// KI-Hub VON STRUKTURAFLOW

COMPLIANCE

EU AI Act: Hochrisiko-KI-Dokumentationspflichten für KMU

Welche KI-Systeme gelten als Hochrisiko? Was müssen österreichische KMU jetzt dokumentieren? Praxisguide mit Checkliste und Aufwandsschätzung.

AUTOR
Strukturaflow-Team

VERÖFFENTLICHT
13. Mai 2026

ONLINE LESEN

https://wissen.strukturaflow.it.com/eu-ai-act-hochrisiko-ki-dokumentationspflicht-oesterreich/

Ein Wiener Personaldienstleister setzt eine Software ein, die Bewerbungen automatisch vorreiht. Ein steirischer Produktionsbetrieb kontrolliert den Zutritt per Gesichtserkennung. Ein Kärntner Leasingunternehmen lässt ein Tool Kreditanfragen vorbewerten. Die Frage, die alle drei beschäftigt: Fällt das unter den EU AI Act — und was müssen sie jetzt tun?

Der EU AI Act ist kein Zukunftsprojekt mehr. Die Verbote nach Art. 5 gelten seit Februar 2025, die Pflichten für Hochrisiko-KI-Systeme greifen ab August 2026 vollständig. Wer jetzt wartet, dokumentiert später unter Zeitdruck — und Nachdokumentation kostet mehr als eine saubere Erststruktur.

Dieser Artikel zeigt Ihnen konkret: Welche Systeme als Hochrisiko eingestuft werden, welche Dokumente Sie anlegen müssen, welche österreichische Behörde kontrolliert — und wie groß der Aufwand für ein KMU realistisch ist.

Was ist überhaupt eine Hochrisiko-KI? Die Definition im EU AI Act

Art. 6 EU AI Act definiert Hochrisiko-KI über zwei Eintrittspforten:

Eintrittspforte 1 — Anhang I: KI-Systeme, die als Sicherheitskomponente in regulierten Produkten eingesetzt werden (z. B. Medizinprodukte, Maschinen, Spielzeug). Diese unterliegen bereits bestehenden EU-Produktsicherheitsvorschriften und müssen von Dritten zertifiziert werden.

Eintrittspforte 2 — Anhang III: KI-Systeme in acht definierten Anwendungsbereichen, die erhebliche Risiken für Gesundheit, Sicherheit oder Grundrechte tragen. Für die meisten KMU ist das die relevante Eintrittspforte.

Die acht Hochrisikobereiche aus Anhang III im Überblick:

1. Biometrische Identifizierung und Kategorisierung
2. Kritische Infrastruktur (Energie, Wasser, Verkehr)
3. Allgemeine und berufliche Bildung
4. Beschäftigung und Personalmanagement
5. Wesentliche private und öffentliche Dienstleistungen (Kredit, Sozialleistungen)
6. Strafverfolgung
7. Migration, Asyl, Grenzkontrolle
8. Justiz und demokratische Prozesse

Für österreichische KMU sind vor allem die Bereiche 1, 4 und 5 praxisrelevant.

Praxisbeispiele aus dem österreichischen KMU-Kontext

HR-Software mit automatisierter Bewerberfilterung fällt unter Anhang III, Nr. 4 (Beschäftigung). Sobald ein System Bewerbungen bewertet, rankt oder aussortiert, ohne dass ein Mensch jede Entscheidung aktiv trifft, ist der Hochrisiko-Tatbestand erfüllt — unabhängig davon, ob die Software zugekauft oder selbst entwickelt wurde.

Kreditscoring-Tools einer Regionalbank oder eines Leasingunternehmens fallen unter Anhang III, Nr. 5 (wesentliche private Dienstleistungen). Automatisierte Kreditwürdigkeitsprüfungen sind damit Hochrisiko, auch wenn ein Sachbearbeiter das Ergebnis formal „absegnet".

Zeiterfassung mit biometrischer Gesichtserkennung und **KI-gestützte Zugangskontrolle** in einem Produktionsbetrieb fallen unter Anhang III, Nr. 1 (biometrische Identifizierung). Hier ist besondere Vorsicht geboten — biometrische Daten sind nach DSGVO auch besonders schützenswerte Datenkategorien. Mehr dazu im Artikel KI DSGVO-konform einsetzen: Leitfaden für KMU.

