EU AI Act

Grundlagen & Überblick zu den aktuellen Entwicklungen

Daniel Lisunkin

Brown Bag Session - 11.12.2025

1. Überblick & Relevanz des AI Acts

- **Einführung:** trat am 1. August 2024 in Kraft
- **Ziele:**
  Förderung verantwortungsvoller AI-Entwicklung und -Einsatz in der EU
- **Risikobasierter Ansatz:**
  Unterscheidung zwischen minimalem, spezifischem, hohem und unakzeptablem Risiko
- **Gestaffelte Einführung:**
  - Übergangszeitraum von 2 Jahren
  - Ab 2. Februar 2025: Verbot bestimmter KI-Praktiken
  - Ab 2. August 2025: Regulierung von GPAI-Systemen
  - Ab 2. August 2026: Die meisten der restlichen Bestimmungen werden angewendet
    - **Änderungsvorschlag EU-Kommission:** Verschiebung auf **12/27**

https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en

1. Überblick & Relevanz des AI Acts

„Ein **maschinengestütztes System**, das für einen in unterschiedlichem Grade **autonomen Betrieb** ausgelegt ist und nach seiner Betriebsaufnahme **anpassungsfähig** sein kann. Es **leitet** aus den erhaltenen Eingaben für explizite oder implizite Ziele **ab**, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können.“

https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en

1. Überblick & Relevanz des AI Acts

- **Merkmale der KI Definition:**
  - **Maschinenbasiert** = nicht rein manuell, sondern technisch
  - **Autonomie** = zumindest zT unabhängig vom Menschen
  - **Adaptivität** = Anpassungs- & Lernfähig
  - **Schlussfolgerungsfähigkeit (Inferencing)** = verarbeitet Input und leitet eigenständig Output ab
  - **Zielgerichtetheit** = Output dienen expliziten/impliziten Zielen und können reale/virtuelle Umgebung beeinflussen
- **Beispiele**:
  - Maschinelles Lernen
  - Selbst logikbasierte Systeme, die aus Daten Muster ableiten
  - Generative KI

https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en

1. Überblick & Relevanz des AI Acts

- **Anwendungsbereich:**
  - **Alle, die KI-Systeme in der EU herstellen, entwickeln, vertreiben, einführen oder nutzen** – unabhängig davon, ob das Unternehmen oder die Organisation ihren Sitz in der EU hat oder nicht.
  - Unternehmen, Start-Ups, öffentliche Institutionen …
  - Sowohl Anbieter (Hersteller, Entwickler) als auch Nutzer (Betreiber, Anwender)
- **Ausnahmen:**
  - KI für ausschließlich militärische/verteidigungspolitische Zwecke
  - zT Forschung und Innovation
  - zT Open-Source-KI
  - private, rein persönliche Nutzung

https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en

aric

2. Risikoklassifizierung

In welche Kategorie fällt mein System?

1. Unannehmbares Risiko

- KI Systeme, die fundamentale Rechte verletzen
- Rechtsfolge: Verboten
- Beispiele: Social Scoring, Beeinflussung von Menschen, Ausnutzen von schutzwürdigen Gruppen, Biometrie

2. Hohes Risiko

- KI Systeme mit potenziell gravierenden Auswirkungen auf Sicherheit, Gesundheit oder Grundrechte
- Rechtsfolge: Strenge Auflagen
- Beispiele: Autonome Autos, Flugzeuge, Betrieb kritischer Infrastrukturen, Bildungszwecke, etc.

2. Risikoklassifizierung

In welche Kategorie fällt mein System?

3. Begrenztes Risiko

- KI Systeme, die mit Menschen interagieren oder Inhalte generieren, mit moderatem Risiko
- Rechtsfolge: Transparenzpflichten
- Beispiele: einfache Chatbots, Systeme zur Manipulation von Daten

4. Minimales Risiko

- Keine spezifischen Anforderungen
- Beispiele: Spam-Filter, automatische Textvorschläge

2. Risikoklassifizierung

Besonderheit: General Purpose AI

- KI Modelle mit allgemeinem Verwendungszweck
- zB sehr große Sprachmodelle (ChatGPT & Co)
- Annahme des systematischen Risikos
- Rechtsfolge:
  - Zusätzliche Transparenz- und Prüfpflichten, die sich nach der Leistungsfähigkeit des Modells richten

2. Risikoklassifizierung

Wie finde ich das heraus?

