LEITFADEN · MAI 2026

EU AI Act Schnellüberblick

Was öffentliche Stellen und Mittelstand wissen müssen.
Mit Checkliste für die eigene Organisation.

Einleitung

Der EU AI Act ist die weltweit erste umfassende Regulierung von Künstlicher Intelligenz. Er ist seit dem 2. August 2024 in Kraft und wird gestaffelt wirksam. Anders als die DSGVO regelt er nicht primär Daten, sondern KI-Systeme: was sie tun dürfen, welche Pflichten ihre Betreiber haben, welche Verbote gelten.

Dieser Leitfaden gibt einen kompakten Überblick für öffentliche Stellen, Mittelstand und politische Organisationen. Er ersetzt keine Rechtsberatung, sondern hilft, die richtigen Fragen zu stellen.

> **Wichtig:** Diese Übersicht beruht auf dem Stand vom Mai 2026. Konkretisierungen durch nationale Behörden und Leitlinien der EU-Kommission kommen laufend hinzu. Für rechtsverbindliche Auskunft wenden Sie sich an einen auf KI-Recht spezialisierten Anwalt.

1. Die vier Risikoklassen

Der EU AI Act klassifiziert KI-Systeme nach Risiko. Die Pflichten ergeben sich aus der Klassifikation. Die meisten Anwendungen im Alltag fallen in die unteren beiden Klassen. Ungewöhnlich ist das nicht, sondern gewollt.

Klasse 1 · Inakzeptables Risiko (verboten)

Anwendungen, die in der EU komplett verboten sind. Dazu gehören Social Scoring durch Behörden, manipulative KI gegen Schutzbedürftige, biometrische Echtzeitüberwachung im öffentlichen Raum und ungezielte Massensammlung biometrischer Daten.

- **Beispiel:** Ein System, das Bürger nach ihrem politischen Verhalten bewertet und ihnen darauf basierend Leistungen gewährt oder verweigert.

Klasse 2 · Hochrisiko (streng reguliert)

Anwendungen, die bei Bildung, Personalwesen, Justiz, kritischer Infrastruktur oder bei behördlichen Entscheidungen mit Außenwirkung eingesetzt werden. Erlaubt mit umfangreichen Pflichten.

- **Beispiel Verwaltung:** KI-gestützte Erstellung rechtsverbindlicher Bescheide. Erlaubt, aber mit Pflicht zu Dokumentation, menschlicher Aufsicht und transparenter Information der Betroffenen.
- **Beispiel Personal:** Vorauswahl von Bewerbern durch KI. Hochrisiko, weil Auswirkung auf den Lebensweg der Person.

Klasse 3 · Begrenztes Risiko (Transparenzpflicht)

Anwendungen mit Pflicht zur Kennzeichnung. Bürger sollen wissen, dass sie mit KI interagieren oder dass Inhalte KI-generiert sind.

- **Beispiel:** Ein Chatbot auf einer Behördenwebsite muss klar als Chatbot erkennbar sein. Ein KI-generiertes Video braucht einen Hinweis.

Klasse 4 · Minimales Risiko (keine Pflichten)

Spam-Filter, Empfehlungsalgorithmen, einfache Automatisierungen. Hierzu zählen die meisten internen KI-Anwendungen in Unternehmen und Behörden.

- **Beispiel:** Ein internes Wissensmanagement, das Mitarbeitenden hilft, in der eigenen Dokumentation zu suchen. Keine besonderen Pflichten.

2. Die wichtigsten Pflichten bei Hochrisiko-Anwendungen

Wer Hochrisiko-KI einsetzt, muss vier Kernpflichten erfüllen. Sie gelten unabhängig davon, ob das System selbst entwickelt oder zugekauft wurde.

Menschliche Aufsicht

Eine konkret benannte Person muss in der Lage sein, das System zu verstehen, es bei Bedarf zu stoppen und seine Entscheidungen zu überstimmen. Bloße „der Sachbearbeiter prüft schon"-Praxis reicht nicht. Es braucht einen dokumentierten Prozess.

Technische Dokumentation

Welches System? Welche Trainingsdaten? Welche bekannten Schwächen? Welches Performance-Niveau? Diese Fragen müssen schriftlich beantwortet sein. Bei zugekauften Systemen liefert diese Doku in der Regel der Anbieter.

