EU AI Act Compliance Guide

Herausgeber: SimpleAct · https://simpleact.de
Version: 1.0
Kontakt: info@simpleact.de · support@simpleact.de
Stand: März 2026 · Keine Rechtsberatung

Rechtlicher Hinweis

Dieses Dokument ersetzt keine rechtsverbindliche Prüfung. Es ordnet typische EU-AI-Act-Begriffe und -Pflichten für **Unternehmen, die KI einsetzen oder bereitstellen**, ein. Für Ihre konkreten Systeme, Verträge und Zuständigkeiten wenden Sie sich an Ihre Legal- und Compliance-Funktion.

Keywords: EU AI Act, EU KI-Verordnung, AI Compliance, Hochrisiko-KI, KI-Dokumentation, Konformitätsbewertung, Betreiber, Provider, GPAI

Core Problem und SimpleAct-Framework

Core Problem

Organisationen stehen vor dem EU AI Act häufig **ohne durchgängige Kette** von Transparenz bis Nachweis:

- **Pflichten** sind bekannt, aber **Inventar**, **Risikoklasse** und **Rollen** sind nicht überall sauber belegt.
- **Technische Dokumentation** und Freitext liegen verstreut in E-Mails, Drives und Tickets - ohne gemeinsames Schema.
- **Änderungen** an Modellen, Datenflüssen oder Schnittstellen sind für **Audits** und **Management** schwer nachvollziehbar.
- **Tool-Inseln** (DMS, Ticketing) speichern Dateien, ersetzen aber **kein** einheitliches Compliance-Modell.

Das SimpleAct-Framework

SimpleAct ist die **AI Act Compliance Platform** mit einem **gemeinsamen Fünf-Phasen-Referenzmodell** in allen Unterlagen:

Phase	Organisatorischer Fokus	Was SimpleAct zusammenführt
1. Inventar	Transparenz über KI-Systeme, Anbieter, Datenflüsse	Ein **zentrales Register** mit einheitlichen Pflichtfeldern

2. Risiko & Rollen	Risikoklassen, Provider / Betreiber, Lieferkette	**Geführte Einordnung** und dokumentierte Entscheidungen
3. Dokumentation	Inhalte zu Anhang IV, Art. 11 und weiteren Pflichten	**Strukturierte Vorlagen** statt lose Dokumente
4. Nachweise & Export	Revisionssichere Historie, Reports für Legal, Führung, Partner	**Einheitliche Exporte** und nachvollziehbare Änderungen
5. Audit-Readiness	Aktualisierung bei Modell-, Daten- und Produktänderungen	**End-to-End-Kette** statt manueller Ordner- und Ticketinseln

Hinweis: Dieses Framework ist in **allen** SimpleAct-Dokumenten **dieselbe gemeinsame Referenz** - Leitfäden, Checklisten, Inventar und Doku-Vorlagen bauen darauf auf.

---

1. Was der EU AI Act regelt

Die **Verordnung (EU) 2024/1689** (häufig **EU AI Act** oder **EU KI-Verordnung**) legt für **KI-Systeme** in der Union verbindliche Anforderungen fest. Ziele sind u. a. ein hohes Schutzniveau für Gesundheit, Sicherheit und Grundrechte sowie ein funktionierender Binnenmarkt für KI.

Wichtige Bausteine im Alltag von Organisationen:

Begriff	Kurzbedeutung
KI-System	Ein System, das maschinelles Lernen und/oder logikbasierte Ansätze nutzt und je nach Definition unterschiedliche Pflichten auslöst.
Provider (Anbieter)	Entwickelt ein KI-System oder lässt es entwickeln und stellt es unter eigenem Namen bereit.
Deployer / Betreiber	Nutzt ein KI-System unter eigener Verantwortung (außer private, nichtberufliche Nutzung).
Importeur / Händler	Rolle entlang der Lieferkette mit spezifischen Pflichten je nach Kontext.
Hochrisiko-KI	KI-Systeme, die in Anhang III genannte Anwendungsfälle betreffen und die dortigen Kriterien erfüllen (und nicht unter Ausnahmen fallen).

