Checklist AI Act + RGPD

Framework de gouvernance IA — Solopreneurs et startups EU

EuTrustedIA

2026-05-30

Checklist 25 points — AI Act + RGPD pour solopreneurs IA EU

Votre prospect vous demande votre framework de gouvernance IA — vous avez 48 h.

Cette checklist regroupe les **25 points opérationnels** que tout déploiement IA en Europe doit pouvoir documenter pour répondre à un audit prospect, un DPO, ou un contrôle CNIL. Elle est **stratifiée en 5 piliers × 5 points** (extrait du Framework EUDAI v1 publié par EuTrustedIA).

Chaque ligne est un **artefact à produire** ou une **action vérifiable** — pas une déclaration d'intention.

Comment l'utiliser

1. **Coche** les points déjà couverts par votre déploiement actuel
2. **Score** : 1 point par case cochée, total sur 25
3. **Interprète** votre score avec le barème en fin de document
4. Pour automatiser le scoring et générer les livrables (AIPD, registre Art. 30, fiche Art. 50) : utilisez **POSITRONIA-CORE** (audit Local-First, votre code ne sort jamais de votre machine)

Pilier 1 — Souveraineté radicale (5 points)

- ☐ **1.1** Inventaire des sous-traitants traitant vos données (LLM, cloud, base de données, vector store, mailing) avec leur juridiction d'établissement principal
- ☐ **1.2** DPA Art. 28 signé avec chaque sous-traitant identifié au point 1.1 (avec liste des sous-sous-traitants ultérieurs)
- ☐ **1.3** Pour chaque sous-traitant hors UE : CCT (Commission UE 2021/914) + Transfer Impact Assessment documenté
- ☐ **1.4** Pour chaque couche critique (LLM, hébergement, vector store, guards) : **3 alternatives EU** documentées dans un fichier `docs/SOUVERAINETE.md` interne
- ☐ **1.5** Procédure de migration documentée pour chaque dépendance critique (combien de temps + quel coût pour basculer si éviction nécessaire)

Pilier 2 — Conformité auto-démontrable (5 points)

- ☐ **2.1** Registre des traitements Art. 30 tenu à jour (8 mentions obligatoires), outil minimum : un fichier `.csv` versionné Git
- ☐ **2.2** AIPD signée par votre DPO pour chaque traitement à risque élevé (Art. 35), référentiel CNIL : guide AIPD
- ☐ **2.3** Journaux opérationnels IA conservés ≥ 6 mois (logs des prompts, sorties, erreurs)
- ☐ **2.4** Procédure écrite de notification de violation sous 72 h (Art. 33-34) avec contact CNIL et personne-référente interne
- ☐ **2.5** Politique d'auto-démontrabilité publique (si vous êtes une entreprise B2B ambitieuse) : *« on documente comment on s'applique nos propres règles »*

Pilier 3 — Humain dans la boucle final (5 points)

- ☐ **3.1** Cartographie de toutes les **décisions automatisées** prises par votre système avec leur **type d'effet** (juridique, financier, accès service, autre)
- ☐ **3.2** Pour chaque décision à effet juridique : procédure d'intervention humaine documentée (qui, quand, sous quels critères, délai max)
- ☐ **3.3** Notice à la personne concernée (RGPD Art. 13-14) mentionnant explicitement le droit d'opposition (Art. 22) et un canal de contact humain
- ☐ **3.4** Si système haut risque (Annexe III) : surveillance humaine continue documentée (Art. 14 AI Act), formation + autorisation des personnes
- ☐ **3.5** Pour les livrables techniques (AIPD, fiche Art. 50, registre) : **revus et signés par un professionnel qualifié** (DPO / avocat / expert vérifié de l'Annuaire EuTrustedIA)

Pilier 4 — Transparence des données d'entraînement (5 points)

- ☐ **4.1** Inventaire des datasets utilisés en entraînement / fine-tuning / inference avec leur provenance déclarée et leur licence
- ☐ **4.2** Pour chaque dataset : analyse base légale (Art. 6 si données personnelles, Art. 9 si catégories particulières)
- ☐ **4.3** Pour les fine-tunes sur données client : consentement explicite Art. 6.1.a documenté + droit de retrait
- ☐ **4.4** Tests d'**inversion d'anonymat** (memorization attack) sur le modèle final, conformément aux recommandations EDPB Opinion 28/2024
- ☐ **4.5** Notice de transparence vis-à-vis des utilisateurs finaux : *« nous utilisons les modèles X / Y entraînés par les fournisseurs Z / W sur les corpus suivants »*

Pilier 5 — Anti-deepfake et anti-empoisonnement (5 points)

- ☐ **5.1** Système conversationnel ? **Annonce explicite** *« Vous interagissez avec une IA »* à chaque ouverture de session (Art. 50.1)
- ☐ **5.2** Génération de contenu IA ? **Marquage technique** (C2PA pour images, watermark textuel pour textes longs) à partir du **2 août 2026** (Art. 50.2)
- ☐ **5.3** *Deepfake* ou contenu manipulé ? **Divulgation explicite** au consommateur final (Art. 50.4)
- ☐ **5.4** Guard d'entrée filtrant les prompts malveillants (Llama-Guard 3 / Mistral Moderation / équivalent) en série avant le LLM principal
- ☐ **5.5** Tests adversariaux trimestriels documentés (Garak ou équivalent) avec rapport archivé

Barème de score

Score	Interprétation
< 10 / 25	Démarrage urgent. Le retard accumulé devient un risque opérationnel à court terme.
10 à 18 / 25	Conformité partielle. Hiérarchisez les manquements et priorisez les piliers les plus exposés à votre activité.
19 à 23 / 25	Très bonne hygiène. Visez le score plein avant tout audit externe — les 5 ou 6 points restants sont souvent les plus discriminants.
24 à 25 / 25	Vous êtes prêt pour un audit externe ciblé. Vous restez responsable de votre conformité — cette checklist est un guide, pas une garantie juridique.

Et après ?

Si votre score est en dessous de 19/25 — vous avez plusieurs voies :

1. **POSITRONIA-CORE** *(POSITRONIA, ex-Sentinel pendant la cohabitation transitoire)* — scanner Local-First qui audite votre stack IA sur votre machine, sans jamais voir votre code. Génère vos livrables (AIPD pré-remplie, registre Art. 30, fiche Art. 50) en quelques minutes.
2. **Framework EUDAI v1 complet** — le livre blanc 143 KB qui documente les 5 piliers en profondeur, avec arbre de décision pre-build et stack recommender souverain EU. Téléchargeable sur eutrustedia.eu/eudai.
3. **Annuaire EuTrustedIA** — pour les points qui nécessitent la signature d'un professionnel (DPO, avocat tech), trouvez un expert vérifié EU sur eutrustedia.eu.

Votre engagement avec EuTrustedIA est piloté par vous : on documente, on génère les livrables, on vous met en relation avec les experts qui signent. Nous ne certifions pas — nous outillons votre auto-démontrabilité.

Mentions

Contact : `contact@eutrustedia.eu` · eutrustedia.eu

Marquage AI Act Article 50 — ce document a été rédigé par un humain à partir d'un cadre documentaire publié par EuTrustedIA. Aucun contenu de cette checklist n'a été généré par IA générative.