

COMPLIANCE

EU AI Act: Was müssen KMU jetzt wirklich tun?

EU AI Act und KMU: Welche Pflichten gelten wann, welche Tools sind betroffen und was kostet Compliance realistisch? Praxis-Guide für Betriebe 2025/2026.

AUTOR

Strukturaflow-Team

VERÖFFENTLICHT

25. April 2026

ONLINE LESEN

<https://wissen.strukturaflow.it.com/eu-ai-act-kmu-was-tun/>

Sie nutzen ChatGPT für Angebotsentwürfe, ein KI-Tool für die Buchhaltung und haben gehört, der EU AI Act tritt in Kraft — und fragen sich nun, ob Sie jetzt einen Compliance-Beauftragten brauchen. Die kurze Antwort: Wahrscheinlich nicht. Die etwas längere Antwort: Es kommt darauf an, welche KI-Tools Sie wie einsetzen.

Der EU AI Act gilt gestaffelt und reguliert nach Risiko, nicht pauschal alle KI-Anwendungen. Für viele KMU ist der konkrete Handlungsbedarf überschaubar — aber nicht null. Wer einen KI-gestützten Bewerbungsfiler einsetzt, steht vor anderen Pflichten als wer ChatGPT für interne Texte nutzt.

Dieser Artikel zeigt, welche Pflichten wann greifen, in welche Risikoklasse typische KMU-Tools fallen, was Compliance realistisch kostet — und was Sie konkret bis Ende 2025 erledigt haben sollten.

Was ist der EU AI Act – die 90-Sekunden-Version für KMU

Der EU AI Act ist am 1. August 2024 in Kraft getreten, gilt aber nicht sofort und vollständig. Die Anwendung erfolgt gestaffelt über mehrere Jahre, mit ersten Pflichten ab Februar 2025.

Das Kernprinzip: Regulierung nach Risiko, nicht nach Technologie. Ein KI-System, das Kreditwürdigkeit bewertet, unterliegt strengeren Regeln als ein KI-Spam-Filter — weil das Schadenspotenzial grundlegend verschieden ist.

Anbieter oder Betreiber — wer sind Sie?

Für die meisten KMU gilt: Sie sind Betreiber, kein Anbieter. Der Unterschied ist wesentlich.

- **Anbieter** entwickeln KI-Systeme, trainieren Modelle und bringen sie auf den Markt. Ihre Pflichten sind umfangreich.
- **Betreiber** nutzen bestehende KI-Systeme im eigenen Geschäftsbetrieb. Ihre Pflichten sind deutlich geringer — aber nicht inexistent.

Wer also ein SaaS-Tool mit eingebauter KI-Funktion abonniert (Buchhaltungssoftware, CRM, Chatbot-Plattform), ist in der Regel Betreiber. Die Anbieter dieser Tools tragen die Hauptverantwortung für die Compliance des Systems selbst — Sie als Betreiber tragen Verantwortung für den konkreten Einsatz.

Die vier Risikoklassen – und wo typische KMU-Tools landen

Der EU AI Act teilt KI-Systeme in vier Kategorien ein. Für den Alltag in einem KMU sind zwei davon besonders relevant.

Unannehmbares Risiko (verboten)

Diese Systeme sind seit Februar 2025 verboten: Social-Scoring-Systeme staatlicher Stellen, KI zur unbewussten Manipulation von Verhalten, biometrische Echtzeit-Überwachung im öffentlichen Raum (mit engen Ausnahmen).

Für nahezu alle KMU im DACH-Raum: nicht relevant. Kein normaler Gewerbebetrieb setzt solche Systeme ein.

Hohes Risiko (umfangreiche Pflichten)

Hier wird es für manche KMU konkret. Als Hochrisiko gelten unter anderem:

- KI-Systeme zur Personalentscheidung (Bewerbungsranking, Leistungsbewertung)
- KI-gestützte Kreditwürdigkeitsprüfung
- Sicherheitskritische Systeme in Infrastruktur, Medizin, Bildung
- Bestimmte biometrische Identifikationssysteme

Typisches KMU-Szenario: Sie nutzen eine HR-Software, die eingehende Bewerbungen automatisch nach Kriterien rankt und Kandidaten vorauswählt. Das fällt unter Hochrisiko – mit erheblichen Pflichten: Technische Dokumentation, Risikobewertung, menschliche Aufsicht, Protokollierung, Transparenz gegenüber Betroffenen.

