Shadow AI Kurz-Checklëscht — Fiduciairë (Lëtzebuerg)

Arx Intelligence

2026-03-12

Contents

1 Shadow AI Kurz-Checklëscht — Fiduciairë (Lëtzebuerg)

Zil: Fiduciaire-Teams hëllefen, KI-Tools (Chat-Assistenten, Dokument-Summarizer, Browser-Plugins) mat kloere Leitplanken ze benotzen.

> Dës Checklëscht gëtt praktesch Guidance (Governance & Sécherheet). **Keng Rechtsberodung.**

1.1 1) Risiko an 60 Sekonnen

Heefeg KI-Risiken am Fiduciaire-Alltag: - **Client-Donnéeën** (PII, Finanzdokumenter, Steier, Kontrakter) - **Berufflecht Geheimnis / Vertraulichkeet** - **Shadow AI** (Tools ouni Review) - **Keen Audit-Trail** (net nozewise wat geschitt ass)

1.2 2) Schnell Klassifikatioun

- ☐ Ëffentlech / Marketing
- ☐ Intern (niddreg Sensibilitéit)
- ☐ Client-PII (Nimm, Adressen, IDs)
- ☐ Finanzdaten
- ☐ Kontrakter / juristesch Dokumenter
- ☐ Steier / Payroll / HR

Faustregel: Client/PII/confidentiel → **High-Risk** bis Kontrollen kloer sinn.

1.3 3) Checklëscht (fir auszdrécken)

1.3.1 A) Inventar & Ownership

- ☐ Lëscht vun KI-Tools (wien, wat, firwat)
- ☐ Governance-Owner (+ Backup)
- ☐ Liichte Review-Prozess fir nei Tools

1.3.2 B) Erlaabt vs net erlaabt

- ☐ Erlaabte Use-Cases definéiert
- ☐ Net erlaabte Use-Cases definéiert
- ☐ “Red List” vun Datentypen (ni an ëffentlech Tools)

1.3.3 C) Accounts & Zougang

- ☐ Company-Accounts (net privat)
- ☐ Rollen-baséiert Zougang
- ☐ MFA wann méiglech

1.3.4 D) Vertraulichkeet (Minimum)

- ☐ Redaction/Anonymiséierung bekannt
- ☐ Keng Uploads vu Client-Dokumenter ouni Freigabe
- ☐ Sensibel Dokumenter am kontrolléierte Storage

1.3.5 E) Output-Qualitéit

- ☐ Mënschleche Check viru Client-Kommunikatioun
- ☐ KI hëlleft – Mënsch ass responsabel

1.3.6 F) Incident-Readiness

- ☐ Prozedur bei Feeler (Upload/Fuite)
- ☐ Eskalatioun intern definéiert
- ☐ Incident-Notizen + Verbesserungen

1.4 4) Mini-Policy (Copy/Paste)

1. Keng Client-PII/confidentiel an ëffentlech KI-Tools ouni Freigabe.
2. Company-Accounts, Zougang no Rollen.
3. KI = Assistenz; Verantwortung bleift beim Mënsch.
4. Bei Zweiwel direkt mellen.

1.5 5) 48h Audit

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