Wichtig — Anbieter oder Betreiber? Für KMU ist die Rollenunterscheidung nach Art. 3 EU AI Act entscheidend. Wer Standard-Software eines Drittanbieters einsetzt, ist in der Regel **Betreiber** („deployer") — mit weniger Pflichten als der Anbieter/Entwickler. Wer KI selbst entwickelt oder wesentlich anpasst, kann zum **Anbieter** werden und trägt die volle Dokumentationslast.

Kurzer Hinweis zu GPAI: ChatGPT-basierte Tools oder Microsoft Copilot fallen nicht automatisch unter die Hochrisiko-Klassifizierung. Sie können es aber werden, wenn sie in Hochrisiko-Anwendungen eingebettet sind. Die Frage, wie Sie DSGVO und AI Act bei solchen Tools kombinieren, behandelt der Artikel DSGVO & ChatGPT im Unternehmen: Was gilt 2025?.

Die Dokumentationspflichten im Detail – was Annex IV verlangt

Annex IV des EU AI Act definiert die Mindestanforderungen an die **technische Dokumentation** für Anbieter von Hochrisiko-KI-Systemen. Betreiber (die meisten KMU) haben ergänzende, aber weniger umfangreiche Pflichten.

Annex IV Checkliste – die 7 Pflichtelemente für Anbieter

1. **Allgemeine Beschreibung des KI-Systems:** Zweck, Einsatzbereich, Version, Überblick über Trainingsdaten und deren Herkunft.
2. **Beschreibung der Elemente und des Entwicklungsprozesses:** Architektur, eingesetzte Algorithmen, Trainings- und Validierungsverfahren, Datenqualitätsprüfung.
3. **Informationen zu Monitoring, Betrieb und Kontrolle:** Wie wird das System im laufenden Betrieb überwacht? Welche Kennzahlen werden gemessen?
4. **Risikomanagementsystem nach Art. 9:** Dokumentiertes Verfahren zur Identifikation, Analyse und Minimierung von Risiken über den gesamten Lebenszyklus.
5. **Änderungsmanagement und Versionierung:** Nachvollziehbare Dokumentation von Modell-Updates, Datensatz-Änderungen und Anpassungen am System.
6. **Konformitätsbewertungsverfahren:** Entweder interne Bewertung (für die meisten Anhang-III-Systeme möglich) oder Prüfung durch eine Notified Body (bei Anhang-I-Produkten oft verpflichtend).
7. **EU-Konformitätserklärung und CE-Kennzeichnung:** Formale Erklärung, dass das System den Anforderungen entspricht; CE-Kennzeichnung wo gesetzlich vorgeschrieben.

Was müssen Betreiber (also die meisten KMU) zusätzlich bereitstellen?

Als Betreiber kaufen Sie ein Hochrisiko-System ein und setzen es ein. Ihre Pflichten sind geringer als die des Anbieters — aber nicht trivial:

Zweckbestimmung dokumentieren (Art. 26 Abs. 1): Sie müssen schriftlich festhalten, für welchen Zweck Sie das System einsetzen. Diese Zweckbeschreibung darf nicht von den Angaben des Anbieters abweichen — ein häufiger Fehler in der Praxis.

Protokollierung während des Betriebs (Art. 12 / Art. 26): Logs des Systems müssen aufbewahrt werden, soweit Sie darüber Kontrolle haben. Wie lange, hängt vom Anwendungsfall ab — mindestens sechs Monate werden diskutiert.

Menschliche Aufsicht sicherstellen (Art. 14): Sie müssen nachweisbar sicherstellen, dass eine Person die Ausgaben des Systems überprüft und Entscheidungen nicht blind übernimmt. „Der Algorithmus hat das entschieden“ ist keine rechtlich haltbare Position.

Incident-Reporting: Bei schwerwiegenden Zwischenfällen — etwa wenn das System eine Person fehlerhaft kategorisiert hat und daraus ein Schaden entstand — besteht eine Meldepflicht an die zuständige Marktüberwachungsbehörde.

Fundamental Rights Impact Assessment (FRIA): Dieses vertiefte Assessment ist primär für öffentliche Stellen vorgesehen. Private KMU sind in den meisten Fällen nicht direkt verpflichtet — sollten aber dokumentieren können, warum nicht.