1. **Systematische Risikoanalyse**
   - Was ist der Zweck und Anwendungsbereich?
   - Vergleiche mit EU AI Act
2. **Checklisten und Tools**

   (Inoffizieller) Compliance Checker: https://artificialintelligenceact.eu/assessment/eu-ai-act-compliance-checker/
3. **Leitfragen zur Einordnung**
4. **Dokumentation und externe Beratung**

2. Risikoklassifizierung

3. Leitfragen zur Einordnung

- Handelt es sich um ein System, das fundamentale Rechte verletzen könnte? **(unannehmbares R)**
- Wird das System in einem sensiblen oder sicherheitskritischen Bereich eingesetzt (z. B. Medizin, Justiz, Bildung, kritische Infrastruktur)? **(hohes R)**
- Interagiert das System mit Menschen, ohne gravierende Folgen zu haben (z. B. Chatbots, Deepfakes)? **(begrenztes R)**
- Hat das System kaum Auswirkungen auf Rechte und Sicherheit (z. B. Musikempfehlungen, Spamfilter)?

2. Risikoklassifizierung

Rechtssicherheit?

- **Grundsatz:** Selbstverantwortung
- **Ausnahme:** Pflicht bei Hochrisiko-KI (aber erst 2026)
  - Diese darf nur nach einer externen Konformitätsbewertung in Verkehr gebracht werden (bei zB TÜV, DEKRA, etc)
  - Dann: EU Konformitätserklärung und CE Kennzeichen
- **Rest:** freiwillige Prüfungen/Audits möglich
  - Bieten aber aktuell keine Vorteile
  - Aktuell noch nicht mal möglich
  - Nur Momentaufnahme

3. Fristen, Gültigkeiten & Zuständigkeiten

Datum	Was gilt ab diesem Zeitpunkt
1. August **24**	- Inkrafttreten des EU AI Act. - Noch keine unmittelbaren Pflichten für Unternehmen.
2. Februar **25**	- **Verbot** von KI-Systemen mit **unannehmbarem Risiko** (z. B. Social Scoring, manipulative Systeme, bestimmte biometrische Verfahren).
2. August **25**	- Regelungen für KI-Modelle mit allgemeinem Verwendungszweck (General Purpose AI, **GPAI**) werden verbindlich. - Governance & Meldepflichten werden scharf gestellt.
2. August **26**	- Die meisten Pflichten des AI Act gelten ab jetzt; insbesondere für **Hochrisiko-KI-Systeme**. Unternehmen müssen umfassende Dokumentation vorlegen. - Definition des Annex III zu Hochrisiko-Systemen war geplant
2. Dezember **27**	- Spätestens: Definition des Annex III zu Hochrisiko-Systemen
2. August **28**	- Spätestens: Definition des Annex I zu Hochrisiko-Systemen (geregelte Produkte)

3. Fristen, Gültigkeiten & Zuständigkeiten

Behörden auf EU-Ebene:

- **EU AI Office:**
  - Zentrale europäische Behörde für Umsetzung & Überwachung, Teil der EU Kommission
  - Einrichtung mit Beschluss vom 21.02.24
  - Kann Bußgelder verhängen
- **KI-Gremium & Wissenschaftliches Beratungsforum:**
  - Gremium: Ein Vertreter je EU-Mitgliedsstaat
  - Beratungsforum: Vertreter aus allen Bereichen
  - Primär Koordination & Beratung
  - Plattform für Erfahrungsaustausch

3. Fristen, Gültigkeiten & Zuständigkeiten

Behörden in DE (nationale Ebene)

➔ Wurden zum **2. August 2025** final benannt

- **Bundesnetzagentur (BNetzA)**
  - **Marktüberwachung:**
    - Generelle Überwachung für die meisten Branchen
    - Überwacht KI-Systeme, prüft Konformität, geht Beschwerden nach und kann Maßnahmen verhängen
  - **Notifizierende Behörde:**
    - Benennung, Überwachung und Kontrolle von Konformitätsbewertungsstellen (zB Zertifizierer wie TÜV)
  - **Zentrale Anlaufstelle**

https://artificialintelligenceact.eu/implementation-timeline/

3. Fristen, Gültigkeiten & Zuständigkeiten

Behörden in DE (nationale Ebene)

➔ Wurden zum **2. August 2025** final benannt

- **Bundesnetzagentur (BNetzA)**
  ergänzend werden eingerichtet:
  - **Koordinierungs- und Kompetenzzentrum (KoKIVO)**
  - **AI Regulatory Sandbox**

https://artificialintelligenceact.eu/implementation-timeline/

3. Fristen, Gültigkeiten & Zuständigkeiten

Behörden in DE (nationale Ebene)

