EU AI ACT · KI-RECHT

EU AI Act – Leitfaden 2026

Europäische KI-Verordnung: Risikoklassen, Pflichten & Handlungsplan für KMU

DEADLINE 2. AUGUST 2026 – Hochrisiko-KI-Systeme müssen ab diesem Datum vollständig dokumentiert, bewertet und compliant sein. Wer heute noch kein KI-Inventar hat, sollte jetzt handeln.

Der EU AI Act (Verordnung (EU) 2024/1689) ist die weltweit erste umfassende KI-Regulierung auf Gesetzgebungsebene. Er ist am 1. August 2024 in Kraft getreten und gilt direkt in allen EU-Mitgliedstaaten. Der Ansatz ist risikobasiert: Je höher das Risikopotenzial eines KI-Systems, desto strenger die Anforderungen. Als KI-System gilt dabei jedes maschinelle System, das auf Basis von Eingaben Ergebnisse wie Vorhersagen, Empfehlungen, Entscheidungen oder Inhalte erzeugt – von Chatbots über Rekrutierungssoftware bis zu Produktionsoptimierungs-Algorithmen. Betroffen sind sowohl Anbieter (Entwickler) als auch Betreiber (Deployer) – also alle Unternehmen, die KI-Systeme im betrieblichen Einsatz haben.

Zeitplan der Anwendbarkeit

Datum	Meilenstein	Betroffen	Status
Aug. 2024	AI Act in Kraft getreten	Alle Unternehmen	■ Abgeschlossen
Feb. 2025	Verbotene KI-Praktiken anwendbar	Alle – verbotene Systeme abschalten	■ Abgeschlossen
Aug. 2025	GPAI-Modell-Anforderungen	Anbieter großer KI-Modelle (>10²■ FLOPs)	■ Abgeschlossen
2. Aug. 2026	Hochrisiko-KI (Anhang II+III)	Anbieter & Betreiber von Hochrisiko-KI	■■ IN KÜRZE
Aug. 2027	Hochrisiko-KI (Anhang I, Produktrecht)	KI in bestehenden EU-Produkten	■ Noch Zeit

Klasse	Typische Systeme	Anforderungen & Sanktionen
■ Verboten (Art. 5)	Social Scoring durch Behörden, manipulative KI, biometrische Echtzeit-Überwachung, Emotion Recognition am Arbeitsplatz/Bildung, Predictive Policing ohne Verdachtsgrundlage	Vollständiges Verbot. Systeme müssen seit Feb. 2025 abgeschaltet sein. Bußgeld: bis 35 Mio. € / 7%
■ Hohes Risiko (Art. 6, Anhang II+III)	CV-Screening & Recruiting-KI, Kreditwürdigkeitsprüfungen, KI in Medizinprodukten, Biometrische Identifikation, KI in kritischer Infrastruktur, KI in Bildungsbewertungen	Konformitätsbewertung, technische Dokumentation, menschliche Aufsicht, Risikomanagementsystem, EU-Register-Eintrag. Bußgeld: bis 15 Mio. € / 3%

Klasse	Typische Systeme	Anforderungen & Sanktionen
■ Begrenztes Risiko (Art. 50)	Chatbots & virtuelle Assistenten, Deep Fakes, KI-generierter Content, Emotionserkennungssysteme mit Offenlegung	Transparenzpflicht: Nutzer müssen wissen, dass sie mit KI interagieren. Kennzeichnung von KI-generierten Inhalten.
■ Minimales Risiko	Spam-Filter, KI in Computerspielen, Produktionsoptimierungsalgorithmen, Empfehlungssysteme ohne personenbezogene Entscheidungen	Keine spezifischen Pflichten. Freiwillige Codes of Conduct empfohlen.

GPAI-Modelle (General Purpose AI): ChatGPT, Claude, Gemini, LLaMA und ähnliche Modelle unterliegen seit August 2025 eigenen Regeln: Transparenzpflichten, Urheberrechts-Compliance und technische Dokumentation. Modelle mit systemischen Risiken (>10²■ FLOPs) haben besonders strenge Pflichten inklusive externer Audits.

