


EPIC 5 — Pipeline RGPD (droits des personnes)

1. Objectif de l'EPIC

Mettre en place un **pipeline RGPD opérationnel** permettant l'exercice effectif et traçable des **droits des personnes concernées** (utilisateurs finaux et personnes dont les données sont traitées via l'IA), conformément au RGPD.

Ce pipeline garantit : - le **recueil et la gestion du consentement**, - la **journalisation conforme** des traitements, - l'**effacement maîtrisé** des données, - l'**export structuré et sécurisé** des données, - la **preuve de conformité** en cas de contrôle.

 **Cadre RGPD** : cet EPIC met en œuvre les obligations relatives aux **droits des personnes** (articles 7, 12 à 23 du RGPD). Les mesures de sécurité infra relèvent d'**EPIC 2**, la structuration du stockage d'**EPIC 4**.

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 (ce document)**
 - EPIC 6 — Stack IA Docker RGPD-ready (industrialisation)
 - EPIC 7 — Kit conformité & audit
-

3. Périmètre couvert

Inclus

- Gestion du consentement utilisateur
- Journalisation RGPD des traitements
- Droit d'accès et de portabilité
- Droit à l'effacement (suppression logique et crypto-shredding)
- Orchestration des demandes RGPD
- Preuves de conformité et audit

Exclus

- Sécurité infra bas niveau (EPIC 2)
 - Gouvernance des accès applicatifs (EPIC 1)
 - Déploiement technique de la stack IA (EPIC 6)
-

4. Principes directeurs (non négociables)

1. Exercice effectif et vérifiable des droits
 2. Traçabilité complète sans exposition de données sensibles
 3. Délai de traitement maîtrisé
 4. Effacement réaliste et juridiquement défendable
 5. Automatisation maximale du pipeline RGPD
-

5. Droits RGPD couverts

- Information et transparence
 - Consentement explicite
 - Droit d'accès
 - Droit de rectification (si applicable)
 - Droit à l'effacement
 - Droit à la portabilité
 - Droit à la limitation du traitement
-

6. User Stories & Exigences

US-1 — Recueil et gestion du consentement

Je veux recueillir un consentement explicite et traçable

Exigences - Consentement non pré-coché - Information claire (finalité, durée, modèles IA) - Horodatage et versionnement - Révocation possible à tout moment

US-2 — Journalisation RGPD des traitements

Je veux disposer de preuves de traitement conformes

Exigences - Logs orientés événements - Aucune donnée métier en clair - Références anonymisées - Horodatage fiable

US-3 — Droit d'accès et de portabilité

Je veux fournir un accès structuré aux données

Exigences - Données regroupées par utilisateur - Format structuré (JSON, CSV) - Export chiffré - Lien à durée de vie limitée

US-4 — Droit à l'effacement

Je veux effacer les données de manière conforme et réaliste

Exigences - Suppression logique immédiate - Purge différée selon rétention - Crypto-shredding des clés
- Traçabilité de l'opération

US-5 — Orchestration des demandes RGPD

Je veux orchestrer les demandes RGPD de bout en bout

Exigences - Authentification renforcée du demandeur - Workflow de validation - Délais réglementaires respectés - Journal des actions

US-6 — Preuve de conformité

Je veux démontrer la conformité en cas d'audit

Exigences - Historique des consentements - Historique des demandes RGPD - Preuves horodatées - Export audit dédié

7. Dépendances

- Dépend de : EPIC 1, EPIC 2, EPIC 4
 - Alimenté par : EPIC 3 (contraintes techniques)
 - Prérequis pour : EPIC 6, EPIC 7
-

8. Livrables

- Mécanisme de consentement opérationnel
 - Journal RGPD des traitements
 - Pipeline d'effacement fonctionnel
 - Export RGPD sécurisé
 - Documentation RGPD prête
-

9. Risques & points de vigilance

- Mauvaise identification du demandeur
 - Effacement techniquement irréaliste
 - Journalisation trop verbeuse
 - Délais non respectés
-

10. Definition of Done (DoD)

- Consentement traçable actif
- Export RGPD fonctionnel

- Effacement vérifiable
 - Preuves d'audit disponibles
 - Délais RGPD respectés
-

Fin EPIC 5