EPIC 1 — Socle applicatif sécurisé (RGPD by design)

---

1. Objectif de l'EPIC

Mettre en place le **socle applicatif sécurisé** de la plateforme IA, garantissant :

- une **architecture multi-tenant stricte** (B2B, métiers à données sensibles),
- une **gestion des identités et des droits robuste** (IAM, RBAC / ABAC),
- une **gouvernance RGPD by design et by default** (minimisation, traçabilité, auditabilité),
- une **intégration IA strictement contrôlée** via une **Gateway LLM unique**,
- une **base applicative saine, testable et vérifiable** servant de fondation à tous les EPIC suivants.

📌**Cadre RGPD**
Cet EPIC met en œuvre les principes de protection des données dès la conception et par défaut (article 25 du RGPD). Les mécanismes opérationnels d'exercice des droits des personnes concernées (consentement, accès, effacement, portabilité) sont **hors périmètre** et traités dans **EPIC 5**.

Cet EPIC constitue un **prérequis absolu** à tout développement IA ou métier.

---

2. Positionnement dans la roadmap

- **EPIC 1** — Socle applicatif sécurisé (ce document)
- EPIC 2 — Durcissement serveur & réseau (Ops/Sec RGPD)
- 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

---

3. Périmètre couvert

Inclus

- Architecture **multi-tenant stricte** (organisation / cabinet / clinique / étude)
- Authentification et gestion des identités (**IAM**)
- Autorisation fine (**RBAC / ABAC**)
- Gouvernance des accès aux fonctionnalités IA
- Journalisation **RGPD-safe**
- Gateway LLM (point de sortie IA unique)
- Standards de sécurité applicative
- Outillage CