JAIKIN

WHITEPAPER

EU AI Act

Der vollständige Referenzleitfaden zur Verordnung (EU) 2024/1689

AUTEUR JAIKIN

DATE Janvier 2026

PAGES 22

VERSION 1.0

Table des matières

01 Introduction 3

02 Chronologie et Cadre Juridique 4

03 Classification des Risques 6

04 Modèles d'IA à Usage Général (GPAI) 9

05 Obligations par Acteur 11

06 Gouvernance et Enforcement 13

07 Sanctions et Pénalités 14

08 Impact Sectoriel 15

09 Comparaison Internationale 17

10 Recommandations Pratiques 18

11 Conclusion 20

12 Annexes 21

1. Einführung

1.1 Kontext: Warum die Europäische Union KI reguliert

Künstliche Intelligenz verändert unsere Gesellschaften, Volkswirtschaften und Lebensweisen grundlegend. Angesichts dieser technologischen Revolution hat sich die Europäische Union entschieden, einen harmonisierten Rechtsrahmen zu schaffen, anstatt jeden Mitgliedstaat einzeln gesetzgeberisch tätig werden zu lassen.

Dieser Ansatz steht im Einklang mit der europäischen Digitalstrategie, die die Datenschutz-Grundverordnung (DSGVO), das Gesetz über digitale Dienste (DSA) und das Gesetz über digitale Märkte (DMA) umfasst.

Die Hauptmotive für diese Regulierung sind:

- **Schutz der Grundrechte**: Verhinderung algorithmischer Diskriminierung und Schutz der Menschenwürde
- **Sicherheit von Personen**: Gewährleistung, dass in Produkte integrierte KI-Systeme keine Gefahr für Gesundheit und Sicherheit darstellen
- **Harmonisierung des Binnenmarktes**: Schaffung eines einheitlichen Rahmens für die 27 Mitgliedstaaten zur Vermeidung regulatorischer Fragmentierung
- **Europäische Wettbewerbsfähigkeit**: Etablierung eines globalen Standards, den die EU exportieren kann („Brüssel-Effekt")

1.2 Ziele der Verordnung

Der AI Act verfolgt mehrere sich ergänzende Ziele, die in den Erwägungsgründen ausdrücklich genannt werden:

1.3 Geografischer und extraterritorialer Geltungsbereich

Der AI Act hat einen **erheblichen extraterritorialen Geltungsbereich**. Er gilt für:

1. **Anbieter**, die in der EU oder in einem Drittland niedergelassen sind und KI-Systeme in der Union in Verkehr bringen oder in Betrieb nehmen
2. **Betreiber** von KI-Systemen mit Sitz in der Union
3. **Anbieter und Betreiber** in Drittländern, wenn die Ergebnisse des KI-Systems in der Union verwendet werden
4. **Importeure und Händler** von KI-Systemen
5. **Produkthersteller**, die ein KI-System mit ihrem Produkt unter eigenem Namen oder eigener Marke in Verkehr bringen

> *„Jedes Unternehmen, unabhängig von seinem Standort, das KI-Systeme für den europäischen Markt vermarktet oder dessen Ergebnisse in der EU verwendet werden, muss den AI Act einhalten."*

2. Zeitplan und Rechtsrahmen

2.1 Entstehung der Verordnung (2021-2024)

Die Entwicklung des AI Acts war ein mehrjähriger Gesetzgebungsprozess:

2.2 Gestaffelter Umsetzungszeitplan

Die Verordnung sieht eine **gestaffelte Umsetzung** über drei Jahre vor, damit sich die Akteure schrittweise anpassen können:

DATUM	ZEITRAHMEN	ANWENDBARE BESTIMMUNGEN
2. Februar 2025	6 Monate	**Verbotene Praktiken** (Artikel 5) **KI-Kompetenz** (Artikel 4)
2. August 2025	12 Monate	**GPAI-Pflichten** (Kapitel V) **Governance**: Benennung nationaler Behörden Verhaltenskodizes für GPAI-Modelle
2. August 2026	24 Monate	**Hochrisiko-Systeme** (Anhang III) **Anbieter- und Betreiberpflichten** **Sanktionsregime** (Artikel 99) Mehrheit der Bestimmungen
2. August 2027	36 Monate	**Hochrisiko-Systeme in regulierten Produkten** (Anhang I) Medizinprodukte, Maschinen, Fahrzeuge, Flugzeuge Vollständige GPAI-Konformität (Modelle vor August 2025)
31. Dez. 2030	6+ Jahre	**Großflächige IT-Systeme** (Anhang X) Bestehende Systeme, die vor diesem Datum in Verkehr gebracht wurden

