

DER EU AI ACT

Was Führungskräfte jetzt wissen müssen

„Ist das eigentlich schon KI – und fällt das unter das Gesetz?“

Die Frage kommt in einem Leitungskreis, nachdem ein neues Analyse-Tool vorgestellt wurde. Angeblich KI-gestützt. Und dann kommt der Satz: „Mit diesem neuen EU-Gesetz müssen wir das ja wahrscheinlich prüfen, oder?“

So beginnt es oft: KI ist längst da – in Tools, Prozessen, Entscheidungen. Und nun gibt es ein verbindliches Regelwerk: den **EU AI Act**. Doch was genau regelt er? Welche Pflichten entstehen – und für wen? Was bedeutet das für Organisationen, die nicht KI entwickeln, sondern einfach nur einsetzen?

Was der EU AI Act genau regelt

Der **EU AI Act** ist das erste umfassende Gesetz zur Regulierung Künstlicher Intelligenz. Er ist am 1. August 2024 in Kraft getreten und gilt ab 2025 schrittweise in allen Mitgliedstaaten.

Ziel ist es, einen einheitlichen Rechtsrahmen schaffen, der Innovation ermöglicht – und gleichzeitig Risiken begrenzt.

Wen betrifft das Gesetz?

Nicht nur **Anbieter**, sondern auch **alle, die KI-Systeme nutzen, weiterverkaufen, verwalten oder in Prozesse integrieren**.

Also auch **öffentliche Einrichtungen, Unternehmen jeder Größe und Branchen** – unabhängig davon, ob sie selbst KI entwickeln oder nicht.

Wie funktioniert der AI Act?

Kern des Gesetzes ist eine Einteilung von KI-Systemen in vier Risikoklassen:

- **Verbotene KI:** Systeme, die Menschen manipulieren oder grundlegend diskriminieren (z. B. Social Scoring, verdeckte Emotionserkennung im Arbeitskontext).
- **Hochrisiko-KI:** Systeme, die wesentliche Lebensbereiche betreffen – etwa Bildung, Personal, Justiz, Kreditvergabe oder Gesundheitswesen.
- **Begrenztes Risiko:** Systeme mit potenziellen Risiken, die aber durch Transparenzpflichten ausreichend abgesichert werden können (z. B. KI-Chatbots).
- **Minimales Risiko:** Systeme mit sehr geringem Risiko, z. B. automatische Sortierfunktionen, Spamfilter, KI-Vorschläge in Texteditoren.

Generative KI (wie ChatGPT) fällt grundsätzlich unter die Kategorie „begrenztes Risiko“, kann aber – je nach Anwendung – auch als Hochrisiko-KI gelten.

Ab wann was gilt – die Zeitleiste zur Umsetzung

Der EU AI Act ist **seit Mitte 2024 offiziell** beschlossen – aber er entfaltet seine Wirkung **schrittweise**. Für Führungskräfte ist es wichtig zu verstehen, wann welche Pflichten greifen, um nicht erst bei der Kontrolle reagieren zu müssen.

Hier die zentralen Zeitpunkte:

- **12. Juli 2024** – Veröffentlichung im Amtsblatt: Die Rechtsgrundlage steht.
- **1. August 2024** – Inkrafttreten: Das Gesetz gilt, aber ohne sofortige Pflichten. Die Übergangszeit beginnt.
- **2. Februar 2025** – Verbot illegaler KI + Pflicht zur Schulung (AI Literacy): Verbotene Systeme sind ab diesem Zeitpunkt untersagt. Zudem müssen Organisationen nachweislich alle Mitarbeitenden informieren und schulen, die mit KI in Berührung kommen.
- **2. Mai 2025** – Veröffentlichung freiwilliger Verhaltenskodizes: Anbieter generativer KI (z. B. ChatGPT) erhalten Orientierung für die Einhaltung der kommenden Pflichten.
- **2. August 2025** – Pflichten für generative KI (General Purpose AI): Transparenz, Kennzeichnung und Governance werden verbindlich. Auch Sanktionen greifen erstmals. Anbieter klassischer Hochrisiko-KI erhalten Übergangszeit bis 2027.
- **2. August 2026** – Vollanwendung des Gesetzes: Alle Vorgaben für Hochrisiko-KI gelten verbindlich – inklusive Registrierung, Risikoprüfung, Dokumentation und Kontrolle.
- **2. August 2027** – Ende der Übergangsfrist: Spätestens jetzt müssen alle Hochrisiko-Systeme vollständig rechtskonform betrieben werden.

Für Führungskräfte gilt:

2024 war der Startschuss. **2025** ist das Jahr der Aufbauarbeit. Bis **2026/2027** müssen Strukturen, Zuständigkeiten, Schulungen und Prozesse stehen – nicht nur auf dem Papier, sondern im Alltag.

Welche Pflichten sich daraus für Organisationen ergeben

Je nach Risikoklasse gelten unterschiedliche Anforderungen. Entscheidend ist: **Wer KI einsetzt, trägt Verantwortung – auch wenn das System von außen kommt.**

Für die meisten Organisationen entstehen dabei folgende zentrale **Pflichten**:

Transparenzpflicht

Wenn KI genutzt wird – etwa in Kommunikation, Service oder Entscheidungsunterstützung –, muss das **klar erkennbar sein**. Nutzende (Kund:innen, Mitarbeitende, Bewerber:innen) dürfen nicht getäuscht werden.

Schulungspflicht

Organisationen müssen sicherstellen, dass **alle Mitarbeitenden, die mit KI arbeiten**, über deren Funktion, Grenzen und Risiken informiert sind. Der AI Act verlangt nachweisbare Schulung – **auf allen Hierarchieebenen**, nicht nur in der IT.

