

EU AI Act für SaaS- und Softwareanbieter

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 Fragen für SaaS- und Softwareanbieter im Kontext des EU AI Act ein. Für Verträge, Produkte und Rollen wenden Sie sich an Legal und Compliance.

Keywords: EU AI Act SaaS, B2B Software KI, Provider Betreiber, Multi-Tenant, DPA Subprozessor, GPAI

Core Problem und SimpleAct-Framework

Core Problem

SaaS- und Softwareanbieter stehen unter einem **Doppeldruck** aus **Produktgeschwindigkeit** und **Regulatorik**:

- **Provider vs. Betreiber** und **Multi-Tenant** sind in **Doku** und **Verträgen** schwer synchron zu halten.
- **Release-Zyklen** und **Modellupdates** brechen **statische** Dokumentationsordner.
- **Kundenkontexte** (Branche, Hochrisiko-Nähe) müssen je **Mandant** abbildbar sein.
- **Lieferketten** (GPAI, **Subprozessoren**) sind im **Nachweis** kaum durchgängig.

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. Ausgangslage SaaS

SaaS-Produkte mit KI-Funktionen verbinden oft:

- **Zentrale Plattform** und **Mandantenfähigkeit** (Multi-Tenant)
- **Schnelle Releases** und Feature-Flags
- **Kundenindustrien** mit unterschiedlichem Risiko (z. B. HR vs. Support-Bot)

Der EU AI Act verlangt Klarheit: **Welche Komponente** ist **hochriskant**, **wer** dokumentiert, **wie** Updates nachvollziehbar bleiben.

2. Rollen im B2B-Kontext

Rolle	Typische Frage
Provider (Sie)	Stellen Sie das KI-System bereit?
Betreiber (Kunde)	Nutzt der Kunde es unter eigener Verantwortung?
Importeur	Falls relevant in der Lieferkette

Fachbegriffe: **Downstream**-Anpassungen, **Feintuning** beim Kunden, **API-only**-Nutzung.

3. Produktarchitektur und Risiko

- Trennen Sie **Basis-Modell**, **Produkt-Layer** und **Kundenkonfiguration**
 - Dokumentieren Sie **Einsatzgrenzen** pro Branche (z. B. keine automatische Endentscheidung ohne Mensch - je nach Produkt)
 - **Annex III**-Use-Cases explizit prüfen, wenn Kunden branchenspezifische Module nutzen
-

4. Verträge: DPA, AVV, Unterauftragsverarbeiter

- **Liste der Subprozessoren** und KI-spezifische Anlagen
- **Zweckbindung** der Datenverarbeitung
- **Audit-** und **Inspektionsrechte**
- **Incident**-Benachrichtigung und SLAs

Keywords: Auftragsverarbeitung Art. 28 DSGVO, TOM, international transfers.

5. Release-Zyklen und "wesentliche Änderungen"

Bei Modell-Updates oder neuen KI-Features:

1. **Change** auslösen
 2. **Risiko** neu bewerten
 3. **Dokumentation** und **Release Notes** für Kunden
 4. **Konformitäts**-Pfad prüfen (intern vs. extern)
-

6. Multi-Tenant und Isolation

- **Tenant-Isolation** technisch und organisatorisch
 - **Logging** pro Mandant
 - **Konfiguration** von KI-Features pro Tenant (Feature Flags)
-

7. GPAI und Allzweck-Modelle

Wenn Sie **GPAI** einbinden: Transparenzpflichten, Dokumentationsketten und ggf. **Systemrisiko**-Themen je nach Rolle - mit Legal klären.

8. Typische SaaS-Fehler

- "Der Kunde ist immer Betreiber" - oft **zu simpel**
 - Keine **Versions**-Historie der KI-Komponenten
 - **Marketing** verspricht mehr als **Dokumentation** hergibt
-

9. Checkliste (Produkt)

- ☐ Inventar aller KI-Module
- ☐ Risiko pro Modul + pro Branchen-Template
- ☐ Doku-Paket für Hochrisiko-Fälle

- ☐ Incident-Prozess mit Kundenkommunikation
 - ☐ Schulungsmaterial für Kunden (Betreiberpflichten)
-

10. Glossar

Begriff	Bedeutung
Tenant	Mandant in Multi-Tenant-SaaS
Feature Flag	Schaltet Funktionen pro Kunde

11. Vertiefung: Customer Success und Compliance

- **Onboarding-Checkliste** für Kunden (Datenklassen, Use Cases)
 - **Health checks** für dokumentierte vs. tatsächliche Nutzung
 - **Quarterly business reviews** mit Compliance-Metriken
-

12. Keyword-Cluster

EU AI Act Softwareanbieter, AI Act B2B SaaS, high-risk AI SaaS, Annex III recruitment, AI vendor documentation.

13. Wie SimpleAct unterstützt

SimpleAct ist die **AI Act Compliance Platform** für **Inventar, Risiko, Dokumentation** und **exportierbare Nachweise** - skalierbar über viele Releases und Mandanten.

Preis: Ab €199/Monat.

Anhang A: Mustervertrag-Anker (mit Legal abstimmen)

- **Leistungsbeschreibung** KI-Feature vs. Basisprodukt
 - **Haftungskappen** und **SLA** für Modellverfügbarkeit
 - **Aufsichtsbehörden**-Benachrichtigung bei schwerwiegenden Vorfällen (Rollen)
-

Anhang B: Release-Checkliste (SaaS)

- ☐ Changelog für Kunden
- ☐ Risiko-Re-Assessment

- ☐ Doku aktualisiert
- ☐ Security Review bei API-Änderung

Anhang C: Branchen-Beispiele (Stichworte)

Branche	Annex-III-Nähe	Hinweis
HR / Recruiting	oft hoch	menschliche Kontrolle
Finanz / Kredit	oft hoch	zusätzliche Finanzregulierung
Support-Bot	oft begrenzt	Transparenz

Anhang D: FAQ

F: Wann müssen Kunden selbst dokumentieren?

A: Wenn sie **Betreiber** sind und **eigene** Daten/Konfigurationen einbringen.

Anhang E: Keyword-Erweiterung

B2B AI compliance platform, SaaS AI Act documentation, multi-tenant AI logging, EU AI Act customer obligations, vendor AI risk.

Anhang F: Integrationsmuster und Nachvollziehbarkeit

Muster	Typische Risiken	Dokumentations-Fokus
REST-API (sync)	Latenz, Timeouts	Request/Response-Schema, Fehlercodes
Batch / ETL	Datenqualität, Drift	Laufpläne, Stichproben, Monitoring
Streaming	Halluzinationen in Echtzeit	Rate-Limits, menschliche Eskalation
Embedded SDK	Version-Split bei Kunden	Mindestversion, Deprecation-Policy

Praxis: Jede Integrationsart braucht einen **eigenen Abschnitt** in der technischen Dokumentation (Schnittstellen, Grenzen, Testnachweise).

Anhang G: Glossar (Kurz)

Begriff	Bedeutung im SaaS-Kontext
---------	---------------------------

Deployer / Betreiber	Oft der Kunde bei On-Prem-Konfiguration
Provider	Sie als Produktanbieter
Substantial modification	Kann neues Konformitätsverfahren auslösen
FRIA	Fundamentale Rechte, oft mit DPIA verknüpft