// KI-Hub VON STRUKTURAFLOW

COMPLIANCE

EU AI Act & General Purpose AI: KMU-Pflichten erklärt

Was müssen KMU als GPAI-Nutzer wirklich tun? Klare Trennung Anbieter vs. Nutzer, Fristen 2025 und Österreich-Anlaufstellen.

AUTOR
Strukturaflow-Team

VERÖFFENTLICHT
24. Mai 2026

ONLINE LESEN

https://wissen.strukturaflow.it.com/eu-ai-act-general-purpose-ai-kmu-pflichten/

Ihr Unternehmen nutzt ChatGPT für Angebotsentwürfe, Microsoft Copilot für E-Mails, vielleicht ein KI-Tool für den Kundenservice. Dann erscheinen Schlagzeilen: „EU AI Act — GPAI-Pflichten ab August 2025". Die Frage, die Geschäftsführerinnen und IT-Verantwortliche in solchen Momenten stellen: „Betrifft mich das — und wenn ja, was muss ich jetzt konkret tun?"

Die ehrliche Antwort: Für die meisten Unternehmen ist der Handlungsbedarf überschaubar — aber er existiert. Und er hängt stark davon ab, in welcher Rolle Sie KI-Systeme einsetzen.

Dieser Artikel ist keine Rechtsberatung, aber er liefert eine strukturierte Orientierung: Welche Pflichten aus dem EU AI Act treffen Firmen als Nutzer von GPAI-Systemen — und welche richten sich ausschließlich an Anbieter wie OpenAI oder Microsoft. Diese Unterscheidung fehlt in den meisten verfügbaren Erklärungen und führt zu unnötiger Verunsicherung in Betrieben ohne eigene Rechtsabteilung.

Was ist ein General Purpose AI Model überhaupt?

Ein „General Purpose AI Model" (GPAI) ist nach Art. 3 Nr. 63 EU AI Act ein KI-Modell, das für eine Vielzahl unterschiedlicher Aufgaben trainiert wurde und breit einsetzbar ist — im Gegensatz zu spezialisierten Systemen, die genau eine Funktion erfüllen.

Konkrete Beispiele, die in österreichischen und deutschen Betrieben täglich im Einsatz sind: GPT-5o (Basis von ChatGPT), Claude von Anthropic, Gemini von Google, Microsoft Copilot (basierend auf GPT-5) sowie verschiedene Mistral-basierte Lösungen. Eine klassische Spam-Filter-Software oder ein regelbasiertes Buchführungsprogramm mit KI-Unterstützung ist hingegen kein GPAI-Modell — die sind auf spezifische Aufgaben beschränkt.

GPAI-Modell vs. GPAI-System: Was ist der Unterschied?

Der AI Act unterscheidet zwischen dem **Modell** (das Basismodell selbst, z. B. GPT-4o) und dem **System** (einer Anwendung, die auf diesem Modell aufbaut, z. B. ein Kundenservice-Chatbot für Ihr Unternehmen).

Für Unternehmen ist diese Unterscheidung praktisch relevant: Die meisten Betriebe setzen GPAI-Systeme ein — also fertige Anwendungen wie ChatGPT, Copilot oder branchenspezifische KI-Tools — nicht die Rohmodelle direkt. Das hat Auswirkungen darauf, welche Pflichten Sie treffen.

Wer ist Anbieter, wer ist Nutzer? Die entscheidende Unterscheidung für KMU

Dies ist der wichtigste Abschnitt für Ihre praktische Einschätzung. Der EU AI Act unterscheidet klar zwischen zwei Rollen:

ROLLE	DEFINITION	TYPISCHES KMU-BEISPIEL
Anbieter	Entwickelt/trainiert das GPAI-Modell oder bringt es in den EU-Markt	OpenAI, Google, Microsoft — selten ein KMU
Nutzer/Deployer	Setzt ein bestehendes GPAI-System im eigenen Betrieb ein	Buchhaltungsbüro nutzt ChatGPT, Handel nutzt Copilot

Die GPAI-spezifischen Pflichten in Kapitel V des AI Act (Art. 53–55) richten sich primär an Anbieter. Das bedeutet: Ein KMU, das ChatGPT über eine Business-Lizenz für interne Textentwürfe nutzt, ist Nutzer — und nicht direkt von den GPAI-Anbieter-Pflichten betroffen.

