



EU AI Act 2026: Was Unternehmen jetzt wissen müssen

Künstliche Intelligenz ist in vielen Unternehmen längst Teil des Arbeitsalltags. Mitarbeitende formulieren Texte mit generativer KI, analysieren Daten, erstellen Präsentationen oder nutzen KI-Funktionen, die unbemerkt in Standardsoftware integriert wurden. Gleichzeitig werden Chatbots, Recruiting-Anwendungen, Prognosemodelle und automatisierte Entscheidungsunterstützung immer häufiger in betriebliche Prozesse eingebunden.

Mit dem EU AI Act erhält diese Entwicklung einen verbindlichen europäischen Rahmen. Seit dem 2. August 2026 gelten weitere zentrale Bestimmungen – darunter Transparenzpflichten für bestimmte interaktive und generative KI-Systeme. Maßnahmen zur Förderung von KI-Kompetenz sind bereits seit Februar 2025 relevant. Für Unternehmen bedeutet das nicht, jede KI-Anwendung vorsorglich zu stoppen. Entscheidend ist vielmehr, die eigene Nutzung zu kennen, Risiken nachvollziehbar einzuordnen und passende Regeln zu etablieren.

Gerade im Mittelstand fehlt häufig nicht der Wille, sondern die gemeinsame Übersicht: Welche KI-Tools werden tatsächlich eingesetzt? Welche Daten fließen ein? Wer entscheidet über Freigaben? Und welche Mitarbeitenden benötigen welches Wissen? Wer diese Fragen strukturiert beantwortet, schafft nicht nur eine bessere Ausgangslage für regulatorische Anforderungen, sondern auch für eine sichere und wirtschaftlich sinnvolle KI-Nutzung.



Was der EU AI Act regelt

Der EU AI Act schafft einheitliche Regeln für die Entwicklung, Bereitstellung und berufliche Nutzung von KI-Systemen in der Europäischen Union. Sein Kern ist ein risikobasierter Ansatz: Je größer die möglichen Auswirkungen eines Systems auf Sicherheit, Gesundheit oder Grundrechte sind, desto umfangreicher sind die Anforderungen.

Welche Pflichten ein Unternehmen treffen, hängt nicht allein von der eingesetzten Technologie ab. Wichtig sind insbesondere:

- der konkrete Verwendungszweck des Systems,
- die mögliche Auswirkung auf Menschen,
- die Rolle des Unternehmens – etwa als Anbieter oder Betreiber eines KI-Systems,
- der Einsatzkontext, beispielsweise Personalwesen, Kundenservice oder kritische Infrastruktur,
- und die Frage, ob ein System wesentlich verändert oder unter eigenem Namen angeboten wird.

Viele mittelständische Unternehmen sind vor allem "Betreiber" – im englischen Verordnungstext „Deployer“ – weil sie KI-Systeme in eigener Verantwortung beruflich einsetzen. Wer ein System

entwickelt, entwickeln lässt und unter eigenem Namen auf den Markt bringt, kann dagegen zum "Anbieter" werden.

Auch eine wesentliche Veränderung eines bestehenden Systems kann die eigene Rolle verändern. Deshalb sollte die Rollenklärung früh erfolgen und nicht erst am Ende einer technischen Einführung.

Der Zeitplan bleibt gestaffelt. Transparenzpflichten nach Artikel 50 gelten grundsätzlich seit dem 2. August 2026. Die Anforderungen an bestimmte Hochrisiko-Systeme greifen nach dem aktualisierten Zeitplan ab dem 2. Dezember 2027; für KI-Systeme, die als Sicherheitskomponenten in regulierte Produkte eingebettet sind, ab dem 2. August 2028.

Unabhängig von diesen Übergangsfristen ist es sinnvoll, Inventar, Verantwortlichkeiten und Prüfprozesse bereits heute aufzubauen.



Risikoklassen im Überblick



Der EU AI Act unterscheidet vier Risikostufen. Für die Praxis ist wichtig: Nicht das verwendete Produkt allein entscheidet über die Einordnung, sondern vor allem der konkrete Anwendungsfall.

1. Unannehmbares Risiko

Bestimmte KI-Praktiken sind grundsätzlich verboten. Dazu gehören beispielsweise bestimmte manipulative oder täuschende Anwendungen, unzulässiges Social Scoring sowie weitere Nutzungsformen, die Menschen in besonderer Weise gefährden können. Unternehmen sollten deshalb schon bei der Beschaffung prüfen, ob ein geplanter Einsatz Berührungspunkte mit verbotenen Praktiken hat.