Praktische Konsequenz für eingekaufte Software: Sie müssen die Annex-IV-Dokumentation vom Anbieter einfordern und aufbewahren. Wer das nicht tut, kann im Kontrolfall nicht nachweisen, dass er ein konformes System betreibt. Nehmen Sie entsprechende Klauseln in Ihre Softwareverträge auf.

Zeitplan – welche Pflichten gelten wann in Österreich?

DATUM	WAS GILT
02.02.2025	Verbotene KI-Praktiken (Art. 5) in Kraft — z. B. Social Scoring, manipulative Systeme
02.08.2025	GPAI-Pflichten (Art. 51–56) + Governance-Kapitel anwendbar
02.08.2026	Hochrisiko-KI-Pflichten aus Anhang III vollständig anwendbar
02.08.2027	Hochrisiko-KI nach Anhang I (eingebettet in regulierte Produkte)

Für die meisten österreichischen KMU ist der **2. August 2026** der entscheidende Stichtag. Das klingt nach ausreichend Zeit — ist es aber nicht, wenn die Dokumentation von Grund auf neu aufgebaut werden muss.

Wer heute ein Hochrisiko-System beschafft oder entwickeln lässt, sollte die Dokumentationsstruktur sofort anlegen. Annex-IV-konforme Unterlagen nachträglich zu erstellen, ist aufwändiger und fehleranfälliger als ein paralleler Aufbau während der Implementierung.

Österreich-spezifisch: Die nationale Umsetzungsgesetzgebung — insbesondere die Benennung der Marktüberwachungsbehörden und die Festlegung der Sanktionshöhen — war zum Zeitpunkt der Erstellung dieses Artikels (Mitte 2025) noch nicht abgeschlossen. Der EU AI Act gilt als EU-Verordnung direkt, auch ohne nationales Durchführungsgesetz. Aktuelle Informationen finden Sie auf rtr.at und bmdw.gv.at.

Zuständige Behörde in Österreich – wer kontrolliert was?

Der EU AI Act ist eine EU-Verordnung und gilt ohne nationale Umsetzung unmittelbar. Die Mitgliedstaaten müssen aber zuständige Marktüberwachungsbehörden benennen — in Österreich ist dieser Prozess noch im Gang.

Voraussichtliche Behördenstruktur:

- **RTR (Rundfunk & Telekom Regulierungs-GmbH):** Wird für allgemeine KI-Marktüberwachung gehandelt, ist auch für GPAI-Aufsicht im Gespräch.
- **Datenschutzbehörde (DSB):** Zuständig für datenschutzrelevante KI-Anwendungen — und da Hochrisiko-KI fast immer personenbezogene Daten verarbeitet, eine relevante Anlaufstelle.
- **FMA (Finanzmarktaufsicht):** Für Kreditinstitute und Finanzdienstleister bei KI-Anwendungen im regulierten Bereich.
- **AGES / BASG:** Bei Medizinprodukten mit KI-Komponente.

Vergleich Österreich — Deutschland: Deutschland hat die KI-Aufsicht stärker auf bestehende Behörden aufgeteilt — BNetzA für bestimmte Bereiche, BSI für Cybersicherheitsaspekte. Österreich befindet sich noch in der Findungsphase. Die praktische Konsequenz: Beobachten Sie WKO-Mitteilungen und RTR-Updates, beginnen Sie aber nicht erst mit der Dokumentation, wenn die Behördenstruktur steht.

Sanktionen: Art. 99 EU AI Act sieht vor: - Bis zu **35 Mio. EUR oder 7 %** des globalen Jahresumsatzes bei Verstößen gegen Verbote (Art. 5) - Bis zu **15 Mio. EUR oder 3 %** bei Verstößen gegen Hochrisiko-Pflichten - Bis zu **7,5 Mio. EUR oder 1 %** bei unrichtigen Angaben gegenüber Behörden

Für KMU ist in Art. 99 Abs. 6 eine verhältnismäßige Anwendung vorgesehen. Das ist kein Freifahrtschein — aber es bedeutet, dass ein KMU mit erkennbaren Compliance-Bemühungen anders behandelt wird als ein Unternehmen ohne jede Dokumentation.