Pflicht	Beschreibung
Technische Dokumentation	Vollständige Dokumentation: Architektur, Trainingsdaten, Testmethoden, Performance-Metriken, Limitations. Muss jederzeit verfügbar sein.
Konformitätsbewertung	Nachweis der EU AI Act-Konformität vor Inbetriebnahme – intern (self-assessment) oder über notifizierte Stelle. CE-Kennzeichnung erforderlich.
EU-Datenbankregistrierung	Eintrag im öffentlichen EU-KI-Register (EUDB) für Hochrisiko-Systeme des Anhangs III. Pflicht ab August 2026.
Menschliche Aufsicht	Technische Maßnahmen: Menschen müssen KI überwachen, eingreifen, stoppen oder Entscheidungen überstimmen können.
Risikomanagement-System	Kontinuierliches Risikomanagementsystem über den gesamten Lebenszyklus – vor, während und nach dem Betrieb.
Post-Market-Monitoring	Überwachung nach Inbetriebnahme. Sicherheitsvorfälle müssen der Marktaufsichtsbehörde gemeldet werden.
Grundrechtsfolgenabschätzung	Für Betreiber im öffentlichen Sektor verpflichtend. Empfohlen für KMU bei HR-KI und Kredit-KI.
Mitarbeiter-Schulungen	Nachweispflichtige Schulungen für alle Mitarbeitenden, die Hochrisiko-KI-Systeme bedienen.

Praxisbeispiel: ChatGPT & Microsoft Copilot im KMU-Alltag

Situation: Ein 35-Mitarbeiter-Maschinenbauunternehmen nutzt ChatGPT für Angebotserstellung und Microsoft 365 Copilot für E-Mail-Zusammenfassungen. Personendaten von Kunden werden dabei nicht systematisch verarbeitet. Risikoklasse: Begrenztes Risiko (Art. 50) – keine Hochrisiko-Klassifizierung. Was ist zu tun: (1) Interne Nutzungsrichtlinie erstellen: Was darf mit welchen Daten eingegeben werden? (2) Mitarbeitende schulen, dass KI-generierte Texte als solche erkennbar sein müssen. (3) AVV mit OpenAI/Microsoft prüfen (DSGVO). (4) Kein EU-Register-Eintrag nötig. Aufwand: 1–2 Tage Richtlinienerstellung + halbtägige Schulung. Kosten: <500 €.

Praxisbeispiel: KI-gestützte Bewerber-Vorselektion (Recruiting-KI)

Situation: Ein mittelständischer Handels-GmbH (80 MA) möchte eine HR-Software einführen, die Bewerbungsunterlagen automatisch analysiert und Kandidaten bewertet. Risikoklasse: HOHES RISIKO (Anhang III, Nr. 4 – Beschäftigung, Personalmanagement). Was ist zu tun: (1) Vom Softwareanbieter CE-Kennzeichnung und technische Dokumentation anfordern. (2) Konformitätsbewertung des Anbieters prüfen. (3) Menschliche Aufsicht technisch sicherstellen (kein Kandidat darf rein KI-basiert abgelehnt werden). (4) Schulung der HR-Mitarbeitenden dokumentieren. (5) System im EU-KI-Register als Betreiber eintragen (ab Aug. 2026). (6) Grundrechtsfolgenabschätzung durchführen empfohlen. Aufwand: 3–5 Tage + externe Beratung (ggf. BAFA-gefördert). Kosten: 1.500–4.000 €.

Praxisbeispiel: KI-Qualitätskontrolle in der Fertigung

Situation: Ein Automobilzulieferer (150 MA) verwendet Computer-Vision-KI zur automatischen Fehlererkennung an Bauteilen. Das System entscheidet, ob ein Teil ausgesondert wird. Risikoklasse: Prüfung erforderlich – Anhang II (Produktsicherheit) relevant. Kommt auf Bauteilkritikalität an. Bei sicherheitskritischen Teilen: Hohes Risiko. Was ist zu tun: (1) Rechtlichen Status mit Anwalt/Berater klären. (2) Bei Hochrisiko: Vollständige technische Dokumentation aufbauen. (3) Mensch-in-the-Loop für Grenzfälle sicherstellen. (4) Regelmäßige Performance-Überprüfung einrichten. Empfehlung: Externer KI-Audit sinnvoll – Klarheit über Risikoklasse schafft Rechtssicherheit.

