Upgrade. Digital

IMPULSE

Was der EU AI Act vorsieht und welche Governance-Chancen sich abzeichnen

Warum der EU AI Act kein IT-, sondern ein Governance-Thema ist – und wie Unternehmen aus regulatorischer Klarheit einen strategischen Vorteil machen.

Von Hubertus von Roenne · Juni 2026 · 7 Minuten Lesezeit

Was der EU AI Act wirklich ist - in drei Minuten

In Ihrem Unternehmen werden gerade Entscheidungen mithilfe von KI getroffen. Manche davon wissen Sie. Viele nicht. Das ist keine Kritik - es ist die Ausgangslage der meisten Unternehmen im Jahr 2026. KI ist nicht als KI beschafft worden. Sie kam als Feature in Microsoft 365, als Modul im ERP-System, als Algorithmus im HR-Tool. Manche Unternehmen haben KI-Lösungen bewusst eingekauft - aber selbst dort ist das vollständige Bild oft lückenhaft.

Genau das ist der Ausgangspunkt des EU AI Act. Das Gesetz, das im August 2024 in Kraft getreten ist, folgt einer risikobasierten Logik: Nicht alle KI ist gleich gefährlich - also wird nicht alle KI gleich reguliert. Es unterscheidet vier Stufen: verbotene KI, Hochrisiko-KI, KI mit begrenztem Risiko und KI mit minimalem Risiko.

Für die meisten Unternehmen ist die entscheidende Frage: Setzen wir Hochrisiko-KI ein? Eine erste Orientierung: Wenn Sie KI in der Personalauswahl, Kreditvergabe, Kundenbewertung, medizinischen Versorgung oder im Betrieb kritischer Infrastruktur einsetzen - dann ja, mit hoher Wahrscheinlichkeit. Wer sich nicht sicher ist, hat damit bereits die erste Antwort: Die Inventur fehlt.

Das Gesetz gilt extraterritorial - analog zur DSGVO. Jedes Unternehmen, dessen KI-System in der EU eingesetzt wird oder dessen Output EU-Bürger betrifft, fällt darunter. Unabhängig vom Firmensitz.

Aktueller Rechtsstand (28. Juni 2026): Der sogenannte Digital Omnibus on AI wurde am 16. Juni 2026 vom EU-Parlament angenommen. Er verschiebt die vollen Hochrisiko-Pflichten für die meisten Systeme auf Dezember 2027. Die förmliche Annahme durch den Rat steht noch aus (erwartet Juli 2026). Was unverändert gilt: Die Schulungspflicht für KI-Kompetenz ist seit Februar 2025 in Kraft — für nahezu alle Unternehmen, unabhängig vom Risikoprofil. Der 2. August 2026 bleibt als regulatorisches Signal und institutioneller Referenzpunkt wirksam.

Was er von Ihnen verlangt - nicht von Ihrer IT

Hier liegt der entscheidende Punkt, der in der öffentlichen Debatte noch unterschätzt wird: Der EU AI Act ist kein IT-Gesetz. Er ist ein Governance-Gesetz. Die Verantwortung liegt nicht in der Technik-Abteilung. Sie liegt beim Vorstand.

Was das konkret bedeutet: Unternehmen, die Hochrisiko-KI einsetzen, müssen sicherstellen, dass natürliche Personen mit ausreichender Kompetenz, Schulung und Befugnis die Aufsicht führen. KI darf nicht autonom entscheiden - sie muss überwacht werden. Und diese Aufsicht muss dokumentiert, nachweisbar und verteidigbar sein.

Daraus folgen drei Aufgaben, die keine IT-Abteilung allein lösen kann:

Erstens. Die Inventur. Welche KI-Systeme setzt Ihr Unternehmen ein - entwickelt, eingekauft, über Dienstleister bezogen? Diese Frage ist in größeren Organisationen strukturell schwer zu beantworten, weil KI nie als KI beschafft wurde. Eine vollständige Inventur dauert in mittelgroßen Unternehmen erfahrungsgemäß drei bis sechs Monate.

Zweitens. Die Risikoentscheidung. Für jedes System muss die Risikostufe bestimmt und methodisch nachvollziehbar dokumentiert werden. Das ist keine technische Einschätzung - es ist eine strategische. Sie betrifft Haftung, Reputation und Risikoappetit. Sie gehört auf die Vorstandsebene.

Drittens. Die Governance-Struktur. Zuständigkeiten, Dokumentationspflichten, Monitoring, Incident-Reporting. Der häufigste Fehler: Unternehmen starten Prozesse, bevor Verantwortlichkeiten geklärt sind. Wer zuständig ist, entscheidet sich zuerst — dann folgen die Prozesse.

