

00 — Analyse de l'objectif (version alignée EPIC 1→7)

1. Objectif global reformulé

Mettre en place une **plateforme applicative IA auto-hébergée**, destinée à des **métiers réglementés manipulant des données sensibles** (comptables, avocats, médecins), permettant : - d'activer des **outils IA spécialisés cœur de métier** (agents, orchestrateurs, automatisations), - via une **UI utilisateur sécurisée** (Next.js), - avec une **architecture FULL RGPD**, sans dépendance non maîtrisée à des services tiers.

L'ensemble doit être **audit-ready**, industrialisable, et conforme aux exigences CNIL.

2. Contraintes majeures (non négociables)

Conformité RGPD stricte

- Données personnelles et sensibles (santé, finance, juridique)
- Privacy by design & by default
- Droits des personnes effectifs (accès, effacement, portabilité)
- Traçabilité complète sans fuite de données





IA sous contrôle

- Modèles IA **locaux ou strictement contrôlés**
- Aucun appel IA direct depuis le front ou le code métier
- Passage obligatoire par une **Gateway LLM**
- Possibilité de fonctionner **sans internet**

Sécurité & auditabilité

- Hébergement en France / UE
 - Infra durcie (réseau, OS, chiffrement)
 - Journaux exploitables en audit
 - Documentation légale complète
-

3. Enjeux clés identifiés

-  Éviter toute illusion de conformité "IA locale = RGPD"
 -  Éviter le mélange infra / app / RGPD / IA
 -  Séparer clairement responsabilités et périmètres
 -  Construire une chaîne de conformité démontrable
-

4. Découpage stratégique retenu

Le projet est structuré autour de **7 EPIC ordonnés**, chacun correspondant à un pilier de conformité et de robustesse.

EPIC	Rôle
EPIC 1	Gouvernance applicative & Gateway IA (art. 25 RGPD)
EPIC 2	Sécurité infra & réseau (art. 32 RGPD)
EPIC 3	Validation technique IA locale (POC contrôlé)
EPIC 4	Stockage des données IA & utilisateur
EPIC 5	Pipeline RGPD (droits des personnes)
EPIC 6	Industrialisation Docker
EPIC 7	Kit conformité & audit

5. Résultat attendu

- Une plateforme **techniquement robuste**
- Une conformité **juridiquement défendable**
- Une architecture **évolutive et maîtrisée**
- Un socle réutilisable pour plusieurs métiers

Document de cadrage stratégique — source de vérité projet