

EU AI Act: Was seit 2. August 2026 gilt – und was die IT jetzt tun sollte.

Ein praxisnaher Leitfaden für Unternehmen, die KI-Systeme, generative KI, Chatbots und KI-gestützte Business-Anwendungen einsetzen

Seit dem 2. August 2026 gelten die Transparenzpflichten aus Artikel 50 des EU AI Act. Unternehmen müssen Menschen je nach Anwendungsfall darüber informieren, dass sie mit KI interagieren, Deepfakes oder bestimmte Texte von öffentlichem Interesse kennzeichnen und prüfen, ob Anbieter synthetische Inhalte maschinenlesbar markieren. Die Pflichten für Hochrisiko-KI wurden auf den 2. Dezember 2027 beziehungsweise den 2. August 2028 verschoben - Transparenz, KI-Kompetenz und verbotene KI-Praktiken jedoch nicht.

Für die meisten Organisationen beginnt die praktische Arbeit mit fünf Fragen: Wo wird KI bereits eingesetzt? Sind wir Anbieter oder Betreiber? Wer verantwortet den jeweiligen Use Case? Auf welche Daten und Identitäten kann das System zugreifen? Und können wir nachweisen, wie es kontrolliert wird?

Fragen Sie Marketing, HR, Customer Service und IT, wo KI genutzt wird, erhalten Sie häufig vier unterschiedliche Listen. Die Lücke zwischen diesen Listen ist das erste Risiko. Ein KI-System, dessen Existenz unbekannt ist, lässt sich weder steuern noch absichern oder dokumentieren.

DIE KURZE ANTWORT. Der EU AI Act wurde nicht einfach 'verschoben'. Die Transparenzpflichten aus Artikel 50 gelten jetzt. Nur bestimmte Pflichten für Hochrisiko-KI greifen später. Die zusätzliche Zeit sollte für ein KI-Inventar, klare Rollen, eindeutige Verantwortung sowie technische Kontrollen und Dokumentation genutzt werden.

Was hat sich am 2. August 2026 geändert?

Artikel 50 des AI Act ist anwendbar geworden. Er regelt Transparenzpflichten für Anbieter und Betreiber bestimmter KI-Systeme - darunter interaktive KI, generative KI, Systeme zur Emotionserkennung und biometrischen Kategorisierung, Deepfakes sowie bestimmte KI-generierte Texte zu Themen von öffentlichem Interesse.

Zudem hat die Europäische Kommission mit der Durchsetzung jener Regeln begonnen, die Anbieter von KI-Modellen mit allgemeinem Verwendungszweck betreffen. Für ein typisches Unternehmen, das KI einkauft, lautet die unmittelbare Frage jedoch selten, ob es ein Basismodell trainiert. Entscheidend ist, ob der konkrete KI-Einsatz eine Informations-, Kennzeichnungs-, Sicherheits- oder Governance-Pflicht auslöst.

Was wurde verschoben - und was nicht?

Mit der Verordnung (EU) 2026/1744, dem Digital Omnibus on AI, wurde die Anwendung der zentralen Pflichten für Hochrisiko-KI verschoben. Der Grund: Harmonisierte Normen, Leitlinien und nationale Umsetzungsstrukturen waren noch nicht ausreichend verfügbar. Die Pflichten wurden neu terminiert, nicht gestrichen.

2. Dezember 2027: eigenständige Hochrisiko-KI-Systeme nach Artikel 6 Absatz 2 und Anhang III.

2. August 2028: Hochrisiko-KI-Systeme als Sicherheitskomponenten regulierter Produkte nach Artikel 6 Absatz 1 und Anhang I.

Die Verschiebung schafft Vorbereitungszeit - keine Wartezeit. Risikomanagement, technische Dokumentation, Protokollierung, menschliche Aufsicht und Cybersecurity hängen von Designentscheidungen ab, die heute getroffen werden. Diese Nachweise nach einem Jahr Produktivbetrieb zu rekonstruieren, ist langsamer, teurer und weniger verlässlich, als sie von Beginn an festzuhalten.