Wer solche Systeme einsetzt, sollte handeln – und im Zweifel externe Beratung hinzuziehen.

Begrenztes Risiko (Transparenzpflichten)

Systeme, die mit Menschen interagieren und dabei nicht als KI erkennbar sein könnten:

- Chatbots im Kundenservice
- KI-generierte Bilder, Texte oder Videos (Deep Fakes)
- Emotion-Recognition-Systeme

Handlungsbedarf: Kennzeichnungspflicht. Wer einen KI-Chatbot auf der Unternehmenswebsite betreibt, muss Besucherinnen und Besuchern kenntlich machen, dass sie mit einem KI-System interagieren. Das ist überschaubar, aber verbindlich.

Minimales Risiko (keine spezifischen Pflichten)

Hier landen die meisten KI-Tools, die KMU heute im Alltag einsetzen:

- ChatGPT und vergleichbare Schreibassistenten
- KI-gestützte Buchhaltungs- und Steuertools
- KI-Spam-Filter, Empfehlungsalgorithmen im eigenen Shop
- Projektmanagement-KI, Terminplanungs-Tools

Für diese Kategorie gibt es keine spezifischen EU AI Act-Pflichten. Eine interne Dokumentation und Nutzungsrichtlinie sind dennoch empfehlenswert – aus praktischen und datenschutzrechtlichen Gründen.

Die Fristen 2025/2026 – was gilt wann

Nicht alles gilt sofort. Die folgende Übersicht zeigt, was wann relevant wird:

FRIST	WAS GILT	RELEVANT FÜR KMU?
Februar 2025	Verbotene KI-Praktiken anwendbar	Nein (für normale KMU)
August 2025	GPAI-Modell-Regeln (<u>General Purpose AI</u>)	Bedingt — nur wenn eigene Modelle feinetuned werden
August 2026	Hochrisiko-Pflichten vollständig in Kraft	Ja, wenn Hochrisiko-KI eingesetzt wird
2027	Spezifische weitere Bereiche (z.B. bestimmte regulierte Produkte)	Selten für Standard-KMU

Die ehrliche Einschätzung: Wer keine Hochrisiko-KI betreibt, hat bis August 2026 Zeit für die vollständige Umsetzung. Das bedeutet aber nicht, dass Abwarten sinnvoll ist. Wer jetzt eine saubere Bestandsaufnahme macht, spart sich später Zeitdruck und mögliche Fehler.

Zeitstrahl mit vier Meilensteinen der EU AI Act-Umsetzung: Februar 2025 Verbote, August 2025 GPAI-Regeln, August 2026 Hochrisiko-Pflichten (hervorgehoben), 2027 weitere Regulierung.

Alltagscheck – Was bedeutet das konkret für Ihren Betrieb?

Szenario 1: ChatGPT und generative KI im Büro

Klassifikation: Minimales Risiko

Sie nutzen ChatGPT, Copilot oder ähnliche Tools, um E-Mails zu formulieren, Angebote zu entwerfen oder interne Dokumentationen zu erstellen. Aus EU AI Act-Perspektive: kein spezifischer Handlungsbedarf.

Was trotzdem zu tun ist: Eine interne Nutzungsrichtlinie für Mitarbeitende — was darf mit KI-Tools getan werden, welche Daten dürfen eingegeben werden? Außerdem bleibt die DSGVO vollständig relevant. Personenbezogene Daten von Kunden oder Mitarbeitenden gehören nicht ungeprüft in externe KI-Systeme.

Szenario 2: KI-Tools für die Bewerbungsauswahl

Klassifikation: Hochrisiko

Das ist die Kategorie, die für KMU am häufigsten unterschätzt wird. Wer Software einsetzt, die Bewerbungen automatisch bewertet, rankt oder filtert — auch wenn das ein Feature einer größeren HR-Plattform ist — betreibt potenziell Hochrisiko-KI.