3. Risikoklassifizierung

Der AI Act führt einen **risikobasierten Pyramidenansatz** ein. Vier Stufen werden definiert, jede mit verhältnismäßigen Pflichten:

> Unannehmbares Risiko
> VERBOTEN

Hohes Risiko
REGULIERT
Begrenztes Risiko
TRANSPARENZ

> Minimales Risiko
> NICHT REGULIERT

3.1 Unannehmbares Risiko – Verbotene Praktiken (Artikel 5)

Die Verordnung **verbietet** acht Kategorien von KI-Systemen, die als Verstoß gegen Grundrechte oder Menschenwürde gelten. Diese Verbote sind **seit dem 2. Februar 2025 in Kraft**.

3.2 Hohes Risiko – Regulierte Systeme (Artikel 6-49)

Hochrisiko-KI-Systeme stellen den Kern der Verordnung dar. Sie unterliegen **strengen Anforderungen** vor dem Inverkehrbringen und während ihres gesamten Lebenszyklus.

KATEGORIE 1: SICHERHEITSKOMPONENTEN REGULIERTER PRODUKTE (ANHANG I)

KI-Systeme, die eine **Sicherheitskomponente** eines Produkts darstellen, das unter die Harmonisierungsrechtsvorschriften der Union fällt, darunter:

- Maschinen und Industrieausrüstung
- Spielzeug
- Aufzüge
- Druckgeräte
- Medizinprodukte und In-vitro-Diagnostika
- Fahrzeuge (Typgenehmigung)
- Luftfahrzeuge und Flugverkehrsmanagementsysteme
- Schiffsausrüstung
- Eisenbahnausrüstung

KATEGORIE 2: SENSIBLE BEREICHE (ANHANG III)

KI-Systeme, die in **Bereichen mit hohem Einfluss** auf die Grundrechte eingesetzt werden:

3.3 Begrenztes Risiko – Transparenzpflichten (Artikel 50)

Bestimmte KI-Systeme bergen ein **Täuschungsrisiko**, gelten aber nicht als hochriskant. Sie unterliegen **Transparenzpflichten**:

- **Chatbots und Konversationsagenten**: Nutzer müssen darüber informiert werden, dass sie mit einer KI interagieren (es sei denn, dies ist aus den Umständen offensichtlich)
- **Emotionserkennungssysteme**: Information der betroffenen Personen (außer bei verbotenen Fällen)
- **Biometrische Kategorisierungssysteme**: Information der Personen (außer bei verbotenen Fällen)

- **Deepfakes und generierte Inhalte**: Deutliche Kennzeichnung, dass der Inhalt (Bild, Audio, Video, Text) von KI erzeugt oder manipuliert wurde

3.4 Minimales Risiko – Nicht reguliert

Die große Mehrheit der KI-Systeme fällt in diese Kategorie und ist vom AI Act **nicht spezifisch reguliert**. Beispiele:

- KI-gestützte Videospiele
- Spam-Filter
- Inhaltsempfehlungssysteme
- Übersetzungsassistenten
- Industrielle Optimierungstools

4. KI-Modelle für allgemeine Zwecke (GPAI)

KI-Modelle für allgemeine Zwecke (General-Purpose AI oder GPAI) sind in einem eigenen Kapitel (Kapitel V) geregelt, das während der abschließenden Verhandlungen hinzugefügt wurde, um auf die Entstehung von Systemen wie ChatGPT, Claude, Gemini oder DALL-E zu reagieren.

4.1 Definition

Ein GPAI-Modell wird definiert als:

> *„Ein KI-Modell, auch wenn es mit einer großen Datenmenge unter Verwendung von Selbstüberwachung im großen Maßstab trainiert wurde, das eine erhebliche Allgemeinheit aufweist und in der Lage ist, eine breite Palette unterschiedlicher Aufgaben kompetent auszuführen, unabhängig davon, wie das Modell in Verkehr gebracht wird, und das in eine Vielzahl von nachgelagerten Systemen oder Anwendungen integriert werden kann."*

Beispiele: GPT-4, Claude, Gemini, LLaMA, Mistral, DALL-E, Midjourney, Stable Diffusion.