Konformitätsbewertung	Nachweis, dass Pflichten des AI Act erfüllt sind (je nach Risikoklasse und Produktart unterschiedlich).
Technische Dokumentation	Nachweisdokumente, insbesondere für Hochrisiko-KI (u. a. Anhang IV).
Post-Market-Monitoring	Überwachung nach Inverkehrbringen/Inbetriebnahme.
GPAI	General-Purpose AI (Allzweck-KI-Modelle) mit eigenem Kapitel und Transparenz-/Sicherheitslogik.

---

2. Risikopyramide und Pflichtenlogik

Der AI Act arbeitet mit **Risikostufen**. Für die operative Einordnung Ihrer KI-Systeme ist entscheidend: **welche Kategorie** liegt vor und **welche Rolle** Ihre Organisation spielt.

Unzulässiges Risiko

Bestimmte Praktiken sind **verboten** (z. B. je nach Ausgestaltung: unzulässiges **Social Scoring**, bestimmte Formen der **Remote-Biometrie** in öffentlich zugänglichen Räumen u. a. nach Maßgabe der Normen). Hier geht es nicht um "Feintuning", sondern um **keine Nutzung** in der verbotenen Ausprägung.

Hochrisiko-KI

Hochrisiko-KI trifft auf Systeme zu, die in **Anhang III** genannte Bereiche betreffen (z. B. kritische Infrastruktur, Bildung, Beschäftigung, wesentliche private und öffentliche Dienstleistungen, Strafverfolgung, Justiz, demokratische Prozesse - jeweils mit den im Rechtstext definierten Grenzen) **und** die Kriterien für Hochrisiko erfüllen. Für Hochrisiko gelten u. a.:

- **Risikomanagementsystem**
- **Daten- und Daten-Governance** (soweit einschlägig)
- **Technische Dokumentation** (u. a. **Anhang IV**)
- **Protokollierung** (soweit vorgesehen)
- **Transparenz** und **menschliche Aufsicht** (je nach Anwendungsfall)
- **Konformitätsbewertung** und **EU-Konformitätserklärung** (wo anwendbar)
- **Post-Market-Monitoring** und Vorgänge bei **schwerwiegenden Vorfällen**

Keyword-Fokus: Hochrisiko-KI, Anhang III, Anhang IV, technische Dokumentation, EU-Konformitätserklärung, Betreiberpflichten.

Begrenztes Risiko

Hier sind vor allem **Transparenzpflichten** zentral (z. B. Kennzeichnung, Nutzerinformation). Beispiele aus der Praxis: **Chatbots**, **Emotionserkennung** (wo erfasst), **KI-generierte Inhalte** - jeweils nach geltender Legal-Einordnung.

Minimales Risiko

Geringe oder keine spezifischen Pflichten; dennoch empfiehlt sich **freiwillige** Transparenz und interne Governance.

---

3. Rollen: Provider, Betreiber, Lieferkette

Provider (Anbieter)

Typische Pflichten liegen bei **Erstellung der technischen Dokumentation**, **Konformitätsprozess**, **CE-Kennzeichnung** (wo Produktrecht zusätzlich greift), **Qualitätsmanagement**, **Meldewesen** bei Vorfällen - **abhängig** von Produkt und Risikoklasse.

Betreiber (Deployer)

Betreiber müssen u. a. **geeignete menschliche Aufsicht** sicherstellen, **Eingaben** und Nutzung **nach Zweck** steuern, **Protokolle** führen (wo vorgeschrieben), **Vorfälle** melden und bei **wesentlichen Änderungen** nachziehen. **Zugekaufte KI** bleibt relevant: Sie sind oft Betreiber, auch wenn Sie nicht trainieren.

Importeur und Händler

Prüfen Sie **Konformität**, **Kennzeichnung**, **Dokumentation** und **Weitergabe** an nachfolgende Akteure - eng mit Einkauf und Legal verzahnen.