Der erste und wichtigste Schritt: alle KI-Systeme im Unternehmen vollständig erfassen. Dazu zählen auch eingebettete KI-Funktionen in ERP, CRM, HR-Tools, Microsoft 365 und anderen Standardsoftwareprodukten. Nutzen Sie diese Vorlage als Ausgangspunkt:

Nr.	System / Tool	Verwendungszweck	Risikoklasse	Ihre Rolle	Maßnahmen
1	Microsoft 365 Copilot	Bürokommunikation, Textzusammenfassung	Begrenztes Risiko	Intern	Nutzungsrichtlinie, AVV
2	ChatGPT / Claude API	Angebotserstellung, Recherche	Begrenztes Risiko	Intern	Keine Kundendaten einpflegen
3	HR-Software XY (Recruiting-KI)	Kandidatenauswahl	■■ Hohes Risiko	Betreiber	CE-Dok. anfordern, EU-Register
4	CRM-Scoring-Modul	Kundenwert-Prognose	Prüfung nötig	Betreiber	Klärung Anbieter erforderlich
5	Chatbot auf Website	Kundensupport	Begrenztes Risiko	Betreiber	Als KI kennzeichnen
Ihr System...					

Tipp: Microsoft 365 Copilot, GitHub Copilot, Adobe Firefly und vergleichbare KI-Assistenten in Standardprodukten fallen in der Regel unter "Begrenztes Risiko" – sofern Sie damit keine personalisierten Entscheidungen über Personen treffen. Wichtig bleibt: Transparenzpflicht und interne Nutzungsrichtlinie.

Rolle	Relevanz & Handlungsbedarf
CEO / GF	Strategische Verantwortung und persönliche Rechenschaftspflicht. KI-Inventar veranlassen, Compliance-Budget freigeben, Verantwortliche benennen. Unwissenheit schützt nicht vor Bußgeldhaftung.
CFO	Compliance-Budget einplanen: Konformitätsbewertungen (1.000–8.000 € je System), externe Beratung, Schulungen. Bußgeld-Risiko quantifizieren. BAFA-Förderung für Compliance-Beratung prüfen (bis 800 € Zuschuss).
CIO / IT	KI-Inventar aller genutzten Systeme erstellen (auch eingebettete KI). Risikoklassifizierung durchführen. Technische Dokumentation und Aufsichtsmechanismen aufbauen.
DSB / Datenschutz	Schnittstelle DSGVO–AI Act koordinieren: Art. 22 DSGVO harmonisieren mit AI Act Hochrisiko-Anforderungen. DSFA und Risikoabschätzung gemeinsam koordinieren.

Rolle	Relevanz & Handlungsbedarf
Projektleiter	Bei jedem KI-Projekt: Risikoklasse vorab bestimmen, Compliance-Anforderungen als Projektbestandteil einplanen. AI Act-Compliance ist kein Nachprojekt.
KMU allgemein	Auch kleine Unternehmen mit Hochrisiko-KI müssen compliant sein. Häufig sind jedoch nur Minimal-Risk-Systeme betroffen – der erste Schritt ist eine strukturierte Bestandsaufnahme.

Die Compliance-Kosten hängen stark davon ab, welche KI-Systeme eingesetzt werden. Für die meisten KMU mit ausschließlich begrenztem Risiko-Systemen hält sich der Aufwand in engen Grenzen. Bei Hochrisiko-Systemen steigt der Aufwand erheblich:

Szenario	Interner Aufwand	Externe Kosten	Leistungsumfang
Nur begrenztes Risiko (Chatbots, GPAI-Tools)	1–2 Tage intern	< 1.000 €	Nutzungsrichtlinie, Kennzeichnung, Schulung
1 Hochrisiko-System (z.B. HR-KI)	3–5 Tage + extern	2.000–6.000 €	Beratung, Dokumentation, EU-Register
2–5 Hochrisiko-Systeme	5–15 Tage + extern	5.000–20.000 €	Vollständiges Compliance-Programm
Vollständiger KI-Audit (AIT-Empowerment)	0,5–1 Tag Ihrerseits	ab 690 € Eigenanteil*	Bestandsaufnahme, Report, Handlungsplan

* Bei BAFA-Förderung (bis 800 € Zuschuss)

Für Hochrisiko-Systeme verlangt der EU AI Act vollständige technische Dokumentation. Für alle anderen Systeme empfiehlt sich zumindest eine interne Grunddokumentation als Nachweis bewussten und verantwortungsvollen Umgangs:

