KI-Governance-Checkliste (EU AI Act)

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

Rechtlicher Hinweis

Diese Checkliste ersetzt keine rechtsverbindliche Prüfung. Sie strukturiert typische Governance-Fragen im Kontext des EU AI Act. Für verbindliche Entscheidungen ziehen Sie Legal und Compliance hinzu.

Keywords: KI-Governance, AI governance, EU AI Act, Compliance, RACI, Audit, Policy, Risk Management

---

Core Problem und SimpleAct-Framework

Core Problem

Governance und **operativer EU AI Act** verlaufen oft **parallel statt verbunden**:

- Policies und RACI landen in **Präsentationen**, **reale KI-Systeme** bleiben in anderen Tools.
- **Freigaben** und Verantwortlichkeiten pro System sind **nicht standardisiert**.
- **Nachweise** für Vorstand, Aufsicht und Audits fehlen in **einheitlichem** Format.
- **Shadow AI** untergräbt den offiziellen Steuerungsansatz ohne sichtbare Korrektur.

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. Governance vs. Compliance

Aspekt	Compliance	Governance
Fokus	Erfüllung konkreter Pflichten	Steuerung, Entscheidungen, Verantwortung
Artefakte	Dokumente, Nachweise	Policies, Rollen, Freigaben
Zeithorizont	Stichtage, Audits	Dauerhafte Steuerung
Typische Frage	"Erfüllen wir Art. X?"	"Wer darf was freigeben?"

Fachbegriffe: Governance Framework, **Three Lines of Defense**, **Policy Lifecycle**, **Risk Appetite**.

---

2. Rollen und RACI (KI-System)

Aktivität	Responsible	Accountable	Consulted	Informed
Inventar-Pflege	IT / AI Owner	CISO / COO	Legal	Management
Risikoklassifikation	AI Owner	Legal/Compliance	DSB	Audit
Freigabe Produktion	Change Board	Produkt	Legal	Support
Incident	SOC / Ops	CISO	Legal	Behörde ggf.

---

3. Policies und Standards

- **KI-Nutzungsrichtlinie** (erlaubte Tools, Shadow-AI-Regeln)
- **Datenklassifikation** und **Zweckbindung**
- **Vendor Management** (DPA, Unterauftragsverarbeiter, GPAI-Bezug)
- **Retention** und **Löschkonzepte**

---

4. Risiko- und Freigabeprozesse

1. **Intake:** Neues KI-System oder Feature melden
2. **Klassifikation:** EU-Risiko + interne Risiko-Score
3. **Freigabe:** Vor Produktion (Change)
4. **Review:** Quartalsweise + bei Modell-Update

Keywords: Change Management, Modell-Update, Wesentliche Änderung, Freigabeprozess.

---

5. Audit und Nachweise

- **Revisionssichere** Historie (kein "PDF von Hand" ohne Version)
- **Export** für Prüfer (Berichte, Snapshots)
- **Playbooks** für Audit-Interviews

---

6. Typische Fehler

- Governance nur auf **Papier**, keine Tool-Unterstützung
- **Kein** zentrales Inventar -> keine Priorisierung
- **Legal** erst nach Launch eingebunden

---

7. Glossar

Begriff	Bedeutung
RACI	Rollenmatrix für Verantwortlichkeiten
Shadow AI	Nicht genehmigte KI-Nutzung
Segregation of Duties	Trennung von Rollen

---

8. Checkliste (kompakt)

- ☐ KI-Inventar vollständig
- ☐ Owner pro System
- ☐ Risikoklasse dokumentiert
- ☐ Freigabe vor Produktion
- ☐ Incident-Prozess definiert
- ☐ Schulung der Fachbereiche

9. Vertiefung: Drei-Linien-Modell

Erste Linie: Fachbereiche nutzen KI und pflegen fachliche Beschreibungen.
Zweite Linie: Compliance/Risk definiert Standards und prüft Stichproben.
Dritte Linie: Interne Revision / externe Prüfung - erhält **strukturierte** Exporte statt Ordner mit PDFs.

---

10. Praxis-Szenarien

Szenario A: Marketing nutzt externes LLM ohne IT-Freigabe -> **Shadow AI**; Maßnahme: Inventar-Pflicht + Allowlist.

Szenario B: Produktteam deployt neues Modell -> **Change** auslösen, Risiko neu bewerten, Dokumentation aktualisieren.

Szenario C: Audit fragt nach **Nachweis** der Risikoklasse -> verweisen auf dokumentierte Begründung + Historie.

---

11. Keyword-Cluster (SEO)

KI-Governance Checkliste, EU AI Act Organisation, AI Act Rollen, Compliance Nachweis, Audit KI, Policy KI, Risk Management KI.

---

12. Wie SimpleAct unterstützt

SimpleAct bündelt **Inventar**, **Risikoklassen**, **Dokumentation** und **exportierbare Reports** in einer **AI Act Compliance Platform** - damit Governance-Entscheidungen auf **Daten** statt auf Excel basieren.

Preis: Ab €199/Monat (siehe Website).

Anhang A: Workshop-Fragen (45 Minuten)

1. Welche **KI-Systeme** sind heute ohne formale Freigabe im Einsatz?
2. Wer ist **Accountable** für ein Hochrisiko-Use-Case in HR?
3. Welche **Nachweise** liegen für die letzte Modelländerung vor?
4. Wie wird **Shadow AI** technisch erkannt (Netzwerk, SaaS-Allowlist)?
5. Welche **KPIs** nutzt das Management (Anzahl Systeme, offene Risiken)?

Anhang B: Erweiterte RACI-Detailtabelle

Aufgabe	R	A	C	I
DPIA / FRIA Trigger	Legal	DSB	IT	Management
Vendor Due Diligence	Procurement	Legal	Security	Owner
Penetrationstest KI-API	Security	CISO	Vendor	Product

Anhang C: FAQ (Vertiefung)

F: Muss die Geschäftsführung KI-Systeme kennen?
A: Mindestens **Kategorien** und **Top-Risiken** - sonst keine fundierte Risikoübernahme.

F: Reicht ein jährliches Audit?
A: Für **stabile** Systeme möglich; bei **monatlichen** Modellupdates ist ein **kontinuierlicher** Review-Prozess sinnvoller.

F: Wie verknüpft man ISO 27001 mit AI Act?
A: ISMS liefert Kontrollen; **AI Act** liefert **domänenspezifische** Pflichten - Mapping in einer **Matrix**.

Anhang D: Keyword-Erweiterung (interne Suche / SEO)

AI Act Governance, EU KI Verordnung Unternehmen, KI Policy Vorlage, AI risk committee, AI Act accountability, compliance evidence AI.

Anhang E: Management-Review (quartalsweise)

Nutzen Sie dieselbe Struktur wie ein **ISMS-Management-Review**, ergänzt um KI-spezifische Kennzahlen:

Prüfpunkt	Frage an die Führung
Transparenz	Kennen wir die **Top 10** KI-Nutzungen nach Risiko?
Ressourcen	Sind Budget und Personal für **Konformität** und **Monitoring** gesichert?
Änderungen	Gab es **wesentliche Änderungen** an Modellen oder Datenflüssen?
Vorfälle	Welche **Incidents** mit KI-Bezug traten auf, und welche **Lessons Learned**?

Fachbegriffe: Managementbewertung, kontinuierliche Verbesserung, Eskalationspfad, Nachweisdokumentation.