Der AI Act im Überblick

Die EU-KI-Verordnung verständlich erklärt
für deutsche Unternehmen

In diesem Whitepaper:

- Was ist der AI Act und warum gibt es ihn?
- Das Risikoklassifizierungssystem verstehen
- Welche KI-Praktiken sind verboten?
- Pflichten für Betreiber von KI-Systemen
- Fristen, Sanktionen und nächste Schritte

AI-Legal-Flow GmbH
www.ai-legal-flow.de

Stand: Dezember 2025

Inhaltsverzeichnis

Einführung: Was ist der AI Act?

Der **AI Act** (offiziell: Verordnung über künstliche Intelligenz) ist das weltweit erste umfassende Gesetz zur Regulierung von künstlicher Intelligenz. Er wurde am 13. Juni 2024 vom Europäischen Parlament verabschiedet und trat am **1. August 2024** in Kraft.

Warum ein KI-Gesetz?

Die EU verfolgt mit dem AI Act mehrere Ziele:

- **Schutz von Grundrechten:** KI soll Menschen nicht diskriminieren oder manipulieren
- **Sicherheit:** KI-Systeme sollen sicher und zuverlässig funktionieren
- **Vertrauen:** Bürger und Unternehmen sollen KI vertrauen können
- **Innovation:** Klare Regeln sollen Rechtssicherheit für Innovationen schaffen

Für wen gilt der AI Act?

Der AI Act gilt für:

- **Anbieter** von KI-Systemen (Entwickler, Hersteller)
- **Betreiber** von KI-Systemen (Unternehmen, die KI einsetzen)
- **Importeure und Händler** von KI-Produkten
- Auch für Anbieter außerhalb der EU, wenn ihre Systeme in der EU genutzt werden

Wichtig für Unternehmen: Wenn Sie KI-Tools wie ChatGPT, Microsoft Copilot oder andere KI-Anwendungen nutzen, sind Sie ein „Betreiber“ im Sinne des AI Act – und damit reguliert.

Das Risikoklassifizierungssystem

Das Herzstück des AI Act ist ein **risikobasierter Ansatz**: Je höher das Risiko eines KI-Systems, desto strenger die Anforderungen.

Die vier Risikostufen

red!20 **Unannehmbares Risiko**	KI-Systeme, die verboten sind
orange!20 **Hohes Risiko**	KI-Systeme mit strengen Anforderungen
yellow!20 **Begrenztes Risiko**	KI-Systeme mit Transparenzpflichten
green!20 **Minimales Risiko**	KI-Systeme ohne spezifische Anforderungen

Unannehmbares Risiko: Verbotene KI-Praktiken

Folgende KI-Anwendungen sind **vollständig verboten**:

1. **Manipulative Techniken:** KI, die unterschwellig manipuliert oder Schwächen ausnutzt
2. **Social Scoring:** Bewertung von Personen basierend auf sozialem Verhalten
3. **Biometrische Echtzeit-Überwachung:** In öffentlichen Räumen (mit Ausnahmen für Strafverfolgung)
4. **Emotionserkennung:** Am Arbeitsplatz oder in Bildungseinrichtungen
5. **Biometrische Kategorisierung:** Nach sensiblen Merkmalen wie Rasse oder Religion
6. **Gesichtserkennung aus dem Internet:** Ungezielte Erfassung für Datenbanken

Hohes Risiko: Streng regulierte KI-Systeme

KI-Systeme gelten als **hochriskant**, wenn sie in sensiblen Bereichen eingesetzt werden:

- **Kritische Infrastruktur:** Energie, Verkehr, Wasserversorgung
- **Bildung:** Zugangsentscheidungen, Bewertungen
- **Beschäftigung:** Recruiting, Beförderungen, Kündigungen
- **Wesentliche Dienstleistungen:** Kreditwürdigkeit, Sozialleistungen, Versicherungen
- **Strafverfolgung:** Risikobewertungen, Beweismittelbewertung
- **Migration:** Grenzkontrollen, Asylverfahren
- **Justiz:** Unterstützung bei Gerichtsentscheidungen

Anforderungen für Hochrisiko-KI:

- Risikomanagementsystem
- Daten-Governance und Qualitätssicherung
- Technische Dokumentation
- Automatische Protokollierung
- Transparenz gegenüber Nutzern
- Menschliche Aufsicht
- Genauigkeit, Robustheit, Cybersicherheit

Begrenztes Risiko: Transparenzpflichten

Bestimmte KI-Systeme unterliegen **Transparenzpflichten**:

- **Chatbots:** Nutzer müssen wissen, dass sie mit einer KI interagieren
- **Deepfakes:** Synthetische Inhalte müssen als solche gekennzeichnet werden
- **Emotionserkennung:** Betroffene müssen informiert werden
- **Biometrische Kategorisierung:** Betroffene müssen informiert werden

Minimales Risiko: Keine spezifischen Anforderungen

Die **Mehrheit der KI-Systeme** fällt in diese Kategorie:

- KI-gestützte Spamfilter
- KI in Videospielen
- Empfehlungssysteme (mit Einschränkungen)
- Allgemeine Produktivitätstools

> **Wichtig:** Auch bei minimalem Risiko gilt die **Kompetenzpflicht nach Artikel 4**. Alle Mitarbeiter, die KI nutzen, müssen über ausreichende KI-Kompetenz verfügen.