- **Systemname & Version:** Eindeutige Bezeichnung, Versions-/Releasenummer
- **Anbieter:** Name, Kontakt, CE-Zertifizierungsstatus
- **Verwendungszweck:** Wofür wird das System eingesetzt? Wer nutzt es?
- **Eingabedaten:** Welche Daten werden verarbeitet? Enthalten sie Personenbezug?
- **Risikoklasse:** Einordnung in die 4 Risikoklassen mit Begründung
- **Verantwortliche Person:** Wer ist intern für das System verantwortlich?
- **Nutzungsrichtlinie:** Was darf/darf nicht eingegeben werden?
- **Schulungsdatum:** Wann wurden Mitarbeitende geschult?
- **Letzte Überprüfung:** Datum der letzten Compliance-Überprüfung

F: Wir nutzen nur ChatGPT intern – müssen wir wirklich etwas tun?

A: Ja, aber der Aufwand ist überschaubar. ChatGPT/GPAI-Tools fallen unter "Begrenztes Risiko". Pflicht: (1) Nutzer müssen wissen, dass Outputs KI-generiert sind. (2) Eine interne Nutzungsrichtlinie sollte klären, welche Daten eingepflegt werden dürfen. (3) AVV mit OpenAI für DSGVO-Compliance.

F: Gilt der EU AI Act auch für kleine Unternehmen?

A: Ja. Es gibt keine Größenschwelle. ABER: Für Unternehmen, die keine Hochrisiko-KI einsetzen, sind die Anforderungen sehr überschaubar. Zunächst: KI-Inventar erstellen, Risikoklassen bestimmen – dann zeigt sich, was wirklich zu tun ist.

F: Was passiert wenn wir nichts tun?

A: Bei Hochrisiko-Systemen: Bußgelder bis 15 Mio. € oder 3% Jahresumsatz. Bei Verstößen gegen verbotene Praktiken: bis 35 Mio. € / 7%. Deutsche Aufsichtsbehörden werden aktiv prüfen. Versicherungen können bei KI-Schäden die

Zahlung verweigern, wenn grundlegende Compliance fehlt.

F: Reicht es, wenn der KI-Anbieter compliant ist?

A: Nein. Anbieter und Betreiber (also Sie) haben getrennte Pflichten. Als Betreiber sind Sie für den korrekten Einsatz verantwortlich – auch wenn das System selbst CE-zertifiziert ist. Sie müssen insbesondere: menschliche Aufsicht sicherstellen, Personal schulen, und das System korrekt einsetzen.

- KI-Inventar erstellen: Alle genutzten KI-Systeme vollständig erfassen (inkl. MS 365 Copilot, ChatGPT, CRM-KI)
- Risikoklassifizierung: Jedes System den 4 Kategorien zuordnen (Anhang II + III des AI Acts)
- Verbotene Praktiken (Art. 5): Prüfen ob betroffene Systeme seit Feb. 2025 abgeschaltet sind
- GPAI-Nutzung dokumentieren: Transparenzpflichten für ChatGPT/Copilot/Claude umsetzen
- Hochrisiko-KI: Konformitätsdokumentation beim Anbieter anfordern
- Menschliche Aufsicht: Technisch sicherstellen, dass Eingriff und Überstimmung möglich ist
- Nutzungsrichtlinie erstellen: Klare Regeln für alle Mitarbeitenden, welche Daten in KI-Tools
- Schulungen durchführen und dokumentieren
- AI-Governance: Interne Verantwortliche für AI Act Compliance benennen
- EU-Register: Hochrisiko-Systeme ab August 2026 eintragen

BAFA-Förderung nutzen: Externe Beratungsleistungen zur EU AI Act Compliance sind über das BAFA-Programm „Förderung unternehmerischen Know-hows" förderfähig. KMU erhalten bis zu 800 € Zuschuss. Antrag muss VOR Projektbeginn gestellt werden. Voraussetzung: Unternehmen seit >2 Jahren am Markt, max. 249 MA.

Beratung & Unterstützung durch AIT-Empowerment: KI-Audit in einem halben Tag: Bestandsaufnahme aller KI-Systeme, Risikoklassifizierung, schriftlicher Report mit Handlungsplan (8–12 Seiten). BAFA-förderfähig. → info@ait-empowerment.de → ait-empowerment.de/ki-audit-eu-ai-act.html → Kostenloses Erstgespräch: calendly.com/florianlehnertwortmann