EPIC 7 — Kit conformité & audit RGPD (IA)

---

1. Objectif de l'EPIC

Fournir un **kit de conformité RGPD complet, cohérent et audit-ready** pour une plateforme IA manipulant des **données sensibles**, afin de :

- démontrer la conformité lors d'un **contrôle** (CNIL, client, DPO, RSSI),
- outiller les équipes **produit, technique et juridique** avec des procédures claires,
- garantir la **transparence** vis-à-vis des utilisateurs finaux et des clients B2B.

📌**Cadre RGPD**
Cet EPIC consolide les exigences transverses du RGPD (articles **5, 12–14, 24, 25, 30, 32, 35**) et les **preuves associées**.

Il **n'introduit aucune nouvelle fonctionnalité applicative**, mais formalise, documente et rend **auditables** les mécanismes mis en œuvre dans les **EPIC 1 à 6**.

---

2. Positionnement dans la roadmap

- EPIC 1 — Socle applicatif sécurisé
- EPIC 2 — Durcissement serveur & réseau
- EPIC 3 — Validation technique IA locale (POC contrôlé)
- EPIC 4 — Stockage IA & données utilisateur RGPD
- EPIC 5 — Pipeline RGPD (droits des personnes)
- EPIC 6 — Stack IA Docker RGPD-ready (industrialisation)
- **EPIC 7 — Kit conformité & audit (ce document)**

📌EPIC 7 constitue la **dernière étape** de la roadmap et rend la plateforme **vendable, auditable et contractualisable**.

---

3. Périmètre couvert

Inclus

- Registre des traitements (art. 30 RGPD)
- DPIA — Analyse d'impact relative à la protection des données (art. 35 RGPD)
- Information des personnes & transparence (art. 12–14 RGPD)
- Procédures internes RGPD (art. 24 RGPD)
- Playbooks incident et violation de données (art. 33–34 RGPD)
- Dossier de preuves d'audit technique et organisationnel
- **Documentation du bootstrap plateforme et de la gouvernance multi-tenant**

Exclus

- Développements techniques (couverts par EPIC 1 à 6)
- Exploitation quotidienne détaillée (Ops récurrents)

---

4. Principes directeurs (non négociables)

- Traçabilité documentaire complète
- Cohérence stricte avec l'implémentation réelle
- Lisibilité pour un **auditeur non technique**
- Mise à jour continue et versionnée
- Centralisation des preuves

---

5. Composants du kit conformité

A. Registre des traitements — art. 30 RGPD

Objectif : décrire de manière exhaustive les traitements IA réalisés par la plateforme.

Contenu minimal : - Finalités des traitements IA - Catégories de données traitées (réf. `DATA_CLASSIFICATION.md`) - Catégories de personnes concernées - Bases légales - Durées de conservation - Mesures de sécurité (réf. EPIC 1 & 2) - Sous-traitants éventuels

📄Artefact attendu : `docs/rgpd/registre-traitements.md`

B. DPIA — Analyse d'impact (art. 35 RGPD)

Objectif : évaluer et réduire les risques pour les droits et libertés des personnes.

Contenu : - Description détaillée des traitements IA - Analyse de nécessité et de proportionnalité - Identification des risques - Mesures techniques et organisationnelles - Décision résiduelle (acceptation / refus / mesures complémentaires)

📄Artefact attendu : `docs/rgpd/dpia.md`

C. Information des personnes & transparence (art. 12–14 RGPD)

Éléments fournis : - Politique de confidentialité claire et accessible - Mentions spécifiques IA (finalités, logique générale) - Références aux droits RGPD et modalités d'exercice

📄Artefact attendu : `docs/rgpd/privacy-policy.md`

📌 Les écrans UI de gestion des droits sont implémentés dans EPIC 5 ; EPIC 7 en fournit la **documentation**.

D. Procédures internes RGPD (art. 24 RGPD)

Procédures documentées : - Gestion des demandes RGPD - Gestion des accès internes - Revue périodique des traitements - Onboarding / offboarding collaborateurs - Gouvernance multi-tenant (plateforme vs clients)

📄Artefact attendu : `docs/runbooks/rgpd-procedures.md`

E. Gestion des violations de données (art. 33–34 RGPD)

Playbooks : - Détection et qualification d'un incident - Mesures immédiates - Notification à l'autorité de contrôle - Communication aux personnes concernées - Journal des incidents

📄Artefact attendu : `docs/runbooks/incident.md`

F. Dossier de preuves d'audit

Objectif : permettre une réponse rapide et structurée à tout audit.

Contenu : - Architecture et schémas (EPIC 1, 2, 6) - Extraits de logs RGPD-safe - Historique des consentements (EPIC 5) - Historique des demandes RGPD (EPIC 5) - Résultats des tests sécurité et RGPD - **Preuves du bootstrap plateforme (EPIC 1)**

📄Artefact attendu : `docs/audit/evidence.md`

---

6. Scripts et preuves automatisées

📌EPIC 7 s'appuie sur des **scripts de collecte de preuves**, sans génération dynamique de code.

Fonctions : - Collecte des rapports de tests RGPD - Collecte des résultats de scans sécurité - Vérification des invariants (no bypass LLM, no sensitive logs) - Génération d'artefacts CI versionnés

📄Emplacement : `scripts/audit/*`

Les scripts sont exécutés manuellement ou via CI et produisent des **preuves statiques exploitables**.

---

7. User Stories & exigences

US-1 — Registre des traitements à jour

Exigences : - Modèle standardisé - Mise à jour à chaque évolution majeure - Versionnement

---

US-2 — DPIA exploitable

Exigences : - Format structuré - Liens explicites avec EPIC 1 à 6 - Décisions tracées

---

US-3 — Information utilisateur transparente

Exigences : - Langage clair - Documents accessibles - Mise à jour contrôlée

---

US-4 — Procédures internes opérationnelles

Exigences : - Procédures écrites - Responsabilités définies - Tests périodiques

---

US-5 — Dossier d’audit prêt

Exigences : - Dossier centralisé - Accès restreint - Preuves à jour et traçables

---

8. Dépendances

- Dépend de : **EPIC 1 à EPIC 6**
- Dernière EPIC de la roadmap

---

9. Livrables

- Registre des traitements complété
- DPIA validé
- Politique de confidentialité
- Procédures RGPD documentées
- Playbooks incident
- Dossier d’audit consolidé
- Scripts de preuves fonctionnels

---

10. Risques & points de vigilance

- Décalage entre documentation et implémentation réelle
- DPIA non mis à jour après évolution
- Procédures non connues des équipes
- Preuves incomplètes ou obsolètes

---

11. Definition of Done (DoD)

- Kit conformité complet, cohérent et versionné

- Documentation alignée avec la stack réelle
- Bootstrap plateforme documenté et auditable
- Scripts de preuves exécutables
- Prêt pour audit externe (CNIL / client / DPO)

Fin EPIC 7