4.2 Pflichten der GPAI-Modellanbieter

Alle GPAI-Modellanbieter müssen **ab dem 2. August 2025**:

1. **Technische Dokumentation erstellen und pflegen** über das Modell und seinen Trainingsprozess
2. **Eine Compliance-Richtlinie erstellen und dokumentieren** zum EU-Urheberrecht
3. **Eine detaillierte Zusammenfassung veröffentlichen** der für das Training verwendeten Inhalte
4. **Informationen und Dokumentation bereitstellen** an nachgelagerte Anbieter, die das Modell integrieren
5. **Einen Vertreter benennen** in der Union (für Nicht-EU-Anbieter)

4.3 GPAI-Modelle mit systemischem Risiko

Ein GPAI-Modell birgt ein **systemisches Risiko**, wenn:

Anbieter von GPAI-Modellen mit systemischem Risiko müssen **zusätzlich** zu den allgemeinen Pflichten:

- **Modellbewertungen durchführen** gemäß standardisierten Protokollen und Tools
- **Adversarial Testing durchführen** zur Identifizierung und Minderung systemischer Risiken
- **Schwerwiegende Vorfälle verfolgen, dokumentieren und melden** an das AI Office und die nationalen Behörden

- **Angemessene Cybersicherheit gewährleisten** für das Modell und seine Infrastruktur
- **Die Kommission innerhalb von 2 Wochen benachrichtigen**, wenn ihr Modell die Schwelle für systemisches Risiko erreicht

5. Pflichten nach Akteuren

Der AI Act unterscheidet mehrere Kategorien von Akteuren in der KI-Wertschöpfungskette, jede mit spezifischen Pflichten.

5.1 Anbieter (Entwickler)

Anbieter sind natürliche oder juristische Personen, die ein KI-System entwickeln oder entwickeln lassen, um es unter eigenem Namen oder eigener Marke in Verkehr zu bringen oder in Betrieb zu nehmen.

PFLICHTEN FÜR HOCHRISIKO-SYSTEME:

1. **Risikomanagementsystem (Artikel 9)**
   Einrichtung, Umsetzung, Dokumentation und Aufrechterhaltung eines Risikomanagementsystems während des gesamten Lebenszyklus des KI-Systems.

2. **Datengovernance (Artikel 10)**
   Sicherstellung, dass Trainings-, Validierungs- und Testdatensätze relevant, repräsentativ, fehlerfrei und vollständig sind.

3. **Technische Dokumentation (Artikel 11)**
   Erstellung einer technischen Dokumentation, die die Konformität des Systems vor dem Inverkehrbringen nachweist.

4. **Protokollierung (Artikel 12)**
   Gestaltung des Systems zur automatischen Aufzeichnung von Ereignissen (Logs) während seines gesamten Betriebs.

5. **Transparenz (Artikel 13)**
   Gestaltung des Systems, um Betreibern das Verständnis seiner Funktionsweise und die Interpretation seiner Ergebnisse zu ermöglichen.

6. **Menschliche Aufsicht (Artikel 14)**
   Gestaltung des Systems zur Ermöglichung einer wirksamen menschlichen Aufsicht während seiner Nutzung.

5.2 Betreiber (Nutzer)

Betreiber sind natürliche oder juristische Personen, die ein KI-System in eigener Verantwortung nutzen (außer bei persönlicher, nicht beruflicher Nutzung).