Sonderfall: Firmen, die eigene KI-Anwendungen auf GPAI aufbauen

Hier wird es komplexer. Wenn ein Software-KMU ein eigenes Produkt auf Basis der OpenAI-API entwickelt — etwa ein maßgeschneidertes Beratungstool für Kunden — dann schlüpft es teilweise in die Rolle des Anbieters. In diesem Fall greifen Transparenzpflichten nach Art. 52 EU AI Act: Systeme, die synthetische Inhalte (Text, Audio, Bild) erzeugen, müssen Nutzer darüber informieren, dass sie mit einem KI-System interagieren oder KI-generierte Inhalte erhalten.

Die Abgrenzung lautet: Wer die API eines GPAI-Modells nutzt, ohne eigenes Modell-Training durchzuführen, gilt in der Regel als Deployer. Wer das Modell selbst anpasst (Fine-Tuning), entwickelt oder in einem eigenen Produkt weitervertreibt, hat erweiterte Pflichten.

Drei Fragen zur Selbstprüfung — Nutzer oder Anbieter?

- [ ] Nutze ich ein fertiges KI-Produkt (SaaS, API-Zugang) ohne eigenes Training?
- [ ] Gebe ich dieses KI-System nicht als eigenes Produkt an Dritte weiter?
- [ ] Treffe ich keine inhaltlichen Entscheidungen über das Modellverhalten selbst?

Wenn Sie alle drei Fragen mit „Ja“ beantwortet haben: Sie sind Nutzer/Deployer. Die direkten GPAI-Anbieter-Pflichten betreffen Sie nicht.

Was der EU AI Act von GPAI-Nutzern konkret verlangt

Die nüchterne Wahrheit zuerst: Als reiner Nutzer eines GPAI-Systems sind die GPAI-spezifischen Pflichten aus Kapitel V EU AI Act (Art. 53–55) nicht an Sie gerichtet. Diese Verpflichtungen — technische Dokumentation, Einhaltung des EU-weiten Code of Practice, Registrierung im GPAI-Register — treffen OpenAI, Google und Microsoft, nicht Ihr Betrieb.

Was Betriebe als Nutzer trotzdem beachten müssen:

Transparenzpflicht gegenüber Endnutzern (Art. 50 EU AI Act): Wenn Ihr Unternehmen KI-generierte Inhalte erstellt und an Kunden oder Mitarbeitende weitergibt, müssen diese darüber informiert werden. Das gilt beispielsweise für KI-verfasste Kundenantworten, automatisch generierte Berichte oder synthetisch erzeugte Bilder. Die Kennzeichnungspflicht gilt — ein einfacher Hinweis wie „Dieser Text wurde mit KI-Unterstützung erstellt" reicht in vielen Fällen aus.

Einhaltung der Anbieter-Nutzungsbedingungen: KMU müssen sicherstellen, dass sie die Terms of Service des GPAI-Anbieters einhalten. Wenn OpenAI bestimmte Anwendungsfälle ausschließt (etwa bestimmte Entscheidungsautomatisierungen), darf die Firma diese nicht umgehen.

Risikobasierte Prüfung des Anwendungsfalls: Sobald ein GPAI-System für einen Hochrisiko-Anwendungsfall eingesetzt wird, gelten zusätzliche Pflichten — dazu mehr im nächsten Abschnitt.

Ein Unternehmen, dass ChatGPT für Textentwürfe, E-Mail-Formulierungen oder interne Recherchen nutzt, hat heute keinen GPAI-spezifischen Handlungsbedarf über Transparenz beim Output hinaus. Das ist die realistische Einschätzung — ohne Verharmlosung, aber auch ohne übertriebene Panikmache.

Wann wird es ernst? Hochrisiko-Nutzung von GPAI-Systemen durch KMU

Wenn ein GPAI-System für einen Hochrisiko-Anwendungsfall eingesetzt wird, ändert sich die Lage grundlegend. Dann gelten nicht nur die allgemeinen Nutzer-Pflichten, sondern die umfangreichen Anforderungen für Hochrisiko-KI-Systeme nach Titel III des AI Act.

