



Schatten-KI-Audit-Checkliste

Was Compliance-Verantwortliche jetzt prüfen müssen — konkret, in der Reihenfolge der Audit-Priorität. Basiert auf Art. 4 EU AI Act, DSGVO, ISO 27001 und TISAX-Anforderungen.

Wer diese Checkliste braucht: Compliance-Manager, Datenschutzbeauftragte, Geschäftsführer, CISOs und IT-Leiter in Organisationen mit interner KI-Nutzung. Laut Bitkom gehen 4 von 10 deutschen Unternehmen davon aus, von Schatten-KI betroffen zu sein — und 57 % der Beschäftigten nutzen KI-Tools heimlich (University of Melbourne / KPMG, 2025).

1. KI-Nutzung inventarisieren (sichtbar machen)

- Welche KI-Tools werden im Unternehmen offiziell freigegeben? (Liste mit Name, Anbieter, Zweck)
- Welche Tools werden inoffiziell genutzt? (Mitarbeiter-Umfrage oder Traffic-Analyse)
- Gibt es eine zentrale Übersicht, wer welches Tool mit welchem Account nutzt?
- Werden KI-generierte Inhalte in Kundenkommunikation, Angeboten oder Berichten gekennzeichnet?

2. Richtlinien und Freigabeprozesse

- Existiert eine schriftliche KI-Nutzungsrichtlinie mit Dos und Don'ts?
- Ist geregelt, welche Daten NICHT in öffentliche KI-Tools eingegeben werden dürfen? (personenbezogene Daten, Geschäftsgeheimnisse, Quellcode)
- Gibt es ein Freigabeverfahren für neue KI-Tools vor produktiver Nutzung?
- Ist „Schatten-KI“ als Verstoß im arbeitsrechtlichen Kontext eindeutig adressiert?
- Ist für Agentic-AI-Tools (autonome Agenten wie Claude Code, AutoGPT) ein separater Review-Prozess definiert?

3. Kompetenz-Nachweis (Art. 4 EU AI Act)

- Ist für alle KI-nutzenden Mitarbeiter ein nachweisbarer Kompetenz-Nachweis erbracht?
- Ist der Nachweis personalisiert, mit eindeutiger Nummer und exportierbarem Format?
- Wurde der Nachweis durch einen staatlich zugelassenen Anbieter erbracht? (z. B. ZFU-Zulassung in Deutschland)
- Werden auch neue Mitarbeiter binnen definierter Frist zum Nachweis geführt (Onboarding-Prozess)?
- Ist dokumentiert, wie die Kompetenz getestet wurde? (Prüfung mit Bestehensschwelle, nicht nur Durchklick)

4. Datenschutz und DSGVO

- Ist dokumentiert, welche Datenkategorien in welchem KI-Tool verarbeitet werden?
- Liegt ein AV-Vertrag (Art. 28 DSGVO) mit jedem genutzten KI-Anbieter vor?
- Ist der Drittland-Transfer (USA, China etc.) rechtlich abgesichert? (Standardvertragsklauseln, ausreichende Schutzgarantien)
- Ist eine Datenschutz-Folgenabschätzung (DSFA) für KI-basierte Verarbeitungen durchgeführt?
- Ist „Halluzinations-Risiko“ in der Qualitätssicherung berücksichtigt? (Vier-Augen-Prinzip für KI-Outputs in Kundenkommunikation)

5. Audit-Reporting und Dokumentation

- Gibt es ein zentrales Dashboard zur KI-Governance mit Status je Mitarbeiter, Tool und Richtlinie?
- Sind Kompetenz-Zertifikate als PDF/Excel exportierbar für den Audit-Ordner?
- Wird die KI-Nutzungsrichtlinie regelmäßig (mindestens jährlich) reviewed und kommuniziert?
- Ist ein Meldeprozess für Schatten-KI-Vorfälle definiert? (analog zu Datenschutz-Incidents)
- Sind Bußgeldrisiken im Risikoregister der Organisation bewertet? (EU AI Act: bis 35 Mio € / 7 %; DSGVO: bis 20 Mio € / 4 %)

Auswertung:

< 10 ✓: Hoher Handlungsbedarf. Starten Sie mit Block 1 und 3 parallel.

10–17 ✓: Grundlagen erkennbar, aber Art. 4-Nachweis muss flächendeckend dokumentiert werden.

18+ ✓: Audit-ready. Dokumentation aktuell halten und jährlich reviewen.

Nächster Schritt: Art. 4-Nachweis flächendeckend herstellen

Rechtssicher-KI ist die einzige ZFU-zertifizierte Online-Zertifizierung (Nr. 7566226) für den Kompetenznachweis nach Art. 4 EU AI Act. Pro Mitarbeiter rund 60 Minuten, personalisiertes Zertifikat mit eindeutiger Nummer, zentrales Dashboard zur Audit-Dokumentation.

Einzellizenz: 149 € (inkl. 19 % MwSt) im Direkt-Checkout — ki-rechtssicher.learnworlds.com

Team ab 10 Lizenzen: 125,21 € netto/Lizenz (Staffelrabatte) — rechtssicher-ki.de/fuer-unternehmen