EPIC 6 — Stack IA Docker RGPD-ready (industrialisation)

1. Objectif de l'EPIC

Industrialiser le déploiement de la **stack IA locale** au moyen de **conteneurs Docker**, afin de fournir un environnement **reproductible, sécurisé et conforme RGPD**, prêt pour une exploitation en production sur des métiers à données sensibles.

Cette stack doit : - implémenter strictement les règles définies dans les EPIC 1 à 5, - garantir l'isolation des composants, - permettre l'observabilité et la maintenance, - rester compatible avec des modèles IA locaux ou contrôlés.

📌**Cadre RGPD** : cet EPIC met en œuvre les exigences techniques découlant des articles **25 (privacy by design)** et **32 (sécurité du traitement)** du RGPD, en application opérationnelle des EPIC précédents.

---

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 (ce document)**
- EPIC 7 — Kit conformité & audit

---

3. Périmètre couvert

Inclus

- Orchestration des services via Docker / Docker Compose
- Déploiement du backend applicatif
- Déploiement de la Gateway LLM
- Déploiement des modèles IA locaux
- Déploiement des bases de données et bases vectorielles
- Gestion des volumes chiffrés
- Observabilité (logs techniques, métriques)

Exclus

- Durcissement OS et réseau hôte (EPIC 2)
- Gouvernance des accès applicatifs (EPIC 1)
- Règles de stockage et rétention (EPIC 4)
- Droits RGPD et workflows légaux (EPIC 5)

---

4. Principes directeurs (non négociables)

1. **Reproductibilité des environnements**
2. **Isolation stricte des services**
3. **Aucun flux réseau non maîtrisé**
4. **Volumes chiffrés par défaut**
5. **Observabilité sans fuite de données**

---

5. Architecture cible (vue stack)

- Reverse proxy TLS (en frontal)
- Backend applicatif (API)
- Gateway LLM
- Runtime IA local (ex : Ollama)
- Base relationnelle
- Base vectorielle
- Services d'observabilité

Tous les services communiquent sur un **réseau interne Docker isolé**.

---

6. User Stories & Exigences

US-1 — Orchestration Docker sécurisée

Je veux déployer la stack de manière reproductible

Exigences - Fichiers Dockerfile versionnés - Docker Compose documenté - Environnements séparés (dev / test / prod) - Aucun secret en clair dans les images

---

US-2 — Isolation des services

Je veux empêcher toute communication non autorisée entre services

Exigences - Réseaux Docker dédiés - Pas d'exposition directe des services internes - Ports exposés strictement nécessaires

---

US-3 — Volumes chiffrés

Je veux protéger les données persistées

Exigences - Volumes chiffrés au repos - Séparation des volumes par type de donnée - Accès restreint par service

---

US-4 — Déploiement des modèles IA

Je veux exécuter des modèles IA locaux de manière contrôlée

Exigences - Modèles packagés ou montés explicitement - Aucun téléchargement automatique non contrôlé - Ressources limitées par conteneur

---

US-5 — Observabilité RGPD-safe

Je veux surveiller la stack sans exposer de données personnelles

Exigences - Logs techniques uniquement - Métriques système (CPU, RAM, latence) - Aucune donnée métier dans l'observabilité

US-6 — Séparation des environnements

Je veux éviter toute contamination entre environnements

Exigences - Configurations distinctes - Données non partagées - Accès restreints

---

7. Dépendances

- Dépend de : EPIC 1, EPIC 2, EPIC 4, EPIC 5
- Alimenté par : EPIC 3 (retours POC)
- Prérequis pour : EPIC 7

---

8. Livrables

- Stack Docker documentée
- Fichiers Compose versionnés
- Volumes chiffrés opérationnels
- Observabilité en place
- Procédure de déploiement

---

9. Risques & points de vigilance

- Mauvaise isolation Docker → fuite de données
- Secrets exposés dans les images
- Logs trop verbeux

---

10. Definition of Done (DoD)

- Déploiement reproductible
- Aucune communication non autorisée
- Données chiffrées au repos
- Observabilité conforme RGPD
- Stack prête pour exploitation

Fin EPIC 6