Welche KMU-Anwendungsfälle könnten in diese Kategorie fallen?

- **Personalentscheidungen:** Ein KI-Tool, das Bewerbungen vorreiht, Kandidaten bewertet oder Kündigungsentscheidungen unterstützt — fällt unter Annex III, Punkt 4 des AI Act
- **Kreditwürdigkeitsprüfung:** Automatisierte Bewertung der Kreditwürdigkeit natürlicher Personen — Annex III, Punkt 5
- **Biometrische Identifikation:** Zugangskontrolle per Gesichtserkennung — Annex III, Punkt 1
- **Kritische Infrastruktur:** KI in Energie-, Wasser- oder Verkehrsmanagement
- **Bildung und Berufsausbildung:** Automatisierte Bewertung von Prüfungsleistungen

Ob Ihr konkreter Anwendungsfall als Hochrisiko gilt und was dann zu dokumentieren ist, erklären wir im Detail in unserem Artikel zu EU AI Act: Was müssen KMU jetzt wirklich tun? — dort finden Sie auch die konkreten Dokumentationspflichten für betroffene Betriebe.

Zeitplan und Fristen – was gilt wann für GPAI?

Der EU AI Act ist am 1. August 2024 in Kraft getreten. Die Anwendung ist gestaffelt:

FRIST	WAS GILT	WEN BETRIFFT ES
Februar 2025	Verbote nach Art. 5 (verbotene KI-Praktiken)	Alle — Anbieter und Nutzer
2. August 2025	GPAI-Regeln, Kapitel V (Art. 53–55)	Primär GPAI-Anbieter
2. August 2025	Transparenzpflichten Art. 50	Anbieter und Nutzer/Deployer
2. August 2026	Hochrisiko-Pflichten vollständig anwendbar	Anbieter und Deployer in Hochrisiko-Bereichen
2. August 2027	Übergangsfrist für bestimmte bestehende Hochrisiko-Systeme endet	Anbieter bestehender Systeme

Für GPAI-Modelle, die vor dem 2. August 2025 bereits auf dem Markt waren, gilt eine Übergangsfrist: Anbieter haben bis zum 2. August 2025 Zeit, die Compliance herzustellen.

Die ehrliche Einschätzung: Für KMU, die GPAI-Systeme als Nutzer einsetzen, ändert sich zum 2. August 2025 im Tagesgeschäft wenig. Die Transparenzpflichten nach Art. 50 sind jedoch ab diesem Datum verbindlich — und für Hochrisiko-Deployer beginnt die konkrete Compliance-Vorbereitung jetzt, nicht 2026.

Kostenabschätzung: Was Compliance realistisch kostet

Zahlen, die in den meisten Artikeln fehlen. Drei Szenarien für österreichische und deutsche KMU:

Szenario A: KMU nutzt SaaS-GPAI-Tools (ChatGPT Business, Copilot for Microsoft 365)

Aufwand ist minimal. Primär geht es um eine interne KI-Nutzungsrichtlinie und eine kurze Mitarbeiterschulung. Einmaliger Aufwand: **500–2.000 €** je nach Betriebsgröße. Viele WKO-Vorlagen und öffentliche Muster helfen dabei kostenlos.

Szenario B: Betriebe baut eigene Applikation auf GPAI-API (z. B. kundenspezifisches Tool)

Hier brauchen Sie rechtliche Beratung, eine technische Dokumentation und ggf. eine Datenschutz-Folgenabschätzung. Realistischer Aufwand: **3.000–8.000 €** einmalig, abhängig von Komplexität und ob Sie externe Beratung hinzuziehen.

Szenario C: KMU in Hochrisiko-Bereich (Personalentscheidungen, Kredit, biometrische Systeme)

Umfassende Compliance ist unumgänglich: technische Dokumentation, Konformitätsbewertung, Registrierung im EU-Datenbank, laufende Monitoring-Prozesse. Externe Rechts- und Technologieberatung ist dringend empfohlen. Orientierungswert: **ab 10.000 €** aufwärts, je nach System-Komplexität.