Erste Frage: Sind Sie Anbieter oder Betreiber?

Ein Anbieter entwickelt ein KI-System, lässt es entwickeln oder bringt es unter eigenem Namen beziehungsweise eigener Marke auf den Markt. Ein Betreiber setzt ein KI-System in eigener Verantwortung im beruflichen Kontext ein. Die meisten Unternehmen, die KI-Tools Dritter nutzen, sind Betreiber - doch die Rolle kann sich ändern, wenn ein System wesentlich verändert oder unter dem eigenen Namen angeboten wird.

Ein und dieselbe Organisation kann bei einem Use Case Betreiber und bei einem anderen Anbieter sein. Klären Sie die Rolle deshalb für jedes System separat. Davon hängt ab, wer die Information im Systemdesign umsetzt, wer maschinenlesbar markiert, wer Inhalte sichtbar kennzeichnet und wer technische Nachweise aufbewahrt.

Die Transparenzpflichten aus Artikel 50 verständlich erklärt

1. Menschen über die Interaktion mit KI informieren

Anbieter von KI-Systemen, die direkt mit Menschen interagieren, müssen die Systeme so gestalten, dass Nutzerinnen und Nutzer über die KI-Interaktion informiert werden - außer dies ist für eine angemessen informierte und aufmerksame Person offensichtlich. Bei einem Service-Chatbot oder KI-Agenten gehört der Hinweis an den Beginn der Interaktion, nicht versteckt in die AGB.

2. Synthetische Inhalte maschinell erkennbar machen

Anbieter von Systemen, die synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen, müssen sicherstellen, dass die Ausgaben maschinenlesbar markiert und als künstlich erzeugt oder manipuliert erkennbar sind. Diese Pflicht richtet sich an Anbieter. Unternehmen, die Tools Dritter einsetzen, sollten dennoch prüfen, was der Anbieter technisch bereitstellt, und dies in Einkauf, Integration und Content-Prozesse aufnehmen.

Für Anbieter relevanter generativer KI-Systeme, die bereits vor dem 2. August 2026 auf dem Markt waren, gilt für diese spezifische Markierungspflicht eine Übergangsfrist bis zum 2. Dezember 2026.

3. Emotionserkennung und biometrische Kategorisierung offenlegen

Betreiber von Systemen zur Emotionserkennung oder biometrischen Kategorisierung müssen betroffene Personen informieren - vorbehaltlich der Ausnahmen und Bedingungen des AI Act. Solche Use Cases sind seltener als Chatbots, wegen der sensiblen Daten sind Discovery und Zugriffskontrolle jedoch besonders wichtig.

4. Deepfakes und bestimmte Texte von öffentlichem Interesse kennzeichnen

Betreiber müssen offenlegen, wenn Bild-, Audio- oder Videoinhalte als KI-generierter oder manipulierter Deepfake einzustufen sind. Ebenfalls zu kennzeichnen sind KI-generierte oder manipulierte Texte, die die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse informieren sollen und keiner menschlichen Prüfung oder redaktionellen Kontrolle unterzogen wurden. Das bedeutet nicht, dass jeder KI-unterstützte Marketingsatz automatisch sichtbar gekennzeichnet werden muss. Rolle, Inhalt, Kontext und Review-Prozess sind entscheidend.

KI-Kompetenz bleibt relevant

Die Regeln zur KI-Kompetenz gelten seit dem 2. Februar 2025. Nach der Änderung durch den Digital Omnibus müssen Anbieter und Betreiber Maßnahmen treffen, um die Entwicklung von KI-Kompetenz bei Mitarbeitenden und anderen Personen zu unterstützen, die in ihrem Auftrag KI-Systeme betreiben oder nutzen. Das Gesetz verlangt nicht, für jede einzelne Person ein bestimmtes Kompetenzniveau zu garantieren. Es verlangt jedoch nachvollziehbare und an den Kontext angepasste Maßnahmen.