Praktischer Tipp: Abonnieren Sie den RTR-Newsletter (rtr.at) und die WKO-IT-Recht-Updates. Bei Unsicherheit über Ihre konkrete Situation bietet die WKO eine IT-Recht-Hotline an.

Realitätscheck – wie groß ist der Aufwand für ein KMU wirklich?

Kein Panikmodus, aber auch keine Verharmlosung. Die Aufwandsschätzung hängt stark von Ihrer Rolle und dem Grad der Individualisierung ab.

Betreiber, Standard-Software (häufigster Fall): Sie kaufen eine fertige Lösung ein und setzen sie im vorgesehenen Zweck ein. Ihre Aufgabe: Dokumentation vom Anbieter einfordern, eigene Zweckbeschreibung verfassen, Logging-Prozess einrichten, Aufsichtsverantwortung intern benennen.

Geschätzter Initialaufwand: **8–20 Stunden** Laufender Aufwand: **2–4 Stunden pro Quartal**

Betreiber mit stärkerem Customizing: Sie passen die Software erheblich an, trainieren auf eigenen Daten nach oder integrieren sie tief in eigene Prozesse. Dann brauchen Sie zusätzlich ein eigenes Risikomanagement-Dokument und möglicherweise externen Rechtsrat für Grenzfälle.

Geschätzter Initialaufwand: **20–60 Stunden**

Anbieter / Entwickler (KMU entwickelt selbst oder lässt entwickeln): Vollständige Annex-IV-Dokumentation, internes Konformitätsbewertungsverfahren, gegebenenfalls Einbindung einer Notified Body. Das ist der aufwändigste Fall.

Geschätzter Initialaufwand: **80–200 Stunden intern** Externe Kosten (Beratung, Zertifizierung): **5.000–25.000 EUR** je nach Systemkomplexität

Wichtige Relativierung: Die überwiegende Mehrheit der KMU, die Hochrisiko-KI-Systeme einsetzen, ist in der Betreiber-Rolle. Der Aufwand ist damit deutlich überschaubarer als bei Eigenentwicklungen.

Template-Hinweis: Das EU AI Office und ENISA stellen erste Muster für die technische Dokumentation bereit (aiact.ec.europa.eu, enisa.europa.eu). Diese sind noch nicht vollständig ausgereift, eignen sich aber als Ausgangsbasis für die Dokumentenstruktur.

Schritt-für-Schritt – so starten österreichische KMU mit der Dokumentation

1. Inventur: Alle KI-Systeme erfassen

Erstellen Sie eine Liste aller KI-gestützten Systeme im Einsatz — auch eingekaufte SaaS-Tools. Viele Unternehmen unterschätzen hier die Zahl. Auch ein „intelligentes" Rechnungsprüfungstool oder eine automatisierte Personalplanungs-Software kann betroffen sein.

2. Einordnung: Hochrisiko oder nicht?

Prüfen Sie für jedes System anhand dieser Fragen:

- Fällt der Anwendungsfall unter einen der acht Anhang-III-Bereiche?
- Trifft das System Entscheidungen über Menschen (Bewerbungen, Kredit, Zugang)?
- Verarbeitet es biometrische Daten?
- Ist es in ein Anhang-I-Produkt eingebettet?

Wenn eine dieser Fragen mit „Ja" beantwortet wird: Hochrisiko-Prüfung vertiefen.

3. Rollenklärung: Anbieter oder Betreiber?

Haben Sie das System selbst entwickelt oder wesentlich angepasst? → Anbieter-Rolle, höhere Pflichten. Kaufen Sie eine fertige Lösung ein? → Betreiber-Rolle, ergänzende Pflichten.

4. Dokumentenstruktur anlegen

Mindestdokumente für Betreiber: - Zweckbeschreibung (Art. 26 Abs. 1) - Risikoprotokoll - Nachweis menschlicher Aufsicht - Incident-Log

5. Anbieter kontaktieren

Fordern Sie beim Softwareanbieter aktiv die Annex-IV-Dokumentation und die EU-Konformitätserklärung an. Wenn der Anbieter diese nicht liefern kann oder will, ist das ein ernstes Warnsignal. Nehmen Sie entsprechende Pflichten in Softwareverträge auf — bei Neuabschlüssen ab sofort, bei bestehenden Verträgen bei der nächsten Verlängerung.