---

4. Technische Dokumentation und Konformität

Für **Hochrisiko-KI** ist die **technische Dokumentation** zentraler Nachweis. Sie strukturiert typischerweise:

- Systembeschreibung, Zweck, **beabsichtigte Nutzer** und **Einsatzgrenzen**
- **Validierung** und **Teststrategie**
- **Daten** (Training, Test, wo relevant)
- **Risikomanagement** und **Überwachung nach Inverkehrbringen**
- **Cybersicherheit** und **Lebenszyklus**

Anhang IV dient als strukturierender Rahmen für den Inhalt der technischen Dokumentation (konkrete Ausgestaltung im Rahmen der verbindlichen Normierung).

Konformitätsbewertung: Je nach Fall interne Bewertung, **Benannte Stelle**, oder Kombination - abhängig von Produkt und Regelwerk.

---

5. GPAI (Allzweck-KI) und Transparenz

GPAI-Modelle unterliegen - je nach Rolle (Provider von Modell, System, downstream) - **Transparenz** und **Dokumentenpflichten** sowie **Sicherheits-/Systemrisiko**-Logik (Stichworte: **Systemrisiko**, **FRIA**-Bezüge in der Praxis). Für SaaS- und Softwareanbieter ist die **Verkettung** aus Basismodell, Produktfeatures und Kundenkonfiguration entscheidend.

Keywords: GPAI, Allzweck-KI, Transparenz, technische Dokumentation Downstream, Lizenzverträge.

---

6. Fristen und Übergang

Die Verordnung schafft **gestaffelte Geltung** (Verbote, GPAI-Regeln, Hochrisiko-Pflichten, Produktbezüge). Nutzen Sie interne **Roadmaps** und **Register** für KI-Systeme, damit **Fristen** und **Nachweise** zusammen gedacht werden - nicht nur "einmalig".

---

7. Wie SimpleAct unterstützt: Die AI Act Compliance Platform

SimpleAct ist **keine reine Einzelsoftware** für ein isoliertes Feature, sondern eine **AI Act Compliance Platform**: Ein durchgängiger Prozess von **KI-Inventar** und **Risikklassifikation** über **Dokumentation** und **revisionssichere Nachweise** bis zu **exportierbaren Reports** für **Audit und Aufsicht**.

Warum "Platform" statt "Tool"?

- **End-to-End:** Ein System, das **alle** relevanten KI-Assets in einem Mandanten abbildet, statt verstreute Tabellen, Tickets und E-Mails.
- **Compliance-by-Design: Pflichtfelder**, **Risikofragen** und **Nachweise** sind strukturiert, nicht "optional".
- **Audit-Readiness: Exporte** (PDF/DOCX) und **Nachvollziehbarkeit** von Änderungen unterstützen **Prüfungen** und **interne Steuerung**.
- **Rollen & Verantwortung:** Abbildung von **Ownership** und **Freigaben** - passend zu Governance-Anforderungen.

Abgrenzung zu generischer Software

- **Ticket-Systeme** erfassen oft Vorgänge, aber **keine** strukturierte **Risikoklasse** und **keine** technische Dokumentation nach Anhang IV.

- **DMS/SharePoint** speichern Dateien, aber **keine** durchgängige **KI-System-Metadaten** mit **Pflichtfeldern** und **Versionierung** der Compliance-Logik.
- **ML-Plattformen** fokussieren Training/Deployment, **nicht** regulatorische **Nachweisketten** für den AI Act.

Was SimpleAct in der Praxis abdeckt (Überblick)

Bereich	Nutzen
KI-Inventar	Vollständige Erfassung inkl. Shadow-AI-Risiko; **Keywords:** KI-Register, AI inventory.
Risikoklassifikation	Geführte Einordnung nach EU-Kategorien; **Anhang III**-Bewusstsein.
Dokumentation	Strukturierung für **technische Dokumentation** und **Betrieb**.
Export & Reports	Nachweise für **Audit**, **Management** und **externe Prüfer**.
Revisionssicherheit	Änderungen nachvollziehbar statt "PDF von gestern".

