

COMPLIANCE

EU AI Act Audit für KMU: Wer prüft, wie und was kostet es?

Wer prüft KMU nach dem EU AI Act wirklich? Risikoklassen, Audit-Kosten und Behörden in Deutschland und Österreich — konkret erklärt.

AUTOR

Strukturaflow-Team

VERÖFFENTLICHT

27. Juli 2026

ONLINE LESEN

<https://wissen.strukturaflow.it.com/eu-ai-act-audit-kmu-wer-prueft-wie-kosten/>

Die meisten Artikel zum EU AI Act erklären, was die Verordnung ist. Was sie nicht beantworten: Wer erscheint konkret auf der Matte, welches Ihrer KI-Systeme löst überhaupt eine Prüfpflicht aus, und mit welchen realistischen Kosten müssen Sie rechnen? Genau das beantwortet dieser Artikel — für KMU in Deutschland und Österreich.

Die wichtigste Nachricht zuerst: Für die überwiegende Mehrheit der KMU mit Standard-KI-Tools gibt es keine externe Pflichtprüfung. Chatbots, KI-gestützte Buchhaltungstools oder Copilot-Integrationen fallen in der Regel unter Limited- oder Minimal-Risk — das bedeutet keine externe Auditpflicht, aber trotzdem interne Dokumentationspflichten. Für den kleinen Teil der KMU, die tatsächlich High-Risk-KI einsetzen, sieht es anders aus.

Erst der Grundsatz: Nicht jedes KI-System muss extern auditiert werden

Der EU AI Act teilt KI-Systeme in vier Risikoklassen ein. Welche Klasse Ihr System hat, entscheidet über alles Weitere — von der Dokumentationspflicht bis zur Frage, ob ein externer Auditor überhaupt ins Spiel kommt.

RISIKOKLASSE	BEISPIELE	EXTERNE PRÜFPFLICHT
Unacceptable Risk (verboten)	Social Scoring, biometrische Massenüberwachung	Verboten — keine Nutzung möglich
High Risk	Recruiting-KI mit Scoring, Kreditbewertung, medizinische Diagnose-KI	Konformitätsbewertung erforderlich
Limited Risk	Chatbots, KI-generierte Texte/Bilder	Transparenzpflichten, keine externe Prüfpflicht
Minimal Risk	Spam-Filter, einfache Empfehlungssysteme	Keine spezifischen Pflichten

Die externe Pflichtprüfung — die sogenannte Konformitätsbewertung — betrifft fast ausschließlich High-Risk-Systeme nach Anhang III des EU AI Acts. Typische KMU-Anwendungen lassen sich so einordnen:

- **Chatbot auf der Website** → Limited Risk (Transparenzpflicht, kein Pflicht-Audit)
- **Recruiting-KI, die Bewerber automatisch bewertet und rankt** → High Risk
- **KI-Buchhaltungstool** → je nach Kontext Minimal oder Limited Risk
- **KI-gestützte Kreditentscheidung** → High Risk

Selbstcheck: 3 Fragen zur Risikoklasse Ihres Systems

- Trifft Ihr KI-System Entscheidungen, die Menschen in Bereichen wie Beschäftigung, Bildung, Kredit oder Sicherheitskritik erheblich beeinflussen?
- Verarbeitet das System biometrische Daten zur Identifikation oder Kategorisierung von Personen?
- Wird das System in einem Bereich nach Anhang III eingesetzt (z. B. Strafverfolgung, kritische Infrastruktur, Medizinprodukte)?

Wenn Sie alle drei Fragen mit „Nein“ beantworten: Sehr wahrscheinlich kein High-Risk-System.

Wenn auch nur eine Frage mit „Ja“ beantwortet wird: Das sollten Sie qualifiziert abklären.

High-Risk-KI im KMU – was dann konkret passiert

Konformitätsbewertung: Die zwei Wege

Wer ein High-Risk-KI-System einsetzt oder entwickelt, muss vor dem Inverkehrbringen eine Konformitätsbewertung durchführen. Dafür gibt es zwei Wege:

Weg 1: Interne Konformitätsbewertung (Self-Assessment)

Für die meisten High-Risk-Anwendungen nach Anhang III ist eine interne Bewertung zulässig – ohne externen Prüfer. Das klingt nach Entlastung, bedeutet aber erheblichen Dokumentationsaufwand:

- Technische Dokumentation (Systembeschreibung, Trainingsdaten, Leistungsmetriken)
- Risikomanagementsystem nach Artikel 9 EU AI Act
- Logging und Monitoring-Protokolle
- Erklärung zur menschlichen Aufsicht
- EU-Konformitätserklärung

Als Deployer (also als KMU, das ein fertiges High-Risk-System eines Anbieters einsetzt) sind Ihre Pflichten etwas geringer – aber Verantwortung für den Einsatzkontext, das Monitoring und die Transparenz gegenüber Betroffenen bleibt bei Ihnen.