Eine allgemeine Schulungsfolie pro Jahr wird selten für jede Rolle ausreichen. Ein Developer, der ein KI-Modell integriert, eine Marketing-Mitarbeiterin, die synthetische Inhalte freigibt, und ein Service-Desk-Mitarbeiter mit KI-Assistent stehen vor unterschiedlichen Risiken und benötigen unterschiedliche Leitlinien.

Welche Sanktionen sind möglich?

Bei Verstößen gegen die Transparenzpflichten aus Artikel 50 liegt der gesetzliche Höchststrafen bei bis zu 15 Mio. EUR oder 3% des weltweiten Jahresumsatzes eines Unternehmens, je nachdem, welcher Betrag höher ist. Der höhere Rahmen von 35 Mio. EUR oder 7% gilt für verbotene KI-Praktiken nach Artikel 5 - nicht für jeden Verstoß gegen den AI Act. Für KMU sieht der AI Act eine

verhältnismäßigere Berechnung vor; die konkrete Durchsetzung hängt vom Einzelfall und den nationalen Verfahren ab.

Die wichtigsten AI-Act-Termine auf einer Seite

Datum	Was gilt
2. Feb. 2025	Verbotene KI-Praktiken und Anforderungen an KI-Kompetenz
2. Aug. 2025	Regeln für KI-Modelle mit allgemeinem Verwendungszweck und EU-Governance
2. Aug. 2026	Transparenzpflichten nach Artikel 50; Durchsetzung der anwendbaren GPAI-Regeln durch die Kommission
2. Dez. 2026	Ende der Übergangsfrist für die Markierung nach Artikel 50 Absatz 2 durch Anbieter relevanter Systeme, die vor dem 2. Aug. 2026 bereits auf dem Markt waren
2. Dez. 2027	Zentrale Hochrisiko-Pflichten für eigenständige Systeme nach Artikel 6 Absatz 2 und Anhang III
2. Aug. 2028	Zentrale Hochrisiko-Pflichten für KI-Sicherheitskomponenten in regulierten Produkten nach Artikel 6 Absatz 1 und Anhang I

Ein pragmatischer 90-Tage-Plan für AI-Act-Readiness

1. **Ein gemeinsames KI-Inventar aufbauen.** Erfassen Sie System, Anbieter, Geschäftszweck, Owner, Nutzergruppen, Datenkategorien, verbundene Anwendungen, betroffene Personen, Anbieter-/Betreiberrolle, Risikohinweis, externe Kennzeichnung, Logging und Vertragsstatus. Beginnen Sie mit einem kontrollierten Register; die technische Reife kann danach wachsen.
2. **Rolle und Risiko mit der Rechtsberatung einordnen.** Trennen Sie die Pflichten von Anbietern, Betreibern, Importeuren und Händlern. Markieren Sie verbotene und potenziell hochriskante Use Cases für eine fachliche Prüfung. Die juristische Einstufung sollte nicht allein bei der IT liegen.
3. **Alle Transparenz-Touchpoints prüfen.** Kontrollieren Sie Chatbots, KI-Agenten, Avatare, Emotionserkennung, biometrische Kategorisierung, synthetische Medien und Inhalte von öffentlichem Interesse. Verifizieren Sie sowohl sichtbare Hinweise als auch maschinenlesbare Markierungen, wo sie relevant sind.
4. **Technische Kontrollen um den Use Case legen.** Definieren Sie Identitäten und Berechtigungen, schützen Sie Prompts und sensible Daten, aktivieren Sie angemessene Protokollierung, überwachen Sie Integrationen, verwalten Sie Maschinenidentitäten und dokumentieren Sie menschliche Prüfung und Eskalation.
5. **Nachweise und Verantwortung schaffen.** Benennen Sie eine verantwortliche Person, dokumentieren Sie Entscheidungen, bewahren Sie Anbieterinformationen auf, legen Sie

Review-Intervalle fest, halten Sie Schulungsmaßnahmen fest und etablieren Sie ein Reporting, das die Wirksamkeit der Kontrollen sichtbar macht.

