Checklist Shadow AI (rapide) — Fiduciaires (Luxembourg)

Arx Intelligence

2026-03-12

Contents

1 Checklist Shadow AI (rapide) — Fiduciaires (Luxembourg) 2

1.1 1) La réalité du risque (60 secondes) 2
1.2 2) Classification rapide des données 2
1.3 3) Checklist (à imprimer) 2
1.4 4) Mini-politique (copier/coller) 3
1.5 5) Audit 48h 3

1 Checklist Shadow AI (rapide) — Fiduciaires (Luxembourg)

Objectif : aider les équipes fiduciaires à utiliser des outils IA (assistants de chat, synthèse de documents, plugins navigateur) avec des garde-fous clairs.

> Cette checklist fournit des conseils pratiques (gouvernance & sécurité). **Ce n'est pas un avis juridique.**

1.1 1) La réalité du risque (60 secondes)

Risques fréquents en contexte fiduciaire : - **Exposition de données clients** (PII, documents financiers, fiscalité, contrats) - **Secret professionnel / confidentialité** - **Outils non approuvés** ("Shadow AI") - **Pas de traçabilité** (audit trail)

1.2 2) Classification rapide des données

- ☐ Public / marketing
- ☐ Interne (faible sensibilité)
- ☐ Données clients (PII : noms, adresses, IDs)
- ☐ Données financières
- ☐ Contrats / documents juridiques
- ☐ Fiscalité / paie / RH

Règle simple : si c'est du client/PII/confidentiel → traiter comme **haut risque** jusqu'à validation des contrôles.

1.3 3) Checklist (à imprimer)

1.3.1 A) Inventaire & ownership

- ☐ Liste des outils IA utilisés (qui, quoi, pourquoi)
- ☐ Responsable gouvernance IA identifié (+ backup)
- ☐ Process léger de revue avant adoption d'un nouvel outil

1.3.2 B) Autorisé vs non autorisé

- ☐ Cas d'usage autorisés définis
- ☐ Cas d'usage non autorisés définis
- ☐ Liste "rouge" des données à ne jamais coller dans des outils publics

1.3.3 C) Comptes & accès

- ☐ Comptes entreprise (pas de comptes personnels)
- ☐ Accès basé sur les rôles
- ☐ MFA activée quand possible

1.3.4 D) Confidentialité (minimum)

- ☐ Redaction/anonymisation comprise par l'équipe
- ☐ Pas d'upload de documents clients sans approbation
- ☐ Documents sensibles gardés dans un stockage contrôlé

1.3.5 E) Qualité des sorties

- ☐ Revue humaine avant toute communication client
- ☐ IA = assistante, humain = responsable

1.3.6 F) Incident readiness

- ☐ Procédure en cas d'erreur (upload / fuite suspectée)
- ☐ Circuit d'escalade interne
- ☐ Journal interne des incidents + améliorations

1.4 4) Mini-politique (copier/coller)

1. Ne pas coller de données clients/confidentielles dans des outils IA publics sans approbation.
2. Utiliser des comptes entreprise, accès par rôles.
3. IA = assistance ; la responsabilité reste humaine.
4. En cas de doute, signaler immédiatement.

1.5 5) Audit 48h

Arx Intelligence peut livrer rapidement : - Inventaire + vue des flux de données - Registre des risques (priorisé) - Feuille de route 0–30 / 30–90 jours

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