Shadow AI Kurz-Checkliste für Treuhänder (Luxemburg)

Arx Intelligence

2026-03-12

Contents

1 Shadow AI Kurz-Checkliste für Treuhänder (Luxemburg)

Ziel: Treuhand- und Fiduciaire-Teams dabei unterstützen, KI-Tools (z.B. Chat-Assistenten, Dokumenten-Summarizer, Browser-Plugins) mit klaren Leitplanken zu nutzen.

> Diese Checkliste bietet praktische Governance- und Security-Guidance. Sie ist **keine Rechtsberatung**.

1.1 1) Risiko in 60 Sekunden

Die häufigsten KI-Risiken im Treuhand-Alltag: - **Exponierung von Kundendaten** (PII, Finanzdokumente, Steuerunterlagen, Verträge) - **Berufsgeheimnis / Vertraulichkeit** - **Ungeprüfte Tools** („Shadow AI“) ohne Governance - **Kein Audit-Trail**: Was wurde wann wie verarbeitet?

1.2 2) Schnell-Check: Welche Daten sind betroffen?

- ☐ Öffentlich / Marketing
- ☐ Intern (niedrige Sensibilität)
- ☐ Kundendaten (PII: Namen, Adressen, IDs)
- ☐ Finanzdaten (Abschlüsse, Kontodaten)
- ☐ Verträge / rechtliche Dokumente
- ☐ Steuer / Payroll / HR

Faustregel: Wenn es Kundendaten oder vertrauliche Dokumente sind → als **High-Risk** behandeln, bis Kontrollen klar sind.

1.3 3) Checkliste (zum Ausdrucken)

1.3.1 A) Inventar & Ownership

- ☐ Liste der KI-Tools (wer nutzt was, wofür)
- ☐ Governance-Owner benannt (inkl. Vertretung)
- ☐ Neue Tools laufen durch einen leichten Review-Prozess

1.3.2 B) Erlaubt vs. nicht erlaubt

- ☐ Erlaubte Use-Cases definiert (z.B. interne Entwürfe, nicht-sensitive Zusammenfassungen)
- ☐ Nicht erlaubte Use-Cases definiert (z.B. komplette Kundendokumente in öffentliche Tools kopieren)
- ☐ „Red List“ an Datentypen definiert (nie in öffentliche Tools)

1.3.3 C) Accounts & Zugriff

- ☐ Company-Accounts (keine privaten Accounts)
- ☐ Rollenbasierter Zugriff
- ☐ MFA aktiv, wo möglich

1.3.4 D) Vertraulichkeit (Minimum)

- ☐ Mitarbeitende wissen: anonymisieren/redacten
- ☐ Keine Uploads von Source-Dokumenten ohne Freigabe
- ☐ Sensible Dokumente bleiben in kontrolliertem Storage

1.3.5 E) Output-Qualität

- ☐ Menschliche Review vor Versand an Kunden
- ☐ Klar: KI assistiert – Menschen entscheiden

1.3.6 F) Incident-Readiness

- ☐ Vorgehen bei Fehl-Upload bekannt (wer, wie schnell, was tun)
- ☐ Incident-Pfad intern definiert
- ☐ Learnings werden dokumentiert

1.4 4) Mini-Policy (Copy/Paste)

1. Keine Kundendaten/Vertrauliches in öffentliche KI-Tools ohne explizite Freigabe.
2. Company-Accounts nutzen, Zugriff nach Rollen.
3. KI ist Assistenz – Verantwortung bleibt beim Menschen.
4. Verdacht auf Datenexponierung sofort melden.

1.5 5) 48h Audit

Arx Intelligence liefert eine pragmatische Bestandsaufnahme: - Tool-Inventar + Datenfluss-Übersicht - Risiko-Register (priorisiert) - 0–30 / 30–90 Tage Roadmap

Kontakt: arx.luxembourg@gmail.com | calendly.com/arx-luxembourg