Weg 2: Externe Konformitätsbewertung durch eine benannte Stelle (Notified Body)

Eine externe Prüfung durch eine akkreditierte Stelle ist verpflichtend bei:

- Biometrischen Identifikationssystemen (Echtzeit oder nachgelagert)
- Bestimmten KI-Systemen im Bereich kritischer Infrastruktur (KRITIS)
- Systemen, für die harmonisierte Normen noch nicht vollständig existieren

Für die meisten KMU, die High-Risk-KI einsetzen (z. B. HR-Software mit automatisiertem Kandidatenscreening), ist Weg 1 der realistischere Einstieg — sofern kein biometrisches System im Einsatz ist.

Benannte Stellen (Notified Bodies): Wer das konkret in DACH ist

Hier ist die ehrliche Einschätzung für 2025/2026: Der Markt für AI-Act-Audits durch offizielle Notified Bodies ist im DACH-Raum noch im Entstehen. Die EU-Kommission führt akkreditierte Stellen in der NANDO-Datenbank, aber Stand Herbst 2025 sind dort für den EU AI Act noch kaum Stellen gelistet. Das wird sich bis 2026/2027 ändern — aber wer heute eine Notified-Body-Prüfung sucht, findet noch keinen funktionierenden Markt mit Preistransparenz.

Bekannte Zertifizierer, die sich für AI-Act-Prüfungen positionieren:

- **TÜV SÜD** — bietet AI-Act-Readiness-Assessments an, positioniert sich als künftiger Notified Body
- **TÜV Rheinland** — ähnliche Positionierung, bereits Beratungsangebote vorhanden
- **TÜV Austria** — relevant für österreichische Unternehmen, AI-Act-Kompetenzaufbau läuft
- **DQS** — bekannt aus ISO-Zertifizierungen, positioniert sich für AI-Act-Konformitätsprüfungen
- **Bureau Veritas** — international aufgestellt, AI-Act-Dienste im Aufbau

In Österreich ist die **Österreichische Akkreditierungsstelle (Akkreditierung Austria, angesiedelt beim BMAW)** die zuständige nationale Stelle für die Anerkennung von Notified Bodies. Österreichische KMU, die eine Notified-Body-Prüfung benötigen, können sich dort über anerkannte Stellen informieren — sobald diese vollständig etabliert sind.

Praktische Einschätzung: Wer jetzt eine High-Risk-Konformitätsbewertung vorbereiten will, startet mit dem Self-Assessment-Weg und begleitet das mit externer Beratung. Den Notified-Body-Markt beobachtet man parallel — für viele KMU wird er erst 2026/2027 wirklich relevant.

Aufsichtsbehörden in Deutschland und Österreich – wer kommt wirklich?

Deutschland

Die Marktüberwachung nach dem EU AI Act ist in Deutschland mehrschichtig geregelt. Die **Bundesnetzagentur** übernimmt die koordinierende Rolle als nationale Marktüberwachungsbehörde. Daneben sind sektorspezifische Behörden zuständig:

- **Bundesagentur für Arbeit** – bei HR-KI und Beschäftigungskontext
- **BaFin** – bei KI-Systemen im Finanz- und Versicherungsbereich
- **Bundesamt für Sicherheit in der Informationstechnik (BSI)** – bei sicherheitskritischen Systemen

Die IHK hat keine Prüfbefugnis, ist aber eine sinnvolle erste Anlaufstelle für Orientierung und Infomaterial – besonders für KMU ohne eigene Compliance-Abteilung.

Realität für KMU 2025/2026: Proaktive Überprüfungen kleiner Unternehmen stehen nicht im Fokus der Anlaufphase. Die Behörden bauen gerade ihre eigenen Strukturen auf. Reaktive Verfahren – ausgelöst durch Beschwerden Betroffener oder durch sicherheitsrelevante Vorfälle – sind wahrscheinlicher als anlasslose Kontrollen. Das bedeutet nicht, dass man Pflichten ignorieren kann, aber die Wahrscheinlichkeit, dass morgen früh ein Prüfer an der Tür steht, ist für Standard-KMU sehr gering.

Österreich

In Österreich ist die Behördenstruktur für den EU AI Act noch im Aufbau. Federführend für die AI-Act-Marktüberwachung ist das **Bundesministerium für Digitalisierung und Wirtschaftsstandort (BMDW)**, die **RTR (Rundfunk und Telekom Regulierungs-GmbH)** wird als mögliche Koordinierungsstelle für digitale Regulierung diskutiert.