HAUPTPFLICHTEN:

- **Konforme Nutzung**: Nutzung des Systems gemäß den vom Anbieter bereitgestellten Anweisungen
- **Menschliche Aufsicht**: Sicherstellung, dass die menschliche Aufsicht von kompetenten und befugten Personen ausgeübt wird
- **Eingabedaten**: Sicherstellung, dass die Eingabedaten für den Zweck des Systems relevant sind

- **Betriebsüberwachung**: Überwachung des Systembetriebs und Aussetzung der Nutzung bei Fehlfunktionen
- **Protokollaufbewahrung**: Aufbewahrung automatisch generierter Protokolle (mindestens 6 Monate)
- **Information der Personen**: Information der betroffenen Personen, dass sie einer Entscheidung durch ein Hochrisiko-System unterliegen
- **Grundrechte-Folgenabschätzung**: Durchführung einer Folgenabschätzung vor der Inbetriebnahme (für bestimmte Betreiber)

5.3 Bereichsübergreifende Pflicht: KI-Kompetenz (Artikel 4)

Seit dem 2. Februar 2025 in Kraft, gilt die KI-Kompetenzpflicht für alle Anbieter und Betreiber:

6. Governance und Durchsetzung

Der AI Act etabliert eine **mehrstufige Governance-Architektur**, die europäische und nationale Aufsicht kombiniert.

6.1 Auf europäischer Ebene

DAS AI OFFICE

Innerhalb der Europäischen Kommission eingerichtet, ist das AI Office verantwortlich für:

- Überwachung von GPAI-Modellen und Modellen mit systemischem Risiko
- Entwicklung von Leitlinien und Verhaltenskodizes
- Koordination mit nationalen Behörden
- Durchsetzung der Regeln für GPAI-Modellanbieter

DAS EUROPÄISCHE KI-GREMIUM (AI BOARD)

Zusammengesetzt aus Vertretern der Mitgliedstaaten:

- Berät und unterstützt die Kommission
- Trägt zur einheitlichen Anwendung der Verordnung bei
- Koordiniert die nationalen Behörden
- Gibt Empfehlungen und Stellungnahmen ab

7. Sanktionen und Strafen

Der AI Act sieht ein **gestuftes Verwaltungssanktionssystem** vor (Artikel 99), anwendbar ab dem 2. August 2025.

7.1 Bußgeldstruktur

7.2 Weitere Konsequenzen

Neben Bußgeldern können die Behörden:

- **Rücknahme vom Markt anordnen** oder Rückruf eines nicht konformen Systems
- **Inbetriebnahme verbieten** eines KI-Systems
- **Korrekturmaßnahmen verlangen** innerhalb einer festgelegten Frist
- **Entscheidungen über Nichtkonformität veröffentlichen** (Name and Shame)

8. Sektorale Auswirkungen

Der AI Act hat differenzierte Auswirkungen auf verschiedene Branchen. Dieser Abschnitt analysiert die vier am stärksten betroffenen Sektoren.

8.1 Personalwesen und Rekrutierung

Der HR-Sektor ist vom AI Act **besonders betroffen**, da die meisten KI-Anwendungen in diesem Bereich als **Hochrisiko** eingestuft werden.

HOCHRISIKO-SYSTEME:

- Lebenslauf-Screening und Scoring-Tools
- Bewerber-Stellen-Matching-Systeme
- Videointerview-Analyse-Tools
- Leistungsbewertungssysteme
- Aufgaben- und Zeitplanzuweisungstools
- Beförderungs- oder Kündigungsentscheidungssysteme

8.2 Gesundheitswesen und Medizinprodukte

Der Gesundheitssektor kombiniert zwei Regulierungsrahmen: den AI Act und die **Medizinprodukteverordnung** (MDR 2017/745).

8.3 Finanzen und Versicherungen

Der Finanzsektor nutzt KI intensiv für Risikobewertungen und fällt damit in den Hochrisikobereich.

8.4 Bildung

KI in der Bildung wird als **Hochrisiko** eingestuft, da sie potenzielle Auswirkungen auf die Lebensläufe der Lernenden hat.

9. Internationaler Vergleich

Der AI Act ist Teil eines **globalen Wettlaufs um die Regulierung von KI**. Die Ansätze variieren erheblich je nach Rechtsordnung.

10. Praktische Empfehlungen

Dieser Abschnitt präsentiert eine **Compliance-Checkliste** für Organisationen, die sich auf den AI Act vorbereiten.

10.1 Sofortmaßnahmen (Bereits anwendbar)

- [ ] Audit verbotener Praktiken
  Überprüfen, dass kein verbotenes KI-System (Social Scoring, Emotionserkennung am Arbeitsplatz usw.) verwendet wird.

- [ ] KI-Kompetenzprogramm
  Schulung des Personals, das KI-Systeme nutzt oder beaufsichtigt.