Transparenz gegenüber Betroffenen

Wer von einer KI-gestützten Entscheidung betroffen ist, muss das wissen. Außerdem hat er Anspruch auf eine Erklärung, warum die Entscheidung so ausgefallen ist. Praktisch heißt das: Hinweise im Bescheid, im Kontaktformular, in der Datenschutzerklärung.

Risikomanagement

Vor Inbetriebnahme und laufend ist zu prüfen: Welche Risiken bringt das System? Welche Maßnahmen mindern sie? Wer ist verantwortlich, wenn etwas schiefgeht? Auch hier reicht ein gut strukturiertes Dokument, kein Riesenwerk.

3. Was öffentliche Stellen besonders beachten müssen

Behörden treffen rechtsverbindliche Entscheidungen mit Außenwirkung. Damit fallen viele ihrer KI-Anwendungen automatisch in die Hochrisiko-Klasse. Drei Punkte sind besonders wichtig.

- **Recht auf Erklärung:** Bürger haben Anspruch auf eine verständliche Erklärung, wenn KI an einer Entscheidung mitgewirkt hat. Bescheide brauchen entsprechende Hinweise und Begründungen.
- **Recht auf menschliche Überprüfung:** Auf Antrag muss eine rein menschliche Prüfung der Entscheidung möglich sein. Das schließt vollautomatische Bescheide bei Belastungen praktisch aus.
- **Personalvertretung:** Einführung von KI-Systemen, die Arbeitsabläufe verändern, ist mitbestimmungspflichtig. Frühzeitige Beteiligung vermeidet Konflikte.

4. Fahrplan zur Einführung

Schritt 1 · Bestandsaufnahme

Welche KI-Anwendungen sind bereits im Haus, auch im Schatten-IT-Bereich? Welche Anwendungen sind geplant? Welcher Risikoklasse gehören sie an?

Schritt 2 · Klassifizierung

Für jede Anwendung wird die Risikoklasse bestimmt. Im Zweifel die höhere wählen. Wenn eine Anwendung Hochrisiko ist, prüfen, ob sie ersetzt werden kann durch eine geringere Klasse oder anders zugeschnitten werden kann.

Schritt 3 · Pflichten umsetzen

Für Hochrisiko-Anwendungen werden die vier Kernpflichten umgesetzt. Praxisnah: ein Dokument pro Anwendung, jährliche Aktualisierung, klare Verantwortlichkeit.

Schritt 4 · Schulung

Wer mit der Anwendung arbeitet, muss sie verstehen. Das ist nicht optional, sondern eigene Pflicht aus dem Gesetz. Schulungen werden dokumentiert.

5. Häufige Fragen

Was passiert, wenn wir die Pflichten nicht erfüllen?

Bußgelder bis zu 35 Millionen Euro oder 7 Prozent des weltweiten Jahresumsatzes. Bei Behörden gelten oft die Sätze des nationalen Rechts. Praktisch wichtiger: Reputationsschaden und persönliche Verantwortung der Leitung.

Brauchen wir zusätzlich noch DSGVO-Compliance?

Ja. EU AI Act und DSGVO ergänzen sich. KI ohne DSGVO ist genauso wenig zulässig wie KI ohne EU-AI-Act-Compliance. In der Praxis sind beide Themen meist eng verzahnt.

Gilt der EU AI Act auch für ChatGPT und ähnliche Tools?

Ja. Auch die Nutzer haben Pflichten, je nach Einsatzfeld. Wer ChatGPT in einer Hochrisiko-Anwendung einsetzt, braucht die volle Compliance. Wer es für unkritische interne Aufgaben nutzt, hat geringe Pflichten, vor allem Schulungspflicht.

Kernbotschaft.

Der EU AI Act ist anspruchsvoll, aber kein KI-Verbot. Er macht klar, was geht und was nicht. Wer ihn ernst nimmt, schafft sich Rechtssicherheit und Vertrauen bei seinen Bürgern, Kunden und Mitarbeitenden.

Über den Autor

Thomas Peter Finger ist KI-Stratege aus Grevesmühlen. Er berät Politik, Verwaltung und Mittelstand bei der praktischen Einführung von KI. Hauptberuflich Referent für Kommunikation im Wahlkreisbüro einer Bundestagsabgeordneten, ehrenamtlich engagiert in CDU und kommunaler Selbstverwaltung.

Kontakt: kontakt@thomas-finger.com · +49 174 949 64 32 · thomas-finger.com