Die **Datenschutzbehörde (DSB)** ist bereits jetzt relevant – und zwar überall dort, wo ein KI-System personenbezogene Daten verarbeitet. Hier gibt es eine direkte Überschneidung mit der DSGVO-Aufsicht. Ein KI-System, das Mitarbeiterdaten auswertet oder Kundenprofile erstellt, kann sowohl unter den EU AI Act als auch unter DSGVO-Prüfkompetenz fallen. Wer in diesem Bereich aktiv ist, sollte beide Regelwerke im Blick behalten – mehr dazu im Artikel KI DSGVO-konform einsetzen: Leitfaden für KMU.

Die **WKO** hat keine Prüfbefugnis, baut aber ihre AI-Act-Guidance aktiv aus. Österreichische KMU sollten ihre WKO-Mitgliedschaft aktiv nutzen – die dort verfügbaren Merkblätter und Beratungsangebote werden laufend ergänzt.

Was kostet ein AI Act Audit für ein KMU wirklich?

Die Kostenfrage hängt stark davon ab, welche Risikoklasse Ihr System hat und wie gut Ihre interne Dokumentation bereits ist. Folgende Kostentreiber sind relevant:

- **Risikoklasse des Systems** (High-Risk vs. Limited-Risk)
- **Systemkomplexität** (Eigenentwicklung vs. Drittsoftware)
- **Dokumentationsstand bei Projektbeginn** (von null starten kostet mehr)
- **Ob ein Notified Body notwendig ist** oder Self-Assessment reicht

Realistische Kostenrahmen (Stand 2025, Markt entwickelt sich)

SZENARIO	TYPISCHE KOSTEN
Interne Self-Assessment-Vorbereitung mit externer Beratung	ca. 2.000–8.000 €
Externe Konformitätsbewertung durch Notified Body (High-Risk)	ca. 15.000–50.000 € und aufwärts
Laufende Compliance (Monitoring, Logging, Updates)	ca. 500–2.000 €/Jahr für kleinere Systeme
Reines Beratungsgespräch zur Risikoklassifizierung	ca. 500–2.000 €

Zum Vergleich: CE-Konformitätsbewertungen für Maschinenrichtlinien bewegen sich in ähnlichen Größenordnungen — das gibt einen Anhaltspunkt, auch wenn AI-Act-Prüfungen noch keine etablierten Marktpreise haben.

Wichtige Einschränkung: Für die meisten KMU mit Limited-Risk-KI sind die Hauptkosten Arbeitszeit für interne Dokumentation und einmalige externe Beratung. Kein Pflicht-Audit, keine Notified-Body-Gebühren.

Kostenreduzierende Faktoren:

- Österreichische Förderungen über **aws** und **FFG** können Compliance-Investitionen teilweise abdecken — mehr dazu im Artikel [KI Förderung Österreich 2026: KMU-Leitfaden](#)
- In Deutschland bietet das **BMWK** Digitalisierungsförderungen, die auch Compliance-Vorbereitung einschließen können
- Wenn Ihr KI-Anbieter ein etabliertes System liefert (z. B. Microsoft Copilot, SAP-KI-Funktionen), übernimmt der Anbieter einen Teil der Dokumentationspflichten — prüfen Sie, welche Unterlagen er bereitstellt

Was KMU intern vorbereiten müssen – auch ohne Pflicht-Audit

Interne Vorbereitung ist keine optionale Fleißaufgabe. Auch KMU ohne High-Risk-Systeme haben Dokumentationspflichten, und wer jetzt eine saubere Grundlage legt, spart später erheblich Zeit und Kosten.

Mindest-Dokumentation für jedes KMU – Checkliste:

- 1. **KI-Systeminventur** — Welche KI-Tools werden wo, von wem und für welche Zwecke eingesetzt? (Auch SaaS-Tools zählen)
- 2. **Risikoklassifizierung dokumentieren** — Auch wenn das Ergebnis „kein High-Risk“ ist, sollten Sie diesen Entscheid schriftlich festhalten und begründen
- 3. **Transparenzpflichten umsetzen** — Bei Chatbots und KI-generierten Inhalten müssen Nutzer informiert werden; mehr dazu im Artikel [Transparenzpflichten für KI-Chatbots im KMU](#)
- 4. **Interne Governance klären** — Wer ist verantwortlich, wenn ein KI-System falsche Entscheidungen trifft oder Daten falsch verarbeitet?
- 5. **Datenschutz-Überschneidungen prüfen** — Bei KI-Systemen mit personenbezogenen Daten DSGVO-Konformität sicherstellen
- 6. **Sicherheitsrisiken berücksichtigen** — Gerade bei [KI-Agenten](#) und automatisierten [Workflows](#) lohnt es sich, auch [Sicherheitsrisiken bei KI-Agenten](#) zu kennen
- 7. **Dokumentation laufend aktualisieren** — Wenn ein neues KI-Tool eingeführt wird, gehört die Risikoklassifizierung in den Einführungsprozess

Wichtige Grundregel: Dokumentation jetzt anzulegen ist deutlich günstiger als sie unter Behördendruck oder nach einem Vorfall nachzurüsten.