10.2 Kurzfristige Maßnahmen (Vor August 2026)

- [ ] KI-System-Inventar
  Katalogisierung aller von der Organisation genutzten oder entwickelten KI-Systeme.

- [ ] Risikoklassifizierung
  Klassifizierung jedes Systems gemäß den AI Act-Kategorien (verboten, Hochrisiko, begrenzt, minimal).

- [ ] Gap-Analyse
  Identifizierung von Lücken zwischen aktuellen Praktiken und AI Act-Anforderungen.

11. Fazit

Die Verordnung (EU) 2024/1689 über künstliche Intelligenz stellt einen **bedeutenden regulatorischen Fortschritt** auf globaler Ebene dar. Als erster umfassender Rechtsrahmen für KI schafft sie ein Gleichgewicht zwischen dem Schutz der Grundrechte und der Bewahrung von Innovation.

Wichtigste Erkenntnisse

1. **Risikobasierter Ansatz**: Die Pflichten sind proportional zum Risikoniveau des KI-Systems
2. **Gestaffelte Umsetzung**: Von Februar 2025 (verbotene Praktiken) bis Dezember 2030 (großflächige IT-Systeme)
3. **Extraterritorialer Geltungsbereich**: Jede Organisation, die Nutzer in der EU betrifft, ist erfasst
4. **Erhebliche Sanktionen**: Bis zu 35 Millionen Euro oder 7% des weltweiten Umsatzes
5. **Mehrstufige Governance**: Koordination zwischen dem Europäischen KI-Büro und den nationalen Behörden

> *„Der AI Act ist kein Selbstzweck, sondern der Beginn eines Prozesses zur Regulierung künstlicher Intelligenz, der sich mit der Technologie weiterentwickeln wird."*

12. Anhänge

Glossar

KI-System
Ein maschinenbasiertes System, das für den Betrieb mit unterschiedlichen Autonomiegraden ausgelegt ist, das nach der Einführung Anpassungsfähigkeit aufweisen kann und das für explizite oder implizite Ziele aus den erhaltenen Eingaben ableitet, wie Ausgaben wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erzeugt werden.
Anbieter
Eine natürliche oder juristische Person, die ein KI-System oder ein GPAI-Modell entwickelt oder entwickeln lässt und es unter eigenem Namen oder eigener Marke in Verkehr bringt oder das KI-System in Betrieb nimmt.
Betreiber

Eine natürliche oder juristische Person, die ein KI-System in eigener Verantwortung nutzt, außer wenn das KI-System im Rahmen einer persönlichen, nicht beruflichen Tätigkeit genutzt wird.
GPAI (General-Purpose AI)
Ein KI-Modell für allgemeine Zwecke, das in der Lage ist, eine breite Palette unterschiedlicher Aufgaben kompetent auszuführen, unabhängig davon, wie es in Verkehr gebracht wird.
Systemisches Risiko
Ein Risiko, das spezifisch für die hochwirksamen Fähigkeiten von GPAI-Modellen ist und erhebliche Auswirkungen auf den Unionsmarkt aufgrund ihrer Reichweite oder tatsächlicher oder vernünftigerweise vorhersehbarer negativer Auswirkungen auf die öffentliche Gesundheit, Sicherheit, Grundrechte oder die Gesellschaft hat.
Regulatorische Sandbox
Ein kontrollierter Rahmen, der von einer zuständigen Behörde eingerichtet wird und die Entwicklung, das Training und die Validierung innovativer KI-Systeme für einen begrenzten Zeitraum vor dem Inverkehrbringen ermöglicht.

Offizielle Ressourcen

- Offizieller Text der Verordnung (EUR-Lex)
- EU AI Act Portal (Analysen und Zusammenfassungen)
- Europäische Kommission - KI-Rechtsrahmen
- Offizieller Umsetzungszeitplan

Zusammenfassender Zeitplan

Dokument: Whitepaper – EU AI Act: Der vollständige Referenzleitfaden

Version: 1.0

Veröffentlichungsdatum: 20. Januar 2026

Autor: JAIKIN

Dieses Dokument dient nur zu Informationszwecken und stellt keine Rechtsberatung dar. Bei spezifischen Fragen zur AI Act-Konformität wenden Sie sich bitte an einen qualifizierten Rechtsberater.