Die Pflichten sind erheblich: nachweisbare menschliche Aufsicht über Entscheidungen, Transparenz gegenüber Bewerbenden, Dokumentation. Empfehlung: Lassen Sie die konkrete Einordnung im Einzelfall rechtlich prüfen, bevor Sie solche Tools produktiv einsetzen.

Szenario 3: KI-Chatbot auf der Unternehmenswebsite

Klassifikation: Begrenztes Risiko

Ein automatisierter Kundenservice-Chat, der Fragen beantwortet, Termine vermittelt oder Produktinformationen liefert — das ist eine der häufigsten KI-Anwendungen in kleinen Betrieben.

Hier ist die Kennzeichnungspflicht verbindlich: Nutzerinnen und Nutzer müssen erkennen können, dass sie mit einem KI-System kommunizieren. Eine klar sichtbare Kennzeichnung („Dieser Chat wird von einem KI-Assistenten beantwortet“) reicht in den meisten Fällen aus. Kein großer Aufwand — aber nicht optional.

Szenario 4: KI-Buchhaltung und KI-Steuertools

Klassifikation: In der Regel minimales Risiko

Tools wie DATEV mit KI-Funktionen, automatische Belegverarbeitung oder KI-gestützte Ausgabenkategorisierung fallen typischerweise unter minimales Risiko — solange sie keine eigenständigen Kreditentscheidungen treffen.

Wichtig zu verstehen: Wenn Ihr Anbieter die Pflichten als Anbieter erfüllt, reduziert sich Ihre Betreiber-Verantwortung erheblich. Prüfen Sie trotzdem, ob Ihr Tool-Anbieter entsprechende Konformitätsnachweise bereitstellt oder kommuniziert.

Szenario 5: KI-Kameraüberwachung im Ladenlokal

Klassifikation: Potenziell Hochrisiko oder verboten — je nach Funktion

Eine normale Überwachungskamera ohne KI-Funktion ist kein Thema für den EU AI Act (wohl aber für die DSGVO). Sobald jedoch Gesichtserkennung, Verhaltensanalyse oder automatisierte Personenidentifikation ins Spiel kommen, ändert sich die Lage grundlegend.

Systeme, die das Verhalten von Kunden analysieren, Emotionen erkennen oder Personen identifizieren, können unter Hochrisiko oder sogar unter die Verbotskategorie fallen. Wer solche Systeme betreibt oder einführen möchte, sollte das dringend prüfen lassen — bevor der Vertrag unterschrieben ist.

Die ehrliche Kosten-Risiko-Einschätzung für Kleinstbetriebe

Was kostet Compliance realistisch? Das hängt entscheidend davon ab, welche KI-Systeme Sie einsetzen.

Für Betriebe ohne Hochrisiko-KI:

Der Aufwand ist überschaubar. Eine interne Bestandsaufnahme (welche KI-Tools nutzen wir?), eine Nutzungsrichtlinie für Mitarbeitende, und die korrekte Kennzeichnung eines etwaigen Chatbots: Das sind 2–4 Stunden Arbeit und, wenn externe Vorlagen genutzt werden, nahezu keine direkten Kosten.

Für Betriebe mit Hochrisiko-KI:

Hier ist der Mehraufwand erheblich. Technische Dokumentation, Risikobewertung, Prozesse für menschliche Aufsicht — das erfordert realistisch externe Unterstützung. Kosten für eine fundierte Rechts- und Technikberatung im Hochrisiko-Bereich liegen je nach Komplexität im vierstelligen Bereich.

Zum Thema Bußgelder:

Der EU AI Act sieht Bußgelder von bis zu 35 Mio. Euro oder 7 % des weltweiten Jahresumsatzes vor. Diese Zahlen kursieren in fast jedem Artikel — und sie sind korrekt, aber kontextlos. In der Praxis richten sich diese Maximalstrafen gegen Anbieter verbotener Systeme oder gegen schwerwiegende Hochrisiko-Verstöße durch größere Marktteilnehmer.

Für einen Handwerksbetrieb mit KI-Angebotssoftware oder ein Einzelhandelsgeschäft mit KI-Kassensystem ist das Bußgeldrisiko bei dokumentiertem, minimalem KI-Einsatz realistisch betrachtet sehr gering. Das ist aber kein Freifahrtschein: Wer wissentlich Hochrisiko-KI ohne Compliance betreibt, bleibt auch als KMU nicht ohne Konsequenzen.