2. Hohes Risiko

Hochrisiko-KI kann unter anderem in Bereichen wie Beschäftigung, Bildung, kritischer Infrastruktur oder bei bestimmten Entscheidungen über den Zugang zu wesentlichen Leistungen vorliegen. Ein typisches Prüffeld im Mittelstand ist der Einsatz von KI im Personalbereich – etwa zur Auswahl, Bewertung oder Steuerung von Beschäftigten.

Für Hochrisiko-Systeme sieht die Verordnung umfangreiche Anforderungen vor. Je nach Rolle können dazu beispielsweise Risikomanagement, Dokumentation, Protokollierung, menschliche Aufsicht, Datenqualität, Überwachung und Meldeprozesse gehören. Ob eine Anwendung tatsächlich als Hochrisiko-System einzustufen ist, sollte nicht pauschal, sondern anhand ihres Zwecks und ihrer konkreten Funktionsweise geprüft werden.

3. Begrenztes Risiko

Bei bestimmten Anwendungen stehen Transparenzpflichten im Vordergrund. Menschen sollen beispielsweise erkennen können, wenn sie unmittelbar mit einem KI-System interagieren. Auch für bestimmte KI-generierte oder manipulierte Inhalte, Deepfakes sowie den Einsatz von Emotionserkennung oder biometrischer Kategorisierung gelten Informations- beziehungsweise Kennzeichnungspflichten.

Für Unternehmen ist dieser Bereich seit August 2026 besonders aktuell. Betroffen sein können beispielsweise öffentlich eingesetzte Chatbots oder bestimmte Veröffentlichungen, die ohne menschliche Prüfung mit generativer KI erstellt wurden. Die konkrete Pflicht und mögliche Ausnahme hängen vom jeweiligen Einsatz ab.

4. Minimales oder kein zusätzliches Risiko

Viele alltägliche Anwendungen fallen nicht unter besondere risikobezogene Zusatzpflichten des EU AI Acts. Das bedeutet jedoch nicht, dass sie ohne Regeln eingesetzt werden sollten. Datenschutz, Informationssicherheit, Urheberrecht, Geschäftsgeheimnisse und arbeitsrechtliche Anforderungen können weiterhin relevant sein. Zudem benötigt auch eine scheinbar harmlose Anwendung klare Zuständigkeiten und eine passende Nutzungskompetenz.

Wichtige Pflichten für Unternehmen

Eine einzelne Standard-Checkliste für alle Unternehmen gibt es nicht. Die Anforderungen richten sich nach Rolle, System und Anwendungsfall. In der betrieblichen Praxis haben sich jedoch sechs Handlungsfelder als besonders wichtig erwiesen.

KI-Nutzung sichtbar machen

Unternehmen sollten eingesetzte und geplante KI-Anwendungen in einem KI-Inventar erfassen. Dazu gehören nicht nur ChatGPT, Microsoft Copilot oder Gemini, sondern auch KI-Funktionen in CRM-, HR-, Marketing-, Sicherheits- oder Analysewerkzeugen. Sinnvolle Angaben sind Zweck, Anbieter, verantwortlicher Bereich, Nutzergruppen, verwendete Daten, betroffene Personen und aktueller Freigabestatus.

Rolle und Risiko einordnen

Für jeden relevanten Anwendungsfall ist zu klären, welche Rolle das Unternehmen übernimmt und welche Risikokategorie in Betracht kommt. Besondere Aufmerksamkeit verdienen Anwendungen in HR, Kundenkommunikation, Bonitäts- oder Leistungsbewertung sowie Systeme, die Entscheidungen über Menschen vorbereiten oder beeinflussen.

Transparenz sicherstellen

Wo Menschen direkt mit KI interagieren oder bestimmte künstlich erzeugte Inhalte veröffentlicht werden, können Kennzeichnungs- und Informationspflichten greifen. Verantwortliche sollten prüfen, ob Hinweise technisch und organisatorisch korrekt umgesetzt sind und wer ihre Aktualität überwacht.

KI-Kompetenz fördern

Anbieter und Betreiber sollen Maßnahmen zur KI-Kompetenz der Personen treffen, die in ihrem Auftrag mit KI-Systemen arbeiten. Ein allgemeines Erklärvideo für alle reicht nicht in jedem Nutzungskontext aus. Sinnvoll sind rollenbezogene Maßnahmen: Die Personalabteilung benötigt anderes Wissen als Marketing, IT-Administration, Kundenservice oder Geschäftsführung. Auch Regeln für vertrauliche Daten, Ergebnisprüfung, menschliche Verantwortung und interne Meldewege gehören dazu.

