AI Act und Reallabore

Neue Erprobungsmöglichkeiten für KI mit der KI -Verordnung?

10. September 2024

Alessandro Blank
KI Bundesverband

Der KI Bundesverband

Der KI Bundesverband setzt sich zusammen aus knapp 450 Innovativen:

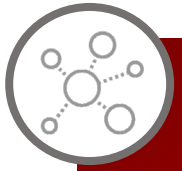
- KMUs
- Start-ups
- Expert:innen

bei denen die **Entwicklung und Anwendung von Technologien** auf **Basis von Künstlicher Intelligenz** im Fokus steht.

Damit sind wir **Deutschlands größtes KI Unternehmer:innen -Netzwerk** .

Politische Stimme

Wir stehen im regen Austausch mit politischen Entscheidungsträgern und setzen die Themen von KI - Entrepreneuren auf die politische Agenda.



Befähiger & Vernetzer

Wir ermöglichen einen Wissens - und Erfahrungsaustausch unter KI -Unternehmerinnen und Unternehmern und bieten die Plattform für den Ausbau eures Netzwerks.

Innovationstreiber

Wir machen KI-Technologie erfassbar und tragen Innovation in die etablierte Wirtschaft.

Überblick

1. Der AI Act in Kürze
2. Reallabore im AI Act
3. Regulatory Sandboxes im AI Act: Eine Einordnung

Der AI Act in Kürze

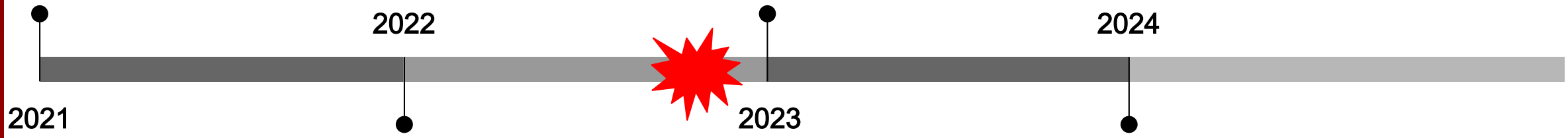
Entstehung der ersten KI -Verordnung der EU

21. April 2021
EU-Kommission publiziert ersten Entwurf des AI Acts

29. November 2021
Veröffentlichung 1. Kompromisstext durch Council

14. Juni 2023
Europäisches Parlament verabschiedet gemeinsame Position

9. Dezember 2023
Trilog -Parteien einigen sich auf vorläufiges politisches Agreement



20. April 2022
Veröffentlichung 1. Kompromisstext durch Council

13. Mai 2022
Französische Ratspräsidentschaft präsentiert Vorschlag zur Regulierung von GPAI

6. Dezember 2022
Rat der Europäischen Union verabschiedet gemeinsame Position

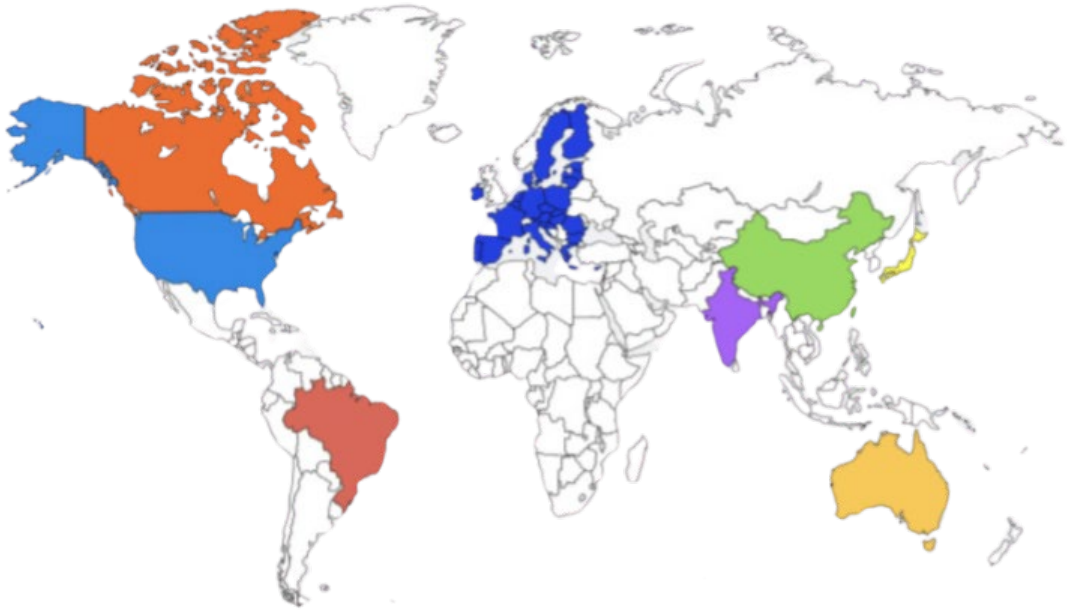
13. März 2024
Verabschiedung im Europäischen Parlament