Die ehrliche Empfehlung: Eine einmalige Einordnung des eigenen KI-Einsatzes lohnt sich für jeden Betrieb — nicht wegen Panik, sondern weil es Sicherheit schafft und in vielen Fällen wenig Aufwand bedeutet.

Checkliste – Was KMU bis Ende 2025 konkret erledigen sollten

Diese Checkliste ersetzt keine Rechtsberatung, gibt aber eine praktische Orientierung:

1. **Bestandsaufnahme:** Erstellen Sie eine Liste aller KI-Tools, die Ihr Unternehmen aktuell nutzt – von der Buchhaltungssoftware über den Website-Chatbot bis zum KI-Assistenten in Ihrer E-Mail-Software.
2. **Risikoklasse bestimmen:** Ordnen Sie jedes Tool einer Risikoklasse zu. Nutzen Sie dafür die offiziellen Ressourcen der EU-Kommission oder die Selbstauskunft Ihrer Tool-Anbieter. Orientierung bietet auch ein KI-Audit für KMU, das genau diese Einordnung systematisch vornimmt.
3. **Hochrisiko-Tools identifizieren und priorisieren:** Sind Bewerbungsfilter, Kreditprüfungen oder Kamerasysteme mit Analyse-Funktionen dabei? Diese brauchen prioritäre Aufmerksamkeit.
4. **Nutzungsrichtlinie für Mitarbeitende erstellen:** Legen Sie schriftlich fest, welche KI-Tools zu welchen Zwecken genutzt werden dürfen, welche Daten eingegeben werden dürfen und wie mit KI-generierten Ergebnissen umzugehen ist.
5. **Datenschutz-Check:** Prüfen Sie, ob Ihre KI-Tool-Nutzung DSGVO-konform ist – besonders wenn personenbezogene Daten verarbeitet werden. Der EU AI Act ändert nichts an den bestehenden DSGVO-Pflichten.
6. **Kennzeichnungspflichten umsetzen:** Betreiben Sie einen KI-Chatbot oder veröffentlichen Sie KI-generierte Inhalte? Sorgen Sie für klar sichtbare Kennzeichnung.
7. **Interne Dokumentation anlegen:** Auch wenn Ihre Tools unter minimales Risiko fallen: Dokumentieren Sie, welche Systeme Sie einsetzen, zu welchem Zweck und wer intern verantwortlich ist. Das kostet wenig und schafft Klarheit.
8. **Bei Hochrisiko: Externe Beratung einholen:** Wenn Schritt 3 einen positiven Befund ergibt, holen Sie rechtliche und technische Unterstützung. Das ist keine Option, sondern eine sinnvolle Investition.

Branchenblick – Besonderheiten für typische DACH-KMU-Sektoren

Handwerk & Bau

Typischer KI-Einsatz: Angebots- und Kalkulationssoftware mit KI-Unterstützung, Zeitplanung, gelegentlich Baustellenüberwachung per Kamera.

Besonderer Hinweis: Kamerabasierte Sicherheitssysteme auf Baustellen sollten hinsichtlich ihrer konkreten Funktionen geprüft werden. Reine Bildaufzeichnung ist anders zu behandeln als Systeme, die Bewegungsanalyse oder Personenerkennung durchführen.

Einzelhandel & Gastronomie

Typischer KI-Einsatz: Kassensysteme mit KI-Analyse, Reservierungstools, Kundenbindungs-Apps mit personalisierten Empfehlungen.

Besonderer Hinweis: Personalisierungsalgorithmen im Marketing (z.B. „Kunden wie Sie haben auch gekauft...“) fallen in der Regel unter minimales Risiko. Systeme, die Kundenverhalten in Echtzeit auswerten und Preise oder Angebote dynamisch anpassen, sollten näher betrachtet werden.

Dienstleister & Agenturen

Typischer KI-Einsatz: Generative KI für Content-Erstellung, KI im Projektmanagement, vereinzelt KI-gestützte Recruiting-Tools.

