

Vorlage: KI-System-Inventar (AI Asset Register)

Herausgeber: SimpleAct · <https://simpleact.de>

Version: 1.0

Kontakt: info@simpleact.de · support@simpleact.de

Stand: März 2026 · Keine Rechtsberatung

Rechtlicher Hinweis

Diese Vorlage ersetzt keine rechtsverbindliche Prüfung. Sie hilft, KI-Systeme zu erfassen und zu klassifizieren; verbindliche Einordnung erfolgt im Einzelfall mit Legal und Compliance.

Keywords: KI-Inventar, AI inventory, AI register, Shadow AI, Risikoklassifikation, EU AI Act

Core Problem und SimpleAct-Framework

Core Problem

Ohne belastbares **Inventar** fehlt die **Grundlage** für Risiko und Nachweise:

- **Schatten-KI** und Zulieferer-APIs bleiben **teilweise unsichtbar**.
- **Excel** und Ad-hoc-Listen sind **weder** revisionssicher **noch** auditfähig.
- **Mapping** vom Asset zur **Risikoklasse** fehlt oft.
- Es gibt **keinen Single Source of Truth** für Owner, Versionen und Datenflüsse.

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. Zweck

Ein **KI-Inventar** ist die Grundlage für **Risikoklassifikation**, **Priorisierung** und **Nachweise** gegenüber internen und externen Prüfern.

2. Stammdaten (Pflichtfelder)

Feld	Beschreibung
System-ID	Eindeutige ID im Unternehmen
Name	Produkt- oder Modellname
Provider / Vendor	Anbieter
Version	Release / Modellversion
Owner	Fachverantwortliche Person
Abteilung	Nutzende Organisationseinheit
Zweck	Geschäftlicher Use Case
Datenarten	personenbezogen? sensibel?
Schnittstellen	API, SaaS, On-Prem

3. Risiko & EU AI Act

Feld	Hinweis
Risikoklasse (EU)	minimal / begrenzt / hoch / unzulässig
Begründung	Kurz, auditierbar
Anhang III	Trifft ein Anwendungsfall zu?
GPAI-Bezug	Basismodell / feintuned?

Fachbegriffe: Betreiber, Provider, Hochrisiko-KI, Konformität.

4. Technik & Betrieb

Feld	Beschreibung
Hosting-Region	EU / außerhalb
Modelltyp	LLM, Vision, Tabular, ...
Training	Eigen / Vendor / API-only
Monitoring	Drift, Qualität
Backup / Verfügbarkeit	falls relevant

5. Compliance & Verträge

- **AVV / DPA** vorhanden?
- **Subprozessoren** bekannt?
- **Löschfristen** definiert?
- **Zugriffsbeschränkung** (RBAC)?

6. Shadow AI und Erkennung

Shadow AI: Tools ohne IT-Freigabe. Maßnahmen: Allowlist, Netzwerkmonitoring, Schulung, **Meldekanal**.

7. Review-Zyklus

Frequenz	Aktion
Quartal	Stichprobe Inventar
Bei Release	Neues System erfassen
Bei Vorfall	Eintrag aktualisieren

8. Beispielzeile (anonymisiert)

System-ID	Name	Vendor	Zweck	Risiko
-----------	------	--------	-------	--------

KI-014	HR-Assist	Vendor X	Vorselektion	Hoch (Annex III)
--------	-----------	----------	--------------	------------------

9. Checkliste

- ☐ Alle bekannten KI-Systeme erfasst
- ☐ Owner benannt
- ☐ Risiko begründet
- ☐ Verträge verlinkt
- ☐ Nächstes Review-Datum

10. Glossar

Begriff	Bedeutung
Asset Register	Verzeichnis digitaler Assets
Data lineage	Nachvollziehbarkeit Datenflüsse

11. Vertiefung: Datenflussdiagramm (textuell)

1. **Quelle** -> Rohdaten
2. **Verarbeitung** -> Feature / Prompt
3. **Modell** -> Ausgabe
4. **Nutzung** -> Entscheidung / UI
5. **Speicherung** -> Logs, Retention

12. Keyword-Cluster

KI-Inventar Vorlage, AI system inventory template, EU AI Act register, high-risk AI inventory, shadow AI enterprise.

13. Wie SimpleAct unterstützt

SimpleAct bietet ein **strukturiertes Inventar** mit **Risikoklassen** und **Export** als Teil der **AI Act Compliance Plattform**.

Preis: Ab €199/Monat.

Anhang A: Erweiterte Felder (optional)

Feld	Nutzen
Business Criticality	Priorisierung bei Ressourcenknappheit
PII-Exposure	Datenschutz-Fokus
Model-Provider-Region	Drittland / Schrems II
Kostenstelle	Chargeback / interne Abrechnung

Anhang B: Beispiel-Matrix "Abteilung x Risiko"

Abteilung	Anzahl Systeme	Hochrisiko (geschätzt)
HR		
Sales		
Engineering		

Anhang C: FAQ

F: Wie oft aktualisieren?

A: Quartalsweise + bei jedem **Onboarding** neuer Tools.

F: Was ist mit "Shadow GPT"?

A: Als **Incident** klassifizieren, inventarisieren, Policy nachziehen.

Anhang D: Keyword-Erweiterung

AI asset register, EU AI Act inventory fields, enterprise AI catalog, third-country transfer AI, vendor risk AI.

Anhang E: Datenqualitätsregeln

- Keine **Duplikate** derselben API-Instanz unter verschiedenen Namen
- **Normalisierung** von Vendor-Strings (z. B. "OpenAI" vs. "api.openai.com")
- **Verknüpfung** mit CMDB / ITSM-IDs

Anhang F: IAM, Zugriff und Protokollierung

Aspekt	Inventar-Feld / Hinweis
Authentifizierung	SSO, API-Keys, Service Accounts - wer darf das Modell aufrufen?
Autorisierung	Rollenmodell (RBAC/ABAC), least privilege
Protokolle	Aufbewahrung, Schutz vor Manipulation, Zugriff nur für berechtigte Rollen
Schlüsselrotation	Zyklus und Verantwortliche

Kurz: Ohne klare **Zugriffskette** fehlt oft der Nachweis für **Überwachbarkeit** und **Incident Response** - ergänzen Sie diese Punkte bei jedem produktiven KI-System.