21. Mai 2024
Verabschiedung durch den Rat der Europäischen Union

12. Juli 2024
Eintragung des AI Acts in das offizielle Journal der EU

1. August 2024
Inkrafttreten des AI Acts

Globale Einordnung



- **EU** AI Act
- **US** Executive Order 14110
- **Canada** AU and Data Act Bill-C27)
- **China** AI Governance Framework
- Digital **India** Act (Gesetzentwurf)
- **Brazil** AI Strategy (Gesetzentwurf)
- **Japan** AI Strategy (Gesetzentwurf)
- **Australian** Safe and Responsible AI (Anhörung)
- **Singapore** Model AI Governance Framework

→ Der **EU AI Act** ist die **weltweit erste umfassende** und horizontale **KI-Regulierung** inmitten einer globalen KI-Regulierungswelle in den meisten Industrieländern.

Der AI Act in Kürze

Was ist der AI Act?

Einheitlicher rechtlicher Rahmen für die Entwicklung, das Inverkehrbringen und die Nutzung von KI-Systemen in der EU auf der Grundlage eines risikobasierten Ansatzes

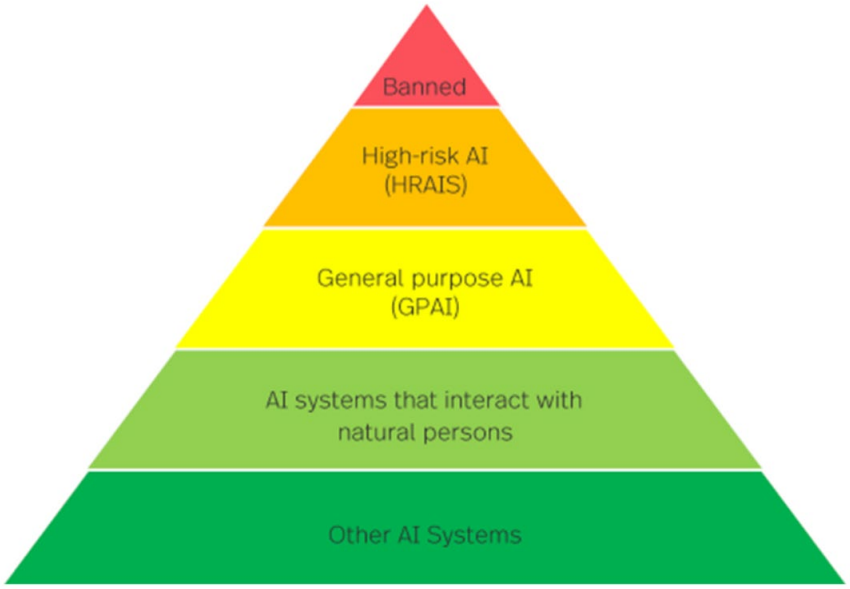
Wen betrifft der AI Act?

- Alle Akteure entlang der KI-Wertschöpfungskette, insbesondere Anbieter ("provider") und Anwender/Betreiber ("deployer")
- Extraterritoriale Wirkung - ggf. auch Anbieter und Anwender mit Sitz außerhalb der EU

Für wen gilt die Regulierung nicht?