6. Internes Review einplanen

Benennen Sie eine verantwortliche Person (IT-Leitung, Compliance-Beauftragter, Geschäftsführung) und planen Sie ein jährliches Review der Dokumentation ein. KI-Systeme ändern sich — die Dokumentation muss mitgehen.

7. Behörden-Updates tracken

RTR-Newsletter, WKO-IT-Recht-Informationen und offizielle Verlautbarungen des AI Office (EU) im Blick behalten. Die Guidance wird in den kommenden Monaten konkreter werden.

Muster-Checkliste Betreiber (zum Kopieren)

- [ ] KI-System-Inventar erstellt
- [ ] Hochrisiko-Einordnung dokumentiert (mit Begründung)
- [ ] Zweckbeschreibung nach Art. 26 Abs. 1 vorhanden
- [ ] Anbieter-Dokumentation (Annex IV) eingeholt und archiviert
- [ ] Logging-/Protokollierungsprozess aktiv
- [ ] Menschliche Aufsicht definiert und nachweisbar
- [ ] Incident-Meldeprozess festgelegt
- [ ] Datenschutzfolgenabschätzung (falls DSGVO-relevant) verknüpft

---

Praxis-Tipp – Dokumentation und DSGVO sinnvoll verbinden

Die meisten Hochrisiko-KI-Systeme verarbeiten personenbezogene Daten. Das bedeutet: DSGVO-Pflichten laufen parallel — Datenschutz-Folgenabschätzung (DSFA), Auftragsverarbeitungsvertrag (AVV), Verarbeitungsverzeichnis.

Der häufige Fehler: Unternehmen führen DSGVO-Dokumentation und AI-Act-Dokumentation getrennt, ohne Querverweise — und haben doppelt so viel Pflegeaufwand.

Die bessere Lösung: Ein einheitliches **KI-System-Register**, das DSGVO-Verarbeitungsverzeichnis, AI-Act-Betreiberdokumentation und Risikoprotokoll in einer Struktur zusammenführt. Das spart Zeit, vermeidet Widersprüche und erleichtert spätere Behördenanfragen.

Wie so ein Register konkret aufgebaut wird und welche Tools sich für KMU eignen, ist stark vom konkreten Betrieb abhängig. Gerade im HR-Kontext — wo Bewerberauswahl, Zeiterfassung und Personalplanung zusammentreffen — lohnt eine strukturierte Betrachtung beider Rechtsebenen. Der Artikel KI DSGVO-konform einsetzen: Leitfaden für KMU gibt dafür eine gute Basis.

Wer bereits den allgemeinen Überblick über den EU AI Act für KMU sucht, findet ihn unter EU AI Act: Was müssen KMU jetzt wirklich tun?.

Nächste Schritte – wann brauchen Sie externe Unterstützung?

Eigenständig machbar ist die Dokumentation für die meisten Betreiber von Standard-Software. Wenn Ihr KI-System klar benennbar ist, der Anbieter eine Konformitätserklärung liefert, keine biometrischen Daten verarbeitet werden und die Zweckbeschreibung unkompliziert ist — dann kommen Sie mit dieser Schritt-für-Schritt-Anleitung und der Muster-Checkliste weit.

Externe Beratung empfehlenswert, wenn:

- Unklar ist, ob Ihr System überhaupt als Hochrisiko gilt (Grenzfälle sind häufiger als gedacht)
- Sie Software stark anpassen oder selbst entwickeln lassen
- Mehrere KI-Systeme im Einsatz sind und eine Gesamtstrategie fehlt
- Ihr Anbieter keine verwertbare Dokumentation liefern kann oder will
- Biometrische Daten, Kreditentscheidungen oder Personalauswahl im Spiel sind

Bei Strukturaflow sehen wir regelmäßig, dass der größte Zeitverlust nicht bei der Dokumentation selbst entsteht — sondern beim Herausfinden, was überhaupt dokumentiert werden muss. Ein strukturiertes Gespräch von 30 Minuten kann diese Orientierungsphase erheblich abkürzen.

Wenn Sie wissen möchten, ob Ihre KI-Systeme unter den EU AI Act fallen und welche Dokumentationsschritte für Ihren konkreten Betrieb sinnvoll sind, bieten wir dafür ein unverbindliches Beratungsgespräch an — ohne Vorbereitung, ohne Agenda außer Ihrer konkreten Situation.

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