicht-EU-Anbietern: **Benennung von EU-Vertreter**

# General Purpose AU – KI mit allgemeinem Verwendungszweck

## **Neu:** Zusätzliche Pflichten für Anbieter von KI-Basismodellen

Einstufung von KI-Basismodellen erfolgt nicht nach Einsatzzweck sondern nach Leistung des KI-Modells:

- **Alle Basismodelle** müssen zusätzliche Transparenzpflichten erfüllen, einschließlich einer umfassenden technischen Dokumentation und einer detaillierten Aufstellung über die Verwendung urheberrechtlich geschützter Trainingsdaten und der Kennzeichnung von mit KI-generierten Inhalten (insb. Wasserzeichen)

- Für **sehr leistungsstarke KI Basismodelle** „mit erheblichen Auswirkungen“, die systemische Risiken bergen können, gelten zusätzliche Pflichten, insbesondere in Bezug auf die Überwachung schwerwiegender Vorfälle, die Modellbewertung und Angriffstests (nur anwendbar, wenn beim Training des Modells mehr als 10^25 Gleitkommaoperationen pro Sekunde benötigt wurden)

# Aufsicht und Sanktionen

## Zuständige Aufsichtsbehörden

- Auf EU-Ebene: **Amt für künstliche Intelligenz** wird geschaffen, welche die Umsetzung der Verordnung in allen Mitgliedstaaten koordiniert.
- Auf nationaler Ebene: **EU-Mitgliedstaaten müssen zuständige nationale Behörden einrichten/bestimmen**, die für die Durchsetzung verantwortlich sind.

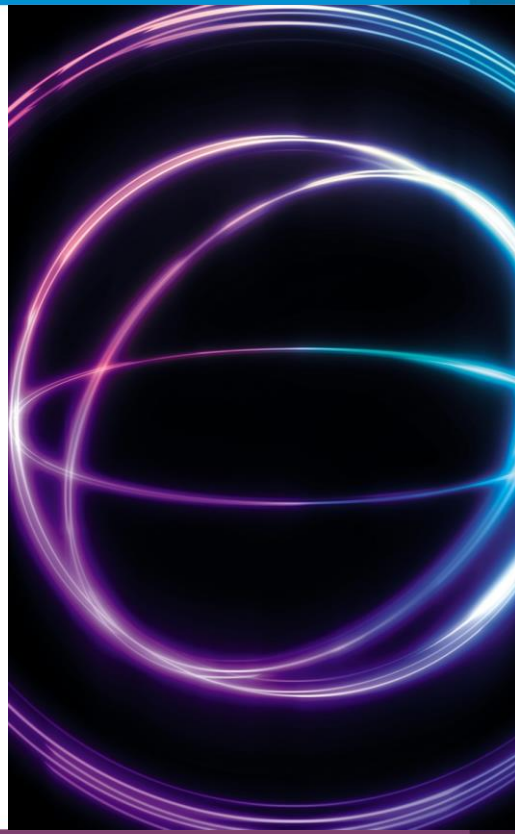
## Mögliche Sanktionen

- Verstöße in Bezug auf **verbotene KI-Systeme** können mit Geldstrafen in Höhe von bis zu **35 Millionen EUR oder 7% des weltweiten Jahresumsatzes** geahndet werden.
- Für ***weniger gravierende Verstöße*** gelten Höchstgrenzen von 15 Millionen / 3% bzw. 7,5 Millionen / 1,5%

# Fazit „AI-Act“ der EU – Was kommt auf Behörden zu?

**Insgesamt soll die KI-Verordnung dazu beitragen, dass der Einsatz von KI in der öffentlichen Verwaltung in Deutschland auf eine rechtlich fundierte und ethisch verantwortungsvolle Weise erfolgt.**

- Die **deutsche Verwaltung fällt daher in den Anwendungsbereich** des „AI-Acts“ der EU, sofern sie selbst KI-Systeme anbietet (in den Verkehr bringt) oder auch die von Dritten zur Verfügung gestellten KI-Systeme nutzt.
- Sofern in der öffentlichen Verwaltung sog. **Hochrisikosysteme** eingesetzt werden, muss unter anderem die Einhaltung von Datenschutzvorschriften, Transparenz und Nachvollziehbarkeit der Systeme sowie die Sicherstellung menschlicher Aufsicht beachtet werden.



# Überblick: Sonstige rechtliche Rahmenbedingungen

- Unternehmensinterne Regelungen zum Umgang mit KI

- Künftig: Spezielle Regelungen im Bereich Produkthaftung

- Rechtsgrundlage für Verwendung von Trainingsdaten
- Rechtsgrundlage für Input-Daten
- Personenbezug bei KI-Modellen
- Sonstige Compliance (Transparenz, Betroffenenrechte)


- Rechte an Input-Daten
- Rechte an Output-Daten
- Schutzfähigkeit des Outputs

- Bias/Diskriminierung

- Verwaltungsrechtliche Grenzen des Einsatzes von KI (z.B. Erfordernis besonderer Rechtsgrundlagen, § 35a VwVfG)

# Vielen Dank!

fieldfisher


**Martin Lose**

Counsel, Technology & Data

martin.lose@fieldfisher.com

Fieldfisher, Hamburg


- Beratung an der Schnittstelle zwischen Technologie und Recht
- Fokus auf innovative Technologien wie Legal Tech und Künstliche Intelligenz
- Starker Fokus auf anwendungsorientierte Rechtsberatung
- Beratung von Unternehmen der öffentlichen Hand bei Fragen der Digitalisierung und dem Einsatz von Künstlicher Intelligenz