In meiner Beratungspraxis erlebe ich eine Reaktion immer wieder, quer durch Branchen und Unternehmensgrößen: »Das macht die IT.« Der Vorstand, der so antwortet, hat das Thema hart gesagt falsch positioniert - nicht weil IT nicht liefern kann, sondern weil die Frage, welche KI-gestützten Entscheidungen ein Unternehmen verantwortet und wie, eine Führungsentscheidung ist.

> **Die IT kann die Inventur durchführen. Den Risikoappetit definiert die Unternehmensleitung.**

»Sie können Compliance-Arbeit delegieren. Die Letztverantwortung können Sie nicht delegieren.« Das gilt hier ohne Einschränkung.

Und: Für Aufsichtsräte und Gesellschafter, die diesen Text lesen: Die Frage, ob und wie das Unternehmen KI-Governance aufgebaut hat, ist eine legitime Frage des Kontrollgremiums - und sie wird es in den nächsten Monaten zunehmend werden.

Was jetzt ansteht - und was möglich wird

Regulierung erzeugt Aufwand. Das ist unbestreitbar. Aber sie erzeugt auch Klarheit - und Klarheit ist in komplexen Organisationen ein knappes Gut. Wer die Inventur ernst nimmt, lernt etwas über sein eigenes Unternehmen, das er vorher nicht wusste: welche Entscheidungen tatsächlich automatisiert sind, wo menschliche Kontrolle fehlt, wo Dokumentation lückenhaft ist. Das ist unbequem. Es ist

auch wertvoll.

Hinzu kommt eine Dimension, die in der Compliance-Diskussion oft übersehen wird: KI-Governance ist nicht nur ein Reputationsthema. Es ist ein Qualitätsthema. Unternehmen, die verstehen, wie ihre KI-Systeme Entscheidungen über Menschen treffen - über Bewerber, Kunden, Mitarbeitende - führen diese Prozesse besser. Das ist kein ethisches Argument. Es ist ein operatives.

Unternehmen, die KI-Governance glaubwürdig aufbauen, gewinnen Vertrauen - bei Kunden, Partnern, Mitarbeitenden, Regulatoren. Das ist kein Nebeneffekt. Es ist ein Wettbewerbsvorteil, der sich in den nächsten Jahren auszahlen wird.

Ich beobachte das in der Praxis immer wieder: Organisationen, die sich ernsthaft mit neuen Regulierungsanforderungen auseinandergesetzt haben - ob Data Act, DSGVO oder sektorspezifische Anforderungen - haben dabei systematisch mehr über sich selbst gelernt als erwartet. Neue Rechtsgrundlagen zwingen zur Inventur. Und wer inventarisiert, versteht. Beim AI Act ist der Mechanismus derselbe - nur dass es diesmal nicht um Datenzugang geht, sondern um Entscheidungsqualität. Im Data Navigator, dem Praxisformat, das ich gemeinsam mit HÄRTING Rechtsanwälten betreibe, diskutieren wir diese Zusammenhänge regelmäßig.

Fünf Fragen, die jede Unternehmensleitung jetzt auf die Agenda nehmen sollte - unabhängig vom finalen Inkrafttreten der Hochrisiko-Pflichten:

- Welche KI-Systeme setzt unser Unternehmen ein - entwickelt, eingekauft, über Dienstleister? Haben wir eine vollständige, aktuelle Übersicht?
- Welche dieser Systeme könnten als Hochrisiko eingestuft werden? Haben wir diese Einschätzung methodisch nachvollziehbar dokumentiert?
- Wer ist in unserem Unternehmen für KI-Governance verantwortlich - und hat diese Person die nötige Befugnis, Kompetenz und Ressourcen?
- Erfüllen wir die Schulungspflicht? Können unsere Mitarbeitenden nachweisbar einschätzen, was die KI-Systeme, mit denen sie arbeiten, tun - und was nicht?
- Was ist unser Risikoappetit? Welche KI-Anwendungen wollen wir verantworten - und welche nicht? Diese Entscheidung ist strategisch, nicht technisch.

Fazit

Der EU AI Act ist kein Grund zur Panik. Er ist ein Anlass zur Klarheit.

Wer jetzt die Fragen stellt, die gestellt werden müssen, stellt sein Unternehmen nicht nur compliant auf - sondern besser auf.

Das Gesetz gibt den Anlass. Die Chance liegt tiefer: Wer weiß, wie KI in seinem Unternehmen entscheidet, weiß mehr darüber, wie sein Unternehmen wirklich funktioniert.

> **Das ist ein starker Ausgangspunkt.**