Deloitte.

AI Act

Die EU-Verordnung für Artificial Intelligence (AI) – risikobasierte Anforderungen für Anbieter, Betreiber und weitere Akteure entlang der AI-Wertschöpfung

Was ist der AI Act?

Der AI Act (Verordnung (EU) 2024/1689) ist die **zentrale EU-Regulierung für Artificial Intelligence (AI)** und verfolgt einen risikobasierten Ansatz: Je nach Art des AI-Systems bzw. AI-Modells und dessen Einsatzkontext steigen die regulatorischen Anforderungen – von Transparenzpflichten bis hin zu umfassenden Governance-, Dokumentations- und Kontrollpflichten bei Hochrisiko-AI.

Die Verordnung enthält außerdem Regeln zu:

- verbotenen AI-Praktiken,
- General-Purpose-AI-Modellen (GPAI; allgemein einsetzbare AI-Modelle, z.B. für Text, Bild oder Code),
- sowie ein eigenes Governance- und Aufsichtsregime.

Wer ist betroffen?

Der AI Act erfasst u.a.:

- Anbieter von AI-Systemen und GPAI-Modellen
- Betreiber/Anwender von AI-Systemen in der EU
- Importeure und Distributoren
- Produkthersteller, die AI in Produkte integrieren

Entscheidend ist nicht nur der Sitz des Unternehmens, sondern u. a., ob AI-Systeme/Modelle auf dem EU-Markt bereitgestellt, in Betrieb genommen oder in der EU genutzt werden. Der AI Act hat damit eine marktbezogene EU-Reichweite.

Wichtig

Der AI Act richtet sich nicht nur an AI-Entwickler, sondern auch an Organisationen, die AI-Systeme einkaufen, integrieren oder produktiv einsetzen (z.B. als Betreiber), sofern die regulatorischen Tatbestände erfüllt sind. Der Anwendungsbereich ist damit rollen- und use-case-basiert, nicht primär größenbasiert.

Kernpflichten für betroffene Organisationen

Verbotene AI-Praktiken
Bestimmte AI-Anwendungen sind grundsätzlich verboten, insbesondere in Bereichen mit besonders hohem Risiko für Grundrechte (z.B. bestimmte manipulative/exploitative Praktiken, Social Scoring und bestimmte biometrische Konstellationen).

AI Literacy
Anbieter und Betreiber müssen Maßnahmen setzen, um eine ausreichende AI Literacy (grundlegende AI-Kompetenz im Unternehmen, z.B. sicherer und informierter Umgang mit AI) bei Mitarbeitenden und sonstigen eingesetzten Personen sicherzustellen, abhängig von Kontext, Kenntnissen, Erfahrung und Risiko des Einsatzes.

Hochrisiko-AI: Klassifizierung und Pflichten
Ein AI-System ist u.a. dann Hochrisiko-AI, wenn es in den Anwendungsbereich bestimmter Produktregime fällt (Annex I) oder in Annex III gelistet ist (mit enger Ausnahmelogik).

Für Hochrisiko-AI gelten u.a. Anforderungen zu:

- Risikomanagement
- Daten-/Data Governance
- technischer Dokumentation
- Logging/Aufzeichnung
- menschlicher Aufsicht
- Genauigkeit, Robustheit und Cybersecurity

GPAI-Modelle
Für Anbieter von General-Purpose-AI-Modellen gelten zusätzliche Pflichten (u.a. Dokumentation, Informationen für nachgelagerte Integratoren, Copyright-Policy, Trainingsdaten-Zusammenfassung).

Für GPAI-Modelle mit systemischem Risiko kommen zusätzliche Anforderungen hinzu (u.a. Evaluierung, Risikominderung, Incident-Reporting, Cybersecurity).

Timeline

2. Februar 2026
Frist für Leitlinien der Kommission zur praktischen Umsetzung bestimmter Artikel (z. B. Post-Market-Monitoring)

2. August 2026
Anwendung aller Vorschriften des AI Act, einschließlich der Verpflichtungen für AI-Systeme mit hohem Risiko (z.B. in Gesundheitswesen, Verkehr, Justiz) außer Artikel 6(1)

2. August 2027
Anwendung aller Vorschriften des AI Act einschließlich Artikel 6(1)

Aufsicht & Sanktionen

Der AI Act sieht ein mehrstufiges Governance-Modell vor:

- **EU-Ebene:** u.a. das AI Office bei der Europäischen Kommission
- **Mitgliedstaaten:** nationale zuständige Behörden und ein Single Point of Contact

Für GPAI-Modelle hat die Europäische Kommission exklusive Aufsichts- und Durchsetzungsbefugnisse; die operative Umsetzung erfolgt über das AI Office (Art. 88).

Sanktionsrahmen (Art. 99 / Art. 101):

- **Verbotene AI-Praktiken nach Art. 5:** bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes
- **Bestimmte Verstöße gegen zentrale Pflichten:** bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes
- **Falsche/irreführende Angaben gegenüber Behörden:** bis zu 7,5 Mio. EUR oder 1 % des weltweiten Jahresumsatzes
- **Bereitsteller von GPAI-Modellen:** bis zu 15 Mio. EUR oder 3 % (separates Kommissionsregime)

Was Unternehmen jetzt konkret tun sollten

01 AI-Inventar aufbauen
(entwickelt, eingekauft, integriert, genutzt – inkl. GenAI/Shadow AI)

02 Rollen bestimmen
(Provider / Deployer / Importeur / Distributor / Integrator)

03 Use-Case-Screening gegen Art. 5 / Art. 6 / Art. 50
(Verbote, Hochrisiko, Transparenz) durchführen

04 Governance & Verantwortlichkeiten festlegen

05 Dokumentations- und Nachweisfähigkeit vorbereiten
(insb. bei Hochrisiko-AI und GPAI-Integration)

06 Betriebsprozesse für Monitoring & Vorfälle definieren

07 AI-Literacy-Programm rollen- und risikobasiert starten

Deloitte.

Kontakt

Karin Mair
Managing Partner |
Technology & Transformation und
Strategy, Risk & Transactions

+43 1 537 00-4840
kmair@deloitte.at

Georg Schwondra
Partner |
Cyber

+43 1 537 00-3760
gschwondra@deloitte.at