Besonderer Hinweis: Der Einsatz von KI-Tools zur Vorauswahl von Bewerbenden — auch wenn es sich nur um ein Feature einer breiteren HR-Plattform handelt — ist in dieser Branche häufiger als gedacht und fällt unter Hochrisiko. Agenturen, die solche Tools einsetzen, sollten das nicht auf die lange Bank schieben.

FAQ: Häufige Fragen zum EU AI Act für KMU

Gilt der EU AI Act auch für mich, wenn ich nur ChatGPT nutze?

In der Regel fallen einfache Nutzungsszenarien — Texte schreiben, E-Mails formulieren, Zusammenfassungen erstellen — unter minimales Risiko. Es gibt keine spezifischen EU AI Act-Pflichten dafür. Eine interne Nutzungsrichtlinie und DSGVO-Compliance bleiben aber relevant, unabhängig vom AI Act.

Was ist der Unterschied zwischen KI-Anbieter und KI-Betreiber laut EU AI Act?

Anbieter entwickeln KI-Systeme und bringen sie auf den Markt. Betreiber nutzen bestehende Systeme im eigenen Betrieb. Die meisten KMU sind Betreiber — mit deutlich geringeren Pflichten als Anbieter. Dennoch: Als Betreiber tragen Sie Verantwortung dafür, dass Sie das System zweckgemäß und nachvollziehbar einsetzen.

Ab wann drohen Bußgelder, und wie hoch sind sie realistisch für kleine Betriebe?

Bußgelder bis 35 Mio. Euro sind möglich, richten sich aber primär nach Schwere des Verstoßes, Unternehmensgröße und ob verbotene Praktiken oder Hochrisiko-Verstöße vorliegen. Für Kleinstbetriebe ohne Hochrisiko-KI ist das Bußgeldrisiko bei korrekt dokumentiertem Handeln gering — aber nicht null. Wer Hochrisiko-KI ohne Compliance betreibt, trägt auch als KMU ein reales Risiko.

Muss ich einen KI-Beauftragten ernennen?

Nein, eine solche explizite Pflicht kennt der EU AI Act für Betreiber nicht. Wer jedoch Hochrisiko-KI einsetzt, braucht nachweisbar funktionierende menschliche Aufsichtsmechanismen — auch wenn diese nicht in einer eigenen Stabsstelle institutionalisiert sein müssen.

Nächste Schritte – Wo Sie jetzt anfangen können

Der EU AI Act ist kein Grund zur Panik — aber auch kein Thema, das sich von selbst erledigt. Für die meisten KMU, die Standard-Tools im minimalen Risikobereich nutzen, ist der Aufwand überschaubar. Für Betriebe mit Hochrisiko-Anwendungen besteht echter Handlungsbedarf, bevor die Fristen 2026 näherrücken.

Drei Sofortmaßnahmen, die Sie noch diese Woche angehen können:

1. Erstellen Sie eine Liste aller KI-Tools, die in Ihrem Betrieb im Einsatz sind — inklusive eingebetteter KI-Funktionen in bestehender Software.
2. Identifizieren Sie, ob darunter Systeme zur Personalentscheidung, Kreditprüfung oder Kameraanalyse sind.
3. Legen Sie intern schriftlich fest, wer für den KI-Einsatz verantwortlich ist und welche Grundregeln gelten.

Wer nach dieser Bestandsaufnahme unsicher ist, in welche Risikoklasse die eigenen KI-Tools fallen — oder welche konkreten nächsten Schritte für den eigenen Betrieb wirklich notwendig sind — dem bietet Strukturaflow ein unverbindliches 30-Minuten-Beratungsgespräch an. Dabei schauen wir uns gemeinsam den konkreten KI-Einsatz an: ohne Fachjargon, ohne versteckte Agenda, mit einem klaren Bild davon, was zu tun ist und was warten kann.

NÄCHSTER SCHRITT

Mehr praktische KI-Anleitungen für KMU

Dieser Artikel ist Teil des KI-Hubs von Strukturaflow — einer deutschsprachigen Plattform für den praktischen KI-Einsatz in kleinen und mittleren Unternehmen.

<https://wissen.strukturaflow.it.com>