Shadow AI Quick Checklist for Fiduciaires (Luxembourg)

Arx Intelligence

2026-03-12

Contents

1 Shadow AI Quick Checklist for Fiduciaires (Luxembourg)

Purpose: help fiduciary teams use AI tools (e.g., chat assistants, document summarizers, browser plug-ins) with clear guardrails.

> This checklist provides practical governance and security guidance. It is **not legal advice**.

1.1 1) The 60-second risk reality

In fiduciary work, the highest AI risks are usually: - **Client data exposure** (PII, financial docs, tax records, contracts) - **Professional secrecy** / confidentiality obligations - **Unapproved tools** ("Shadow AI") used without governance - **No audit trail**: you cannot prove what happened, when, and why

---

1.2 2) Quick classification (before you start)

1.2.1 What kind of data is involved?

- ☐ Public / marketing content
- ☐ Internal admin content (low sensitivity)
- ☐ Client PII (names, addresses, IDs)
- ☐ Financial statements / bank data
- ☐ Contracts / legal documents
- ☐ Tax / payroll / HR

Rule of thumb: if it's client PII or confidential documents, treat it as high-risk unless you have explicit controls.

1.3 3) The checklist (print-and-use)

1.3.1 A) Inventory & ownership

- ☐ We have a simple list of AI tools in use (who uses what, for what).
- ☐ There is an owner for AI governance (name + backup).
- ☐ New tools require a lightweight review before use.

1.3.2 B) Allowed vs. not allowed

- ☐ We defined **allowed use cases** (e.g., drafting internal emails, summarizing non-sensitive notes).
- ☐ We defined **not allowed use cases** (e.g., pasting full client documents into public tools).
- ☐ We defined a **red list** of data types that should never be pasted into public AI tools.

1.3.3 C) Access & accounts

- ☐ AI tools are used with **company accounts**, not personal accounts.
- ☐ Access is role-based (only those who need it).
- ☐ MFA is enabled where possible.

1.3.4 D) Confidentiality controls (minimum viable)

- ☐ Users know how to anonymize/redact client data when needed.
- ☐ We avoid uploading source documents unless the tool is approved for it.
- ☐ We keep sensitive documents in controlled storage (not in random chat histories).

1.3.5 E) Output quality & human checks

- ☐ AI outputs are always reviewed by a human before sending to clients.
- ☐ We documented where AI is acceptable (assist) vs. where it is not (decide).

1.3.6 F) Logging & incident readiness

- ☐ We know what to do if someone uploads a sensitive file by mistake.
- ☐ We have a simple incident contact path (who to tell, within how long).
- ☐ We keep an internal note of incidents and improvements.

1.4 4) A minimal policy snippet (copy/paste)

AI Use Policy (short): 1. Do not paste client PII or confidential documents into public AI tools unless explicitly approved. 2. Use company accounts and follow role-based access. 3. Treat AI as an assistant: humans remain responsible for decisions and client communications. 4. If you suspect a data exposure, report it immediately to the AI governance owner.

1.5 5) Want a 48h audit?

Arx Intelligence can deliver a fast, pragmatic assessment: - AI tool inventory + data-flow overview - risk register (prioritized) - 0–30 / 30–90 day governance roadmap

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