- "Free and open source" (FOS) KI-Systeme/-Modelle
  (Ausnahme von der Ausnahme: wenn nicht für Hochrisiko-Zwecke/als Komponenten in Hochrisiko-Systemen verwendet)
- Systeme ausschließlich für militärische oder Verteidigungszwecke
- Systeme ausschließlich für wissenschaftliche Forschung und Entwicklung

Eine Risikopyramide als Grundlage



Grafik: Eigene Darstellung

Verbote:

- *Social Scoring*
- *Predictive Policing* (bestimmte Anwendungen)
- Emotionserkennung am Arbeitsplatz/in Bildungseinrichtungen
- Gesichtserkennung durch ungezieltes *Scraping* von Gesichtsbildern

High risk

General Purpose AI:

- Unterschiedliche Anforderungen für "General Purpose AI **with** or **without systemic risk** "

Limited risk

Other AI Systems:

- keine Auflagen, freiwillige Verhaltensregeln (Codes of Conduct)

Limited Risk vs. High Risk

Limited Risk = KI-Systeme mit begrenztem Risiko für die Rechte oder die Sicherheit von EU-Bürger:innen

Welche KI -Systeme sind "limited risk"?

- KI-Systeme, die mit Menschen interagieren (z.B. Chatbots)
- KI-Systeme, die Inhalte (Bild, Audio, Video, Text) generieren oder manipulieren (z.B. Deepfakes)

Anforderungen "limited risk"

im Wesentlichen Transparenzanforderungen:

- Kennzeichnung (*Labeling/Watermarking*) synthetischer Inhalte, auch in maschinenlesbarer Form
- Nutzer:innen müssen informiert werden, wenn diese Systeme verwendet werden bzw. wenn sie mit diesen Systemen interagieren

Limited Risk vs. **High Risk**

High Risk = KI-Systeme, die das Potenzial haben, Gesundheit, Sicherheit, Grundrechte, Umwelt, Demokratie und Rechtsstaatlichkeit in der EU erheblich zu beeinträchtigen

Welche KI -Systeme sind "high risk"?

- Auflistung von Hochrisikobereichen gemäß ANNEX II und ANNEX III
- "Filtersystem": nicht alle Anwendungen in Hochrisikobereichen unterliegen automatisch den Auflagen für Hochrisiko-KI-Systeme

Anforderungen "high risk"

strenge Marktzugangsvoraussetzungen (Zertifizierung/CE-Kennzeichnung) für Anbieter

- Risikomanagement
- Data Governance
- menschliche Aufsicht
- Transparenz
- Robustheit, Genauigkeit, Cybersicherheit

Geltungsbereich und Strafen

→ AI Act adressiert **alle Akteure entlang der KI -Wertschöpfungskette** und betrifft damit sowohl **Anbieter** als auch **Anwender** .

→ AI Act hat **extraterritoriale Wirkung,** betrifft also auch **Anbieter und Anwender außerhalb der EU**.

35 Mio. Euro / 7% des globalen Jahresumsatzes

im Falle von Verstößen gegen verbotene Applikationen

15 Mio. Euro / 3% des globalen Jahresumsatzes

bei sonstiger Nichteinhaltung von Anforderungen oder Verpflichtungen

7,5 Mio. Euro / 1.5% des globalen Jahresumsatzes

im Falle Offenlegung von falschen und irreführender Informationen gegenüber nationalen Behörden

Reallabore im AI Act

Reallabore im AI Act

Aufgabe:
Bereitstellung von Testumfeld (physisch, digital oder hybrid) zur Entwicklung und Erprobung von KI -Systemen (auch unter realen Bedingungen) in enger Abstimmung mit Aufsichtsbehörde.

Ziel:
Rechtssicherheit, Innovationsförderung KI, Sicherstellung der Einhaltung der Vorgaben der KI -VO durch Aufsicht.

→ Im AI Act werden (KI-)Reallabore als ***Regulatory Sandboxes*** bezeichnet.

Was steht im AI Act?

- Mindestens eine Regulatory Sandbox pro EU -Mitgliedstaat
- Frist für Einrichtung: 24 Monate nach Inkrafttreten des AI Act → spätestens 01. August 2026.
- "Reallabor-Plan" wird zwischen Aufsichtsbehörde und teilnehmenden Anbietern von KI-Systemen vereinbart
- Einzelheiten (Einrichtung, Entwicklung, Implementierung, Betrieb, Beaufsichtigung) werden durch Durchführungsrechtsakte der Europäischen Kommission noch festgelegt
- Verarbeitung personenbezogener Daten zulässig (DSGVO-Ausnahme) für Entwicklung bestimmter KI-Systeme, die dem öffentlichen Interesse dienen
- Erprobung von Hochrisiko-KI-Systemen unter bestimmten Voraussetzungen außerhalb von Reallaboren, d.h. unter realen Bedingungen für bis zu 12 Monate möglich
- Bevorzugter Zugang ("priority access") zum Reallabor für Start-ups und KMU mit Sitz in der EU

AI Act ist in Kraft - Wie geht es nun weiter?