Risikoprüfung

Bei Hochrisiko-KI ist eine strukturierte Risikobewertung vorgeschrieben – **vor dem Einsatz**. Dazu gehören: Prüfung auf Diskriminierung, Fehleranfälligkeit, Nachvollziehbarkeit, technische Robustheit.

Technische & organisatorische Maßnahmen

Je nach Risikoklasse müssen Prozesse zur Qualitätssicherung, zum Monitoring und zur Reaktion auf Fehler eingerichtet werden. Diese können je nach Einsatz stark variieren – sie müssen aber **dokumentiert und nachvollziehbar** sein.

Registrierungs- und Informationspflichten

Hochrisiko-Systeme müssen in ein **zentrales EU-Register** eingetragen werden. Auch **externe Anbieter** müssen überprüft und dokumentiert werden – es reicht nicht, sich auf deren Aussagen zu verlassen.

Verantwortung bleibt – auch bei externen Tools

Viele Organisationen entwickeln keine eigenen KI-Systeme, sondern kaufen Tools ein oder nutzen integrierte Funktionen in Standardsoftware.

Gerade hier entsteht ein möglicher blinder Fleck: **Nur weil eine KI „von außen“ kommt, entfällt die Verantwortung nicht.**

Externe Anbieter entbinden nicht von Pflichten

Auch bei zugekauften Systemen müssen Organisationen prüfen, ob es sich um **KI mit Risiko** handelt. Sie müssen sich vergewissern, ob **Transparenzpflichten** bestehen, ob eine **Risikobewertung** notwendig ist oder ob **Mitarbeitende geschult** werden müssen.

Ein Verweis auf das Whitepaper des Herstellers genügt nicht – genauso wenig wie ein „Trust me“-Versprechen in Marketingmaterialien.

Gefahr durch Embedded KI

Besonders anspruchsvoll sind **versteckte KI-Funktionen**, z. B. in CRM-Systemen, HR-Software oder Kundenportalen. Sie sind häufig standardmäßig aktiviert – und werden gar nicht als eigenständige KI erkannt.

Doch auch hier gelten Pflichten: **Sichtbarkeit, Nachvollziehbarkeit und ggf. Dokumentation.**

Führungsimplikation: Tool-Auswahl wird zur Compliance-Frage

Die Auswahl digitaler Werkzeuge ist nicht länger nur eine IT- oder Effizienzentscheidung. Wer Tools einführt, führt Pflichten ein. Führungskräfte müssen sich daher gezielt fragen:

- Ist der Anbieter AI-Act-konform aufgestellt?
- Liegen aussagekräftige Risikoeinschätzungen vor?
- Wer verantwortet die Überprüfung und Einhaltung der Pflichten bei externer Software?

Was Organisationen jetzt tun sollten

Die gute Nachricht: Der AI Act betrifft nicht jede kleine KI-Funktion. Aber er verlangt dort Klarheit, wo KI systematisch eingesetzt wird. Besonders in sensiblen Bereichen. Führungskräfte sollten deshalb jetzt:

Bestandsaufnahme machen

Wo wird in der Organisation bereits KI eingesetzt – sei es offensichtlich oder eingebettet in bestehende Tools?

Risikoeinstufung prüfen

Fallen einzelne Systeme unter Hochrisiko-KI? Wird etwa in der Personalabteilung KI-gestützte Vorauswahl betrieben? Oder im Kundenservice automatisiert bewertet?

Zuständigkeiten klären

Wer trägt Verantwortung für Prüfung, Dokumentation, Schulung? Gibt es interne Prozesse, oder geschieht alles nebenbei?

Schulungen vorbereiten

Die Pflicht zur Information gilt – und betrifft auch die Führungsebene. Schulung ist keine Formalie, sondern ein Organisationsmerkmal: Versteht die Organisation, was sie tut?

Den AI Act als Führungsrahmen begreifen

Der AI Act ist kein reines Compliance-Thema. Er schafft Struktur, um mit KI verantwortungsvoll und nachvollziehbar zu arbeiten – das stärkt auch Vertrauen, Wirkung und Führbarkeit.

Reflexionsfragen

1. Gibt es bei uns KI-gestützte Prozesse, über deren Risikostufe noch nicht gesprochen wurde?
2. Wer entscheidet bei uns, ob ein neues Tool unter die Regeln des AI Acts fällt und wie fundiert?
3. Sind Schulung und Transparenz gegenüber Mitarbeitenden und Kund:innen systematisch geregelt – oder ad hoc?

Fazit

Der EU AI Act will Innovation nicht bremsen, sondern steuerbar machen.

Für Führungskräfte ist das kein juristisches Thema – sondern eine Frage der Klarheit: Was geschieht in der Organisation? Wo sind Risiken? Und wie zeigen wir, dass wir Verantwortung ernst nehmen?

Künstliche Intelligenz weiterdenken

Dieses Briefing ist Teil einer Serie für Führungskräfte, die Orientierung rund um KI suchen. Und es ist (natürlich) in enger Zusammenarbeit mit Künstlicher Intelligenz entstanden.

Nächstes Briefing: #4 Führen mit KI - Warum Sie mehr braucht als ein Go für ChatGPT & Co.

Unverbindliche Erstberatung: <https://calendly.com/freudung/beratung-ki>

Bisherige Briefings & weitere E-Books zum Download: ki-briefing.kit.com

Kontakt: Dr. Beate Freudung, freudung@digital-leader.eu, 0152 05188026