Zeitplan – bis wann muss was erledigt sein?

DATUM	WAS GILT
Februar 2025	Verbotene KI-Praktiken sind verboten (Unacceptable Risk)
August 2026	Transparenzpflichten aktiv, GPAI -Regeln in Kraft, Aufsichtsbehörden operativ
August 2027	High-Risk-Pflichten vollständig in Kraft, Konformitätsbewertungen für bestehende Systeme erforderlich

Für KMU mit High-Risk-KI bedeutet August 2026 bereits erhöhte Aufmerksamkeit der Behörden — nicht weil sofort Strafen drohen, aber weil Aufsichtsbehörden ab dann operativ tätig sind und auf Beschwerden reagieren können. Die vollständige detaillierte Fristen-Übersicht für KMU finden Sie in einem gesonderten Artikel.

Praktische Konsequenz: Wer 2026 mit der Dokumentation beginnt, hat für High-Risk-Systeme gerade noch ausreichend Zeit bis August 2027 — aber keinen Puffer für Überraschungen.

Österreich vs. Deutschland – die wichtigsten Unterschiede für KMU

Beide Länder setzen denselben EU AI Act um — aber die Umsetzungsstrukturen unterscheiden sich.

Behörden und Zuständigkeiten

ASPEKT	DEUTSCHLAND	ÖSTERREICH
Koordinierende Marktüberwachung	Bundesnetzagentur	BMDW (im Aufbau)
Sektorspezifische Aufsicht	BaFin, BA, BSI	DSB (für datenschutzrelevante KI)
Unternehmensberatung	IHK (keine Prüfbefugnis)	WKO (keine Prüfbefugnis)
Akkreditierung Notified Bodies	DAkKS	Akkreditierung Austria (BMAW)

Förderangebote

In Österreich sind **aws** und **FFG** die zentralen Anlaufstellen für KMU-Förderungen im Digitalisierungs- und KI-Bereich. Die aws bietet Zuschüsse und zinsgünstige Kredite, die FFG fördert Forschungs- und Innovationsprojekte — beides kann für Compliance-Vorbereitung relevant sein.

In Deutschland koordiniert das **BMWK** Digitalisierungsförderungen, das Programm „Digital Jetzt“ ist ein bekanntes Instrument für KMU-Investitionen.

WKO vs. IHK

Österreichische KMU haben über die WKO Zugang zu laufend aktualisierten AI-Act-Merkblättern und können kostenlose Erstberatungen in Anspruch nehmen. Das ist ein praktischer Vorteil, den man nutzen sollte — besonders in der Orientierungsphase.

Steuerliche Behandlung

Compliance-Investitionen können in beiden Ländern als Betriebsausgaben geltend gemacht werden. In Österreich existieren zusätzlich Investitionsfreibeträge, die für digitale Infrastruktur gelten können — konkrete steuerliche Fragen sollten mit dem Steuerberater geklärt werden, da die Einordnung von Compliance-Kosten von Fall zu Fall variiert.

Praxis-Tipp – So gehen Sie es strukturiert an

Die empfohlene Reihenfolge für ein DACH-KMU ohne eigene Compliance-Abteilung:

1. **Inventur** — Alle eingesetzten KI-Tools erfassen (auch eingebettete Funktionen in bestehender Software)
2. **Klassifizierung** — Risikoklasse für jedes System bestimmen und dokumentieren
3. **Lücken identifizieren** — Wo fehlt Dokumentation, wo fehlt Transparenz gegenüber Nutzern?
4. **Externe Beratung** — Für komplexe Fälle oder Unsicherheiten bei der Risikoklassifizierung
5. **Notified Body** — Nur wenn tatsächlich ein externer Audit verpflichtend ist (biometrische Systeme, KRITIS-relevante Bereiche)

Häufiger Fehler: Viele KMU beauftragen zu früh teure externe Auditoren, bevor intern Klarheit über die eigene KI-Systemlandschaft besteht. Das Ergebnis: Die Beratung kostet das Dreifache, weil der Berater erst grundlegende Informationen zusammentragen muss, die intern bereits vorhanden wären.