Pflichten für Betreiber von KI-Systemen

Als **Betreiber** (Nutzer von KI-Systemen) haben Sie je nach Risikokategorie unterschiedliche Pflichten:

Allgemeine Pflichten (alle KI-Systeme)

1. **KI-Kompetenz sicherstellen** (Art. 4)
    - Mitarbeiter müssen geschult sein
    - Proportional zum Einsatzzweck
2. **Bestimmungsgemäße Verwendung**
    - KI-Systeme nur wie vorgesehen einsetzen
    - Anweisungen des Anbieters befolgen

Zusätzliche Pflichten bei Hochrisiko-KI

1. **Menschliche Aufsicht** gewährleisten
2. **Eingabedaten** müssen relevant und repräsentativ sein
3. **Überwachung** des Betriebs auf Anomalien
4. **Aufbewahrung von Protokollen** (mind. 6 Monate)
5. **Information** von Betroffenen über KI-gestützte Entscheidungen
6. **Datenschutz-Folgenabschätzung** durchführen
7. **Registrierung** in EU-Datenbank (für bestimmte Systeme)

Pflichten bei generativer KI (z.B. ChatGPT)

Wenn Sie generative KI-Systeme nutzen:

- **Kennzeichnung** von KI-generierten Inhalten (wenn öffentlich)
- **Keine Umgehung** von Sicherheitsmaßnahmen des Anbieters
- **Urheberrecht** beachten bei KI-generierten Inhalten

Fristen und Zeitplan

Der AI Act wird **schrittweise** wirksam:

Datum	Was passiert
1. August 2024	Inkrafttreten der Verordnung
2. Februar 2025	**Verbote für unzulässige KI-Praktiken**
2. August 2025	Regelungen für GPAI-Modelle (z.B. GPT-4)
2. August 2026	**Kompetenzpflicht (Art. 4) + meiste Regelungen**
2. August 2027	Vollständige Anwendung inkl. Hochrisiko-KI in Produkten

Handeln Sie jetzt: Die Kompetenzpflicht gilt ab August 2026. Beginnen Sie frühzeitig mit der Schulung Ihrer Mitarbeiter, um ausreichend Zeit für die Umsetzung zu haben.

Sanktionen bei Verstößen

Der AI Act sieht **erhebliche Bußgelder** vor:

Verstoß	Maximales Bußgeld
Verbotene KI-Praktiken	35 Mio. € oder 7% des weltweiten Jahresumsatzes
Hochrisiko-Anforderungen	15 Mio. € oder 3% des Umsatzes
Andere Verstöße	7,5 Mio. € oder 1% des Umsatzes
Falsche Angaben	7,5 Mio. € oder 1% des Umsatzes

Für KMUs: Die Bußgelder werden verhältnismäßig angewendet. Kleine Unternehmen werden nicht dieselben Strafen erhalten wie Großkonzerne. Dennoch können die Auswirkungen erheblich sein.

Aufsicht und Durchsetzung

Nationale Behörden

Jeder EU-Mitgliedstaat muss **Marktüberwachungsbehörden** benennen. In Deutschland wird dies voraussichtlich die **Bundesnetzagentur** in Zusammenarbeit mit dem **BSI** sein.

EU-Ebene

- **AI Office:** Koordiniert die Durchsetzung auf EU-Ebene
- **AI Board:** Beratungsgremium aus Vertretern der Mitgliedstaaten
- **Wissenschaftliches Gremium:** Berät zu technischen Fragen

Was bedeutet das für Ihr Unternehmen?

Sofort-Checkliste

☐ **Inventar erstellen:** Welche KI-Systeme nutzen Sie?

☐ **Klassifizieren:** Welches Risiko haben diese Systeme?

☐ **Verbote prüfen:** Nutzen Sie verbotene KI-Praktiken?

☐ **Kompetenz planen:** Wer muss geschult werden?

☐ **Verantwortlichen benennen:** Wer kümmert sich um KI-Compliance?

☐ **Budget einplanen:** Für Schulungen und ggf. Anpassungen

Empfohlene nächste Schritte

1. **Bewusstsein schaffen:** Informieren Sie Geschäftsführung und relevante Abteilungen
2. **Bestandsaufnahme:** Erfassen Sie alle KI-Tools im Unternehmen
3. **Risikoanalyse:** Bewerten Sie Ihre KI-Nutzung nach dem Risiko-Framework
4. **Schulungsplan:** Entwickeln Sie einen Plan zur Erfüllung der Kompetenzpflicht
5. **Dokumentation:** Beginnen Sie mit der Dokumentation Ihrer Maßnahmen
6. **Monitoring:** Verfolgen Sie regulatorische Entwicklungen

Zusammenfassung

Die wichtigsten Punkte:

- Der AI Act ist seit August 2024 in Kraft
- Er folgt einem risikobasierten Ansatz mit vier Stufen
- Bestimmte KI-Praktiken sind vollständig verboten
- Die Kompetenzpflicht gilt ab August 2026 für alle KI-Betreiber
- Bei Verstößen drohen erhebliche Bußgelder
- KMUs sollten jetzt mit der Vorbereitung beginnen

Glossar

AI Act	Kurzbezeichnung für die EU-Verordnung über künstliche Intelligenz
Anbieter	Unternehmen, das KI-Systeme entwickelt oder auf den Markt bringt
Betreiber	Unternehmen, das KI-Systeme unter eigener Verantwortung einsetzt
Generative KI	KI, die neue Inhalte erzeugen kann (Text, Bild, Audio, Video)
GPAI	General Purpose AI – KI-Systeme für allgemeine Zwecke
Hochrisiko-KI	KI-Systeme mit erhöhtem Risiko für Grundrechte oder Sicherheit
KI-Kompetenz	Fähigkeiten und Wissen für den sachkundigen Umgang mit KI
Risikobasierter Ansatz	Regulierungsprinzip: höheres Risiko = strengere Regeln