➔ Wurden zum **2. August 2025** final benannt

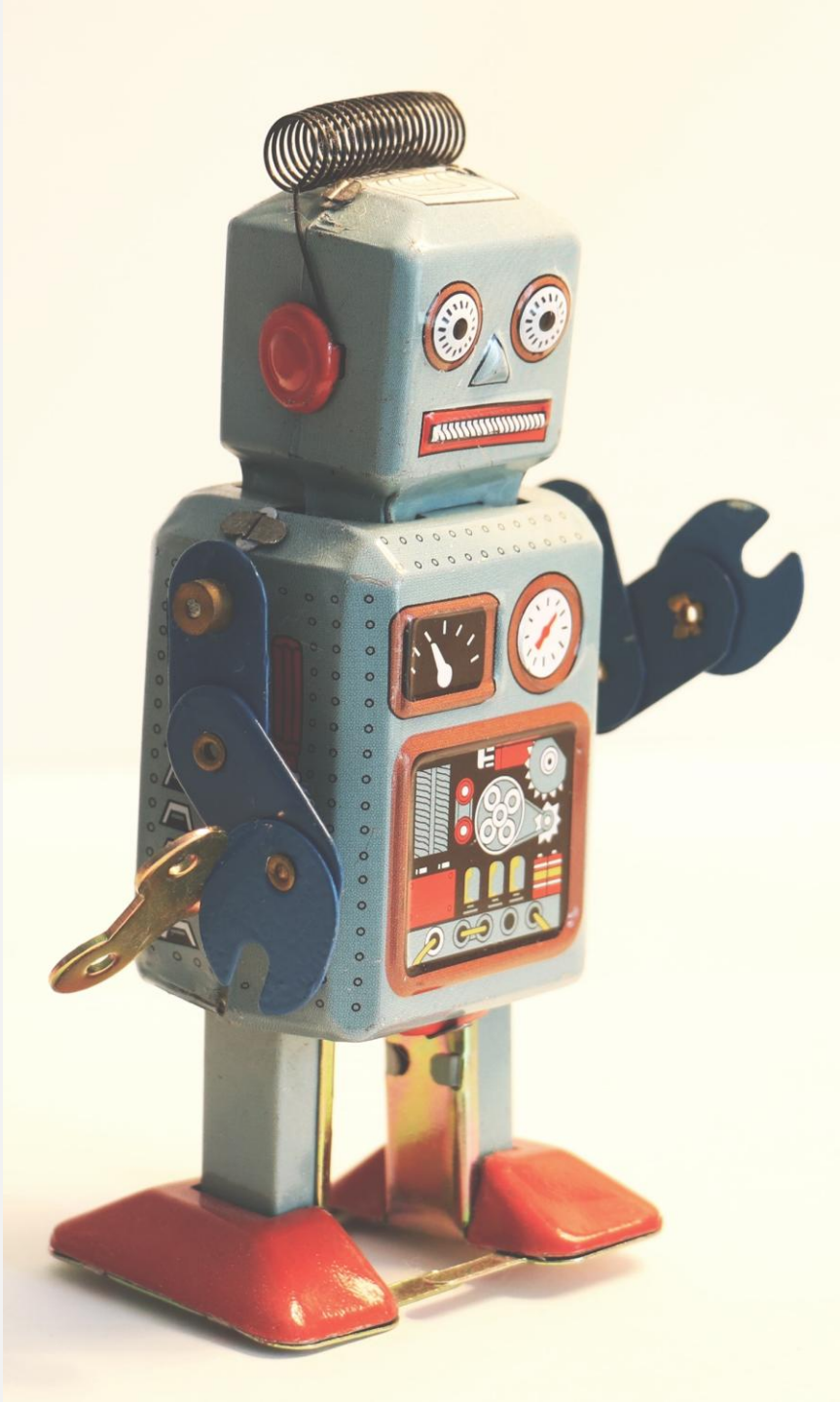
- **BaFin**
  - **Marktüberwachung:**
    - Sektorspezifische Überwachung für Finanzen
    - Überwacht KI-Systeme, prüft Konformität, geht Beschwerden nach und kann Maßnahmen verhängen
- **Weitere sektorale Behörden folgen**
  - Justiz, Bildung, etc.

https://artificialintelligenceact.eu/implementation-timeline/

4. Aktuelle Entwicklungen:

Verschiebungen der Deadlines

- **02/25:** Verbot von verbotenen KI-Praktiken ✅
- **08/25:** GPAI-Governance ✅
- **08/25:** Annex III ⚠️
  - Kommission schlägt Verschiebung bis **12/27** vor
  - Grund: Harmonisierte Standards noch nicht fertig
  - Max. Verlängerung: 16 Monate
- **08/27:** Annex I ⚠️
  - Betrifft: Hochrisiko-KI in regulierten Produkten
  - Kommission schlägt Verschiebung bis **08/28** vor
  - Max. Verlängerung: 24 Monate