Drei Fragen, die Unternehmen besonders häufig stellen

Wurde der EU AI Act verschoben?

Nein. Bestimmte Pflichten für Hochrisiko-KI wurden verschoben. Die Transparenzpflichten aus Artikel 50 gelten seit dem 2. August 2026; andere Teile des AI Act sind bereits seit 2025 anwendbar.

Muss jeder KI-generierte Text sichtbar gekennzeichnet werden?

Nein. Anbieter müssen relevante synthetische Ausgaben maschinenlesbar markieren. Betreiber müssen Deepfakes sowie Texte von öffentlichem Interesse ohne menschliche Prüfung oder redaktionelle Kontrolle sichtbar kennzeichnen. Der konkrete Use Case entscheidet.

Werden wir durch den Einsatz eines KI-Tools eines Drittanbieters selbst zum Anbieter?

In der Regel ist das nutzende Unternehmen Betreiber, aber nicht immer. Wer ein System unter eigenem Namen anbietet oder wesentlich verändert, kann eine andere Rolle übernehmen. Jedes System und jede Bereitstellung sollte separat bewertet werden.

Offizielle Quellen

- [Europäische Kommission: Quick Facts - Transparency rules for AI systems](#)
- [Europäische Kommission: Leitlinien zu den Transparenzpflichten aus Artikel 50](#)
- [EUR-Lex: Verordnung \(EU\) 2024/1689 - Artificial Intelligence Act](#)
- [EUR-Lex: Verordnung \(EU\) 2026/1744 - Digital Omnibus on AI](#)
- [Rat der EU: endgültige Annahme der Vereinfachungsregeln](#)

Von der rechtlichen Vorgabe zum technischen Betriebsmodell: Wo Bacher Systems unterstützt

Die juristische Bewertung gehört in die Hände Ihrer Rechtsberatung. Unsere Arbeit beginnt dort, wo diese Bewertung in eine sichere, transparente und steuerbare IT-Umgebung übersetzt werden muss.

- **Consulting und Roadmap:** Analyse der bestehenden Umgebung, Identifikation technischer Lücken, Priorisierung von Initiativen und Entwicklung einer realistischen KI-Governance-Roadmap.

- **Implementierung und Migration:** Umsetzung des Zielbilds in funktionierende Lösungen, Integrationen, Prozesse und Plattform-Anpassungen - mit Projektmanagement und bewährten Best Practices.
- **Data Analytics und Observability:** Zusammenführung von Logs, Metriken, Traces und Events für Transparenz, Dashboards, Alerts und Reporting über KI-gestützte Services hinweg.
- **Cybersecurity und Digital Identities:** Schutz von Daten, Modellen und Integrationen durch Access Management, Privileged Access Controls, Machine Identity Management und kontinuierliches Security Monitoring.
- **Support und Managed Services:** Betrieb und Monitoring von Plattformen, Incident-, Change- und Lifecycle-Management sowie kontinuierliche Weiterentwicklung nach dem Go-live.

Gerade der letzte Punkt ist entscheidend. AI-Act-Readiness ist keine einmalige Tool-Implementierung. In unserem Adoption Circle arbeiten wir auch nach dem Go-live gemeinsam mit unseren Kunden weiter, erhöhen kontinuierlich den Mehrwert der Plattform, passen die Roadmap an und reagieren auf neue technische und regulatorische Anforderungen. Wir übernehmen Mitverantwortung für das Ergebnis - nicht nur für die Technologie.

Mehr erfahren:

[Bacher Systems Consulting, Implementierung, Support und Managed Services](#)

Wichtig: Bacher Systems ist keine Rechtsanwaltskanzlei und erbringt keine Rechtsberatung. Wir können Sie dabei unterstützen, die juristische Bewertung in technische Realität zu übersetzen - vom KI-Inventar, der Roadmap und einer sicheren Architektur bis zu Access Management, Logging, Observability, Reporting, Implementierung und laufendem Managed Service.