Ehrliche Einschätzung: Für die meisten DACH-KMU reicht als erster Schritt eine gut strukturierte 2–4-stündige externe Beratung kombiniert mit einer internen KI-Inventur. Das gibt ausreichend Klarheit für eine fundierte Entscheidung über weitere Maßnahmen.

FAQ: Die häufigsten Fragen zu AI-Act-Audits im KMU

Muss mein KMU zwingend einen externen Auditor beauftragen?

Nein — nur High-Risk-Systeme in bestimmten Kategorien (insbesondere biometrische Systeme und KRITIS-relevante Bereiche) brauchen eine externe Konformitätsbewertung durch eine Notified Body. Die Mehrheit der KMU-KI-Anwendungen fällt unter Limited- oder Minimal-Risk und kommt ohne externen Pflicht-Audit aus.

Was ist der Unterschied zwischen einer Konformitätsbewertung und einem Datenschutz-Audit?

Beide Prüfungen können sich überschneiden, wenn ein KI-System personenbezogene Daten verarbeitet — sind aber rechtlich separate Pflichten mit unterschiedlichen Zuständigkeiten. Die Konformitätsbewertung nach EU AI Act prüft die technische und risikobezogene Compliance des KI-Systems. Ein Datenschutz-Audit prüft die DSGVO-Konformität der Datenverarbeitung. Ein System kann beide Prüfungen gleichzeitig betreffen.

Wer ist in Österreich die zuständige Aufsichtsbehörde für den EU AI Act?

Die Zuständigkeiten werden derzeit aufgebaut. Das BMDW ist federführend für die AI-Act-Marktüberwachung. Die Datenschutzbehörde (DSB) ist bei datenschutzrelevanten KI-Systemen bereits jetzt zuständig — das ist die relevanteste Behörde für die meisten österreichischen KMU, solange die AI-Act-spezifische Aufsichtsstruktur noch nicht vollständig operativ ist.

Was kostet ein AI-Act-Audit für ein kleines Unternehmen mit 10 Mitarbeitenden?

Wenn kein High-Risk-System vorliegt: primär interne Arbeitszeit plus optionale Beratungskosten — typisch 1.500–5.000 €. Bei High-Risk-Systemen mit Notified-Body-Pflicht: externe Prüfung ab ca. 15.000 € aufwärts, Preistransparenz ist derzeit noch eingeschränkt.

Gilt der EU AI Act auch, wenn wir nur fertige KI-Tools wie ChatGPT oder Microsoft Copilot nutzen?

Ja — aber mit reduzierten Pflichten. Als Deployer (nicht als Entwickler) tragen Sie vor allem Verantwortung für den Einsatzkontext, die Transparenz gegenüber Nutzern und das interne Monitoring. Die technische Konformität des Systems verantwortet primär der Anbieter. Einen ausführlichen Überblick zu den Pflichten als KMU bietet der Artikel EU AI Act: Was müssen KMU jetzt wirklich tun?.

Nächste Schritte

Drei Erkenntnisse, die Sie aus diesem Artikel mitnehmen sollten:

- **Externe Pflichtprüfung betrifft die wenigsten KMU** — aber interne Dokumentation ist Pflicht für fast alle, die KI einsetzen.
- **Der Markt für AI-Act-Notified-Bodies ist 2025/2026 noch im Entstehen** — wer jetzt einen Notified Body sucht, findet noch keinen funktionierenden Markt mit Standardpreisen.
- **Der sinnvolle erste Schritt** ist eine KI-Inventur kombiniert mit einer qualifizierten Einschätzung der Risikoklassen Ihrer Systeme — nicht ein teures Audit.

Die häufigste Ausgangsfrage, mit der Unternehmen zu uns kommen, lautet: „Bin ich überhaupt betroffen, und was muss ich konkret tun?“ Das ist auch die richtige Frage — und sie lässt sich in einem strukturierten Gespräch deutlich effizienter klären als durch stundenlange Eigenrecherche in Regulierungstexten.

In unserem unverbindlichen 30-Minuten-Beratungsgespräch klären wir gemeinsam, welche Risikoklassen Ihre eingesetzten KI-Systeme haben, wo Handlungsbedarf besteht und welche Schritte für Ihre konkrete Situation realistisch sind — ohne Verpflichtung und ohne Vorabkosten.

Auch wenn Sie noch nicht entscheidungsreif sind: Eine Orientierung jetzt kostet Sie 30 Minuten und kann später erheblichen Aufwand sparen.

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>