Klare Regeln und Freigabewege schaffen

Eine praxistaugliche KI-Nutzungsrichtlinie sollte verständlich festlegen, welche Tools für welche Zwecke zugelassen sind, welche Daten nicht eingegeben werden dürfen, wann eine menschliche Prüfung erforderlich ist und an wen sich Mitarbeitende bei Unsicherheiten wenden. Ergänzend braucht es einen nachvollziehbaren Prozess für Auswahl, Prüfung, Freigabe und regelmäßige Neubewertung von KI-Tools.

Entscheidungen dokumentieren und überprüfen

Dokumentation sollte nicht als einmalige Ablage verstanden werden. Verantwortlichkeiten, Freigaben, Schulungsmaßnahmen, Prüfanfragen und offene Fragen müssen nachvollziehbar bleiben. Bei Änderungen am Tool, Einsatzbereich oder Anbieter ist eine erneute Bewertung sinnvoll. So entsteht schrittweise eine belastbare KI-Governance.

Unser praxisorientierter EU-AI-Act-Ansatz

Viele Unternehmen benötigen zunächst keine umfangreiche Zertifizierungsinitiative, sondern ein verlässliches Lagebild und eine klare Priorisierung. Unser Ansatz übersetzt regulatorische Anforderungen in einen umsetzbaren betrieblichen Prozess.

1. EU AI Act Readiness Check

Der Readiness Check verbindet einen Management-Fragebogen, eine standardisierte Mitarbeitendenbefragung, die Sichtung vorhandener Unterlagen & ein geführtes Analysegespräch. Dadurch werden Managementsicht & gelebte Praxis zusammengeführt.

Das Ergebnis ist ein organisatorisches Lagebild mit sichtbaren Lücken, offenen Prüffragen und priorisierten nächsten Schritten.

Der Check ist keine Compliance-Zertifizierung, keine vollständige Inventarisierung und keine abschließende Rechtsprüfung. Er schafft die Grundlage, um Zeit und Budget dort einzusetzen, wo tatsächlich Handlungsbedarf besteht.

2. Governance-Workshop

Im bereichsübergreifenden Workshop arbeiten Geschäftsführung, IT, HR, Datenschutz, Compliance und relevante Fachbereiche an konkreten Anwendungsfällen. Gemeinsam werden erste Verantwortlichkeiten, Freigabewege, Regeln und Maßnahmen festgelegt. Statt abstrakter Diskussionen entsteht ein umsetzbarer Fahrplan.

3. Rollenbezogene KI-Kompetenzmaßnahmen

Aus den eingesetzten Systemen und den Aufgaben der Beteiligten wird ein passender Kompetenzbedarf abgeleitet. Darauf aufbauend können Basisschulungen und zielgruppenspezifische Module für Führungskräfte, HR, Marketing und Vertrieb, IT oder Kundenservice entwickelt und dokumentiert werden.

4. Vorlagen und laufende Governance

KI-Inventar, Tool-Freigabe, Nutzungsrichtlinie, Anwendungsfall- und Risikobogen, Rollenmatrix, Schulungsnachweise und Meldewege machen Governance im Alltag nutzbar. Regelmäßige Reviews sorgen dafür, dass die Unterlagen nicht veralten, wenn neue Tools, Funktionen oder Einsatzbereiche hinzukommen.

Rechtliche Grenzfälle werden dabei nicht mit Scheinsicherheit beantwortet, sondern für eine gezielte fachkundige Prüfung aufbereitet. Unsere Leistung ist die strukturierte operative Vorarbeit, nicht der Ersatz einer Rechtsberatung.





Praxisbeispiel: Vom Tool-Wildwuchs zum gemeinsamen Maßnahmenplan

Ein typisches mittelständisches Unternehmen nutzt bereits generative KI in mehreren Bereichen. Das Marketing erstellt Textentwürfe, der Vertrieb bereitet Kundentermine vor, Mitarbeitende testen öffentliche Chatbots und in der Bürosoftware werden neue KI-Funktionen freigeschaltet. Die Geschäftsführung geht davon aus, dass die IT den Einsatz steuert. Die IT wiederum kennt nicht alle Anwendungen, weil viele Tools direkt in den Fachbereichen eingeführt wurden.