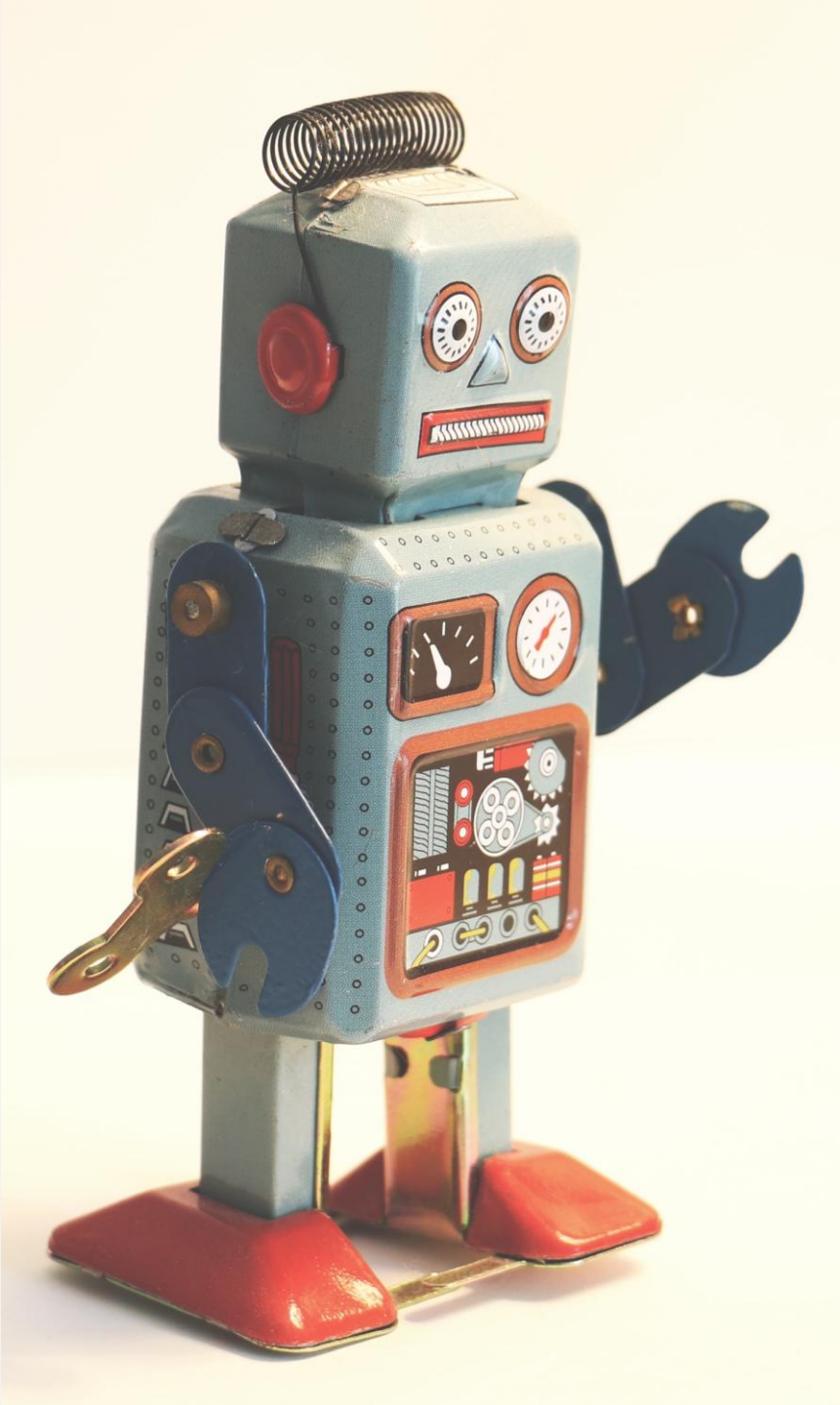


4. Aktuelle Entwicklungen:

Compliance-Status: Deutschland

1. **Behörden designiert** ✅
2. **Umsetzungsgesetz** ⚠️
   - Entwurf vorgestellt (11.09.25)
   - Status: im legislativen Prozess
3. **Infrastruktur** ⚠️
   - Aufbau läuft
   - AI Service Desk (BNetzA) seit 07/25 aktiv

Prognose: DE orientiert sich an EU-Fristen, hat Verzögerungen bei Gesetz



5. Ressourcen und Links

- artificialintelligenceact.eu/de
- netzpolitik.org
- https://artificialintelligenceact.eu/assessment/eu-ai-act-compliance-checker/
- BNetzA AI Service Desk: https://www.bundesnetzagentur.de/AI
- Offizielle Timeline: https://artificialintelligenceact.eu/implementation-timeline/