Preis: Ab **€199/Monat** (bzw. **From €199/month**) - wie auf der Website.

---

8. Glossar (Auswahl)

Begriff	Erklärung
FRIA	Fundamental Rights Impact Assessment - wo relevant, Einbindung von Grundrechten in die Bewertung.
Benannte Stelle	Konformitätsbewertung durch akkreditierte Stelle
CE-Kennzeichnung	Wo Produktrecht greift, Kennzeichnung nach harmonisierten Regeln
Protokollierung	Speicherung von Ereignissen für Nachvollziehbarkeit und Aufsicht
Menschliche Aufsicht	Human oversight - menschliche Kontrolle und Eingriffsmöglichkeiten

---

9. Praxis-Checkliste und typische Fehler

Checkliste (Auszug):

1. Ist jedes **KI-System** im Inventar mit **Owner** und **Zweck** erfasst?
2. Ist die **Risikoklasse** dokumentiert und **begründet**?

3. Liegt für Hochrisiko die **technische Dokumentation** (Anhang IV) in **arbeitbarer** Form vor?
4. Sind **Betreiberpflichten** (Protokolle, Meldungen) geklärt?
5. Sind **Änderungen** (Modell-Update, Datenquelle) **versioniert**?

Typische Fehler:

- **"Wir nutzen nur API"** - ohne Betreiberrolle und ohne Dokumentation.
- **"Excel reicht"** - keine revisionssichere Historie.
- **"Vendor macht alles"** - ohne Nachweis, dass **Ihre** Rolle und **Ihre** Datenflüsse abgedeckt sind.

Anhang A: Detaillierte Rollenmatrix (vereinfacht)

Die folgende Tabelle hilft in Workshops, **wer** welche Artefakte liefern muss. Sie ersetzt keine juristische Einzelfallprüfung.

Thema	Provider-Typische Punkte	Betreiber-Typische Punkte
Zweckbindung / Nutzungskontext	Spezifikation in Dokumentation	Abgleich mit interner Policy
Datengrundlagen	Trainings-/Testdaten-Doku	Zweckbindung bei Eingaben, AV-Verträge
Risiko & FMEA-ähnliche Logik	Risikomanagement-System	Betriebliche Kontrollen
Logging	Spezifikation der Logs	Betrieb, Aufbewahrung, Zugriff
Incident	Meldewege, Fixes	Eskalation, Behördenkontakt wo nötig
Änderungen	Change-Log, Re-Assessment	Freigabe in Produktion

Anhang B: Vertiefung Hochrisiko und Anhang III

Anhang III nennt Anwendungsbereiche, unter denen KI-Systeme **als Hochrisiko** einzustufen sein können, sofern die dortigen Bedingungen erfüllt sind. In der Praxis ist eine **zweistufige Prüfung** sinnvoll:

1. Trifft ein Anwendungsfall **buchstäblich** auf Ihr System zu (z. B. Rekrutierung, Kreditwürdigkeit, kritische Infrastruktur)?

2. Greifen **Ausnahmen** oder Überschneidungen mit anderen Regelwerken ein?

Dokumentieren Sie **Annahmen** und **offene Punkte** explizit - das beschleunigt spätere Audits.

Keywords: Annex III high-risk AI, recruitment AI, critical infrastructure AI, biometric categorization.

Anhang C: FAQ

Frage: Reicht ein Vendor-DPA für AI Act?
Antwort: Verträge sind notwendig, ersetzen aber **keine** technische Dokumentation und **keine** interne Risikobewertung Ihrer Nutzung.

Frage: Müssen wir jedes Chat-Tool inventarisieren?
Antwort: Für **Governance** ja; für **Pflichten** hängt es von Risikoklasse und Rolle ab - ohne Inventar fehlt jedoch die Entscheidungsgrundlage.

Frage: Was ist der Unterschied zwischen "AI Software" und "AI Act Compliance Platform"?
Antwort: Software kann ein Feature sein; eine **Platform** verbindet **Prozess, Daten, Nachweise und Export** zu einem wiederholbaren Compliance-Pfad.