Diese Zahlen sind grobe Orientierungswerte — keine verbindlichen Angebote. Für Digitalisierungs- und Compliance-Maßnahmen sollten österreichische KMU die Förderangebote der Austria Wirtschaftsservice (aws) und des WKO Digital-Programms prüfen. KI-Förderungen in Österreich für 2026 sind ein eigenständiges Thema, das wir separat aufbereitet haben.

Österreich-spezifisch: Anlaufstellen, Behörden und nationale Umsetzung

Dieser Abschnitt fehlt auf den meisten deutschsprachigen Plattformen — und genau deshalb ist er für österreichische KMU besonders wertvoll.

Nationale Marktüberwachungsbehörde in Österreich: Nach aktuellem Stand ist die Rundfunk- und Telekom-Regulierungs-GmbH (RTR) als eine der zuständigen Behörden im Gespräch, ergänzt durch das Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie (BMK) im Kontext der nationalen KI-Strategie. Die finale Behördenstruktur wird durch ein nationales Ausführungsgesetz geregelt, das zum Zeitpunkt der Erstellung dieses Artikels noch in Ausarbeitung ist — überprüfen Sie den aktuellen Stand auf der Website des Digitalisierungsministeriums.

WKO als erste Anlaufstelle für KMU: Die Wirtschaftskammer Österreich bietet über ihr Programm „WKO Digital" Leitfäden, Mustervorlagen und Erstberatungen an. Für viele KMU ist die WKO der praktischste erste Ansprechpartner — ohne Rechtsanwaltskosten, mit direktem Branchenbezug.

Digitalisierungsagentur Austria (DIA): Die DIA begleitet die österreichische KI-Strategie und bietet aufbereitete Informationen für Unternehmen. Website: digital.austria.gv.at.

Vergleich Deutschland: In Deutschland ist die Bundesnetzagentur als koordinierende nationale Behörde für den AI Act vorgesehen. Für DACH-Unternehmen mit grenzüberschreitendem Betrieb lohnt es sich, beide nationale Stellen im Blick zu behalten.

Ähnlich wie bei NIS-2 lohnt es sich, frühzeitig zu prüfen, welche österreichischen Stellen für Ihre Branche zuständig sind — NIS2 / NISG 2026: Auch ohne direkte Pflicht relevant für KMU? zeigt, wie dieser Prozess bei einer vergleichbaren EU-Verordnung aussehen kann.

Self-Assessment in 5 Minuten: Sind Sie als KMU von GPAI-Pflichten betroffen?

Gehen Sie diese drei Blöcke durch — je nach Ergebnis ergibt sich Ihr konkreter Handlungsbedarf.

Block 1: Welche KI-Tools nutzen Sie?

- [ ] Ich nutze ChatGPT, Claude, Gemini oder Copilot im Unternehmen
- [ ] Ich nutze KI-Tools, die auf diesen Modellen aufbauen (z. B. branchenspezifische Lösungen)
- [ ] Ich nutze KI ausschließlich in Form klassischer Automatisierung (regelbasiert, kein generatives KI-Modell)

Wenn Sie die ersten zwei Punkte angekreuzt haben: Sie setzen GPAI-Systeme ein und sind potenziell vom AI Act betroffen.

Block 2: Wie nutzen Sie diese Systeme?

- [ ] Ich nutze fertige SaaS-Lösungen oder API-Zugänge ohne eigenes Modell-Training
- [ ] Ich gebe KI-generierte Inhalte direkt an Kunden oder externe Dritte weiter
- [ ] Ich habe ein eigenes Produkt/Tool entwickelt, das auf einem GPAI-Modell basiert und an Kunden verkauft wird

Wenn Sie Punkt 3 angekreuzt haben: Sie haben teilweise Anbieter-Pflichten — konsultieren Sie eine Rechtsberatung.

Block 3: Für welche Zwecke setzen Sie KI ein?