Im Readiness Check werden Managementsicht, Mitarbeitendenperspektive und vorhandene Regeln zusammengeführt. Dabei zeigt sich: Es gibt einzelne Datenschutzvorgaben und engagierte Schulungsaktivitäten, aber kein gemeinsames KI-Inventar, keine eindeutigen Verantwortlichkeiten und keinen abgestimmten Freigabeprozess.

Im anschließenden Governance-Workshop priorisiert das Unternehmen drei konkrete Maßnahmen:

1.

Alle relevanten KI-Anwendungen und Anwendungsfälle in einem gemeinsamen Inventar erfassen

2.

einen einfachen Prüf- und Freigabeweg mit klaren Verantwortlichen einführen

3.

rollenbezogene Regeln und Kompetenzmaßnahmen für besonders aktive Fachbereiche umsetzen.

Das Ergebnis ist keine pauschale Bestätigung vollständiger Compliance. Das Unternehmen verfügt jedoch über Transparenz, benannte Zuständigkeiten und einen realistischen Maßnahmenplan. Offene rechtliche, datenschutzrechtliche und technische Fragen können nun gezielt geprüft werden, statt im Tagesgeschäft unentdeckt zu bleiben.

Dieses Beispiel ist eine typisierte Darstellung häufiger Ausgangslagen und keine Kundenreferenz.

Was Sie jetzt tun sollten

Der sinnvollste Einstieg ist eine strukturierte Bestandsaufnahme. Diese fünf Schritte können Unternehmen unmittelbar beginnen:

- 1. KI-Anwendungen erfassen:** Sammeln Sie alle offiziell eingeführten, getesteten und in Standardsoftware enthaltenen KI-Funktionen – einschließlich der konkreten Anwendungsfälle.
- 2. Verantwortung klären:** Benennen Sie für jede relevante Anwendung eine fachlich verantwortliche Person oder Funktion und beteiligen Sie IT, Datenschutz, Compliance und gegebenenfalls den Betriebsrat angemessen.
- 3. Rolle und Anforderungen prüfen:** Klären Sie, ob Ihr Unternehmen Betreiber, Anbieter oder in einer weiteren Rolle betroffen ist. Prüfen Sie verbotene Praktiken, mögliche Hochrisiko-Einstufungen und Transparenzpflichten.
- 4. Sofortmaßnahmen festlegen:** Schließen Sie erkennbare Lücken bei Kennzeichnung, Datenverwendung, menschlicher Kontrolle, Tool-Freigabe und internen Regeln.
- 5. Kompetenz und Governance verstetigen:** Planen Sie rollenbezogene Maßnahmen, dokumentieren Sie Entscheidungen und überprüfen Sie Anwendungen regelmäßig.

Wenn Sie mehrere dieser Fragen heute nur teilweise beantworten können, ist das kein ungewöhnlicher Befund. Es zeigt vor allem, dass eine gemeinsame Übersicht und ein abgestimmter Prozess fehlen. Genau hier setzt ein EU AI Act Readiness Check an.

Sie möchten wissen, wie gut Ihr Unternehmen seine KI-Nutzung bereits kennt und steuert? In einem unverbindlichen Erstgespräch klären wir Ihre Ausgangslage und ob ein EU AI Act Readiness Check für Sie der passende nächste Schritt ist.





Fazit

Der EU AI Act macht 2026 deutlich: KI darf im Unternehmen kein unverbundener Flickenteppich aus Einzeltools, stillen Tests und unklaren Zuständigkeiten bleiben. Entscheidend ist nicht, möglichst viele Dokumente zu produzieren, sondern die eigene KI-Nutzung zu verstehen und wirksam zu steuern.

Ein KI-Inventar, klare Verantwortlichkeiten, passende Transparenzmaßnahmen, rollenbezogene Kompetenzentwicklung und nachvollziehbare Freigabewege bilden dafür eine solide Grundlage. Unternehmen, die diese Strukturen jetzt aufbauen, reduzieren nicht nur regulatorische Unsicherheit. Sie schaffen zugleich bessere Voraussetzungen für sichere, vertrauenswürdige und wirtschaftlich sinnvolle KI-Anwendungen.

Author

Thomas Müller, Partner

Tel. +49 179 3949 817

E-Mail tmueller@eragroup.com

TÜV- zertifizierter AI Automation Manager

value through insight™

Want to know more?
eragroup.com