- Benennung der nationalen behördlichen Aufsichtsstruktur im Rahmen eines nationalen Durchführungsgesetzes bis spätestens Anfang August 2025
- Erwartung der EU -Kommissions -Durchführungsrechtsakte im 1. Halbjahr 2025

→ Eine genaue Analyse der Ausgestaltung der Regulatory Sandboxes im AI Act ist daher zum jetzigen Zeitpunkt noch nicht möglich.

Status Quo in Deutschland

- Nationales Reallabore -Gesetz:
  - Angekündigt im Koalitionsvertrag 2021 -2025
  - Entwicklungen:
    - September 2021: BMWK veröffentlicht Konzept für ein Reallabore -Gesetz (vor Bundestagswahl 2021)
    - Mai 2023: Bund -Länder -Arbeitskreis Reallabore eingesetzt
    - Juli 2023: BMWK veröffentlicht Grünbuch Reallabore und startet öffentliche Konsultation
  - Status quo: Konsultationsbeiträge werden aktuell mit den zuständigen Ressorts diskutiert, Referentenentwurf geplant für “Sommer 2024”
- Es gibt schon laufende KI -Reallabore → alle keine Regulatory Sandboxes, d.h. nicht von Aufsichtsbehörden eingerichtet und nicht mit Befreiung von regulatorischen Anforderungen verbunden
  - Z.B. SmartFactoryOWL (seit 2016) in NRW

Regulatory Sandboxes im AI Act

Eine Einordnung

- Sind Regulatory Sandboxes eine innovationsfördernde Maßnahme?
- Welche Vor- und Nachteile ergeben sich für ein KI -Unternehmen aus der Teilnahme an einer Regulatory Sandbox?
- Wie sollen Regulatory Sandboxes nach dem KI -Gesetz ausgestaltet sein?
- Bewerben sich Unternehmen mit einzelnen KI -Anwendungsfällen, verschiedenen Anwendungsfällen in einer bestimmten Branche/Sektor oder als ganzes Unternehmen für die Regulatory Sandbox?
- usw.

Mögliche Herausforderungen

- **Wettbewerbsnachteile für teilnehmende KI -Unternehmen** , da (unnötigerweise?) frühzeitig im Visier der Aufsichtsbehörden
- **Keine Vorteile durch Teilnahme** z.B. beim Haftungsschutz durch haftungsrechtliche Gleichbehandlung von KI -Systemen in den Regulatory Sandboxes und auf dem Markt
- Generell: **Fehlende Anreize zur Teilnahme** an Regulatory Sandboxes
- Je nach Ausgestaltung der Regulatory Sandboxes: **Komplexe Strukturen, viel Bürokratie,** etc.

Daher ist wichtig: Ein wesentlicher Anreiz zur Teilnahme an KI -Reallaboren darf sich in der Praxis nicht ins Gegenteil verkehren und zum Flaschenhals für die gesamte Umsetzung des AI Acts werden.

Was braucht es für eine Teilnahme?

- Niedrige/keine Teilnahmekosten
- Vereinfachte Antragsverfahren für Start -ups mit begrenzten Ressourcen
- Mentoring und Beratung bei der Erfüllung regulatorischer Anforderungen
- Zugang zu gemeinsamen technischen Ressourcen und Datensätzen
- Kooperationsmöglichkeiten mit größeren Unternehmen und Forschungseinrichtungen
- Klarer Weg vom Testen im Reallabor bis zur Markteinführung
- Teilnahme an Reallaboren durch Start -up-Netzwerke und Inkubatoren fördern

Fazit

Fragen?

Herzlichen Dank!

Fragen? Dann melden Sie sich gerne bei mir!

Alessandro Blank

Public Affairs & Innovationsprojekte

alessandro.blank@ki -verband.de

+49 (0)152 34688860