- [ ] Interne Texterstellung, E-Mails, Dokumentation (kein Hochrisiko)
- [ ] Personalentscheidungen: Bewerber-Screening, Mitarbeiterbeurteilung
- [ ] Kreditentscheidungen oder Bonitätsprüfungen
- [ ] Biometrische Identifikation oder Zugangskontrolle
- [ ] Medizinische oder juristische Empfehlungen als primäre Entscheidungsgrundlage

Auswertung:

- Alle Antworten in Block 1 und 2 zeigen „fertiger Tool-Nutzer“ + Block 3 nur Punkt 1 angekreuzt → Ihr primärer Handlungsbedarf ist eine **interne KI-Nutzungsrichtlinie** und Transparenzkennzeichnung für KI-Outputs. Aufwand: überschaubar.
- Block 3 zeigt Punkte 2–5 → Prüfen Sie, ob Ihr System als Hochrisiko einzustufen ist. Externe Beratung ist sinnvoll.
- Block 2, Punkt 3 angekreuzt → Sie haben Anbieter-Pflichten. Rechtliche Beratung ist notwendig.

Diese Checkliste eignet sich als Grundlage für ein internes KI-Governance-Meeting — drucken Sie sie aus oder teilen Sie sie mit Ihrer IT-Verantwortlichen.

Praxis-Tipp: Ihre Daten sind das Fundament jeder KI-Compliance

Unabhängig davon, ob Sie als KMU Anbieter oder Nutzer sind: Die Qualität und Struktur Ihrer eigenen Daten entscheidet, wie sicher, nachvollziehbar und regelkonform KI-Systeme in Ihrem Betrieb laufen.

Ein konkretes Beispiel aus der Praxis: Ein KMU, das unstrukturierte Kundendaten — Namen, Vertragsdetails, persönliche Notizen — direkt in einen GPAI-Chatbot eingibt, riskiert nicht nur DSGVO-Probleme. Es riskiert auch AI-Act-Compliance-Lücken, weil keine Datendokumentation vorliegt und keine Nachvollziehbarkeit gegeben ist. Wenn eine Behörde später fragt, welche Daten warum in das System eingegeben wurden — kann Ihr Betrieb das beantworten?

Gerade im Umgang mit Mitarbeiterdaten und GPAI-Tools gibt es erhebliche Überschneidungen zwischen AI Act und DSGVO, die wir in DSGVO & ChatGPT im Unternehmen: Was gilt 2025? gesondert aufbereitet haben. Und für alle, die KI-Workflows mit sensiblen Unternehmensdaten absichern wollen, lohnt sich auch ein Blick auf KI-Workflows mit Unternehmensdaten absichern.

Nächste Schritte – Was Sie jetzt konkret tun können

Vier Maßnahmen, die für die meisten KMU sinnvoll und sofort umsetzbar sind:

1. GPAI-Tools im Unternehmen inventarisieren Erstellen Sie eine Liste aller KI-Tools, die in Ihrem Betrieb eingesetzt werden — von ChatGPT bis zur KI-Funktion im CRM. Notieren Sie: Wer nutzt sie, für welche Zwecke, welche Daten werden eingegeben?

2. Eigene Rolle klären: Nutzer oder (auch) Anbieter? Nutzen Sie das Self-Assessment oben. Wenn Sie ein eigenes KI-Produkt entwickeln oder verkaufen, ist eine rechtliche Kurzberatung der nächste sinnvolle Schritt.

3. Anwendungsfälle auf Hochrisiko prüfen Gleichen Sie Ihre Anwendungsfälle mit Annex III des EU AI Act ab. Die oben genannten Kategorien (Personal, Kredit, Biometrie) sind die häufigsten Stolperstellen für KMU.

4. Interne KI-Nutzungsrichtlinie einführen Für die meisten KMU ist das die wichtigste und unmittelbar umsetzbare Maßnahme: eine klare interne Regelung, welche Tools wie genutzt werden dürfen, wie mit KI-generierten Outputs umgegangen wird und wie Mitarbeitende geschult werden.

Bevor Sie sich mit den rechtlichen Feinheiten des AI Acts weiter vertiefen, lohnt ein strukturierter Blick auf den Status quo in Ihrem Betrieb: Welche KI-Tools sind im Einsatz, wer nutzt sie wofür – und wo bestehen bereits Compliance-Lücken? Ein systematischer KI-Audit ist für die meisten KMU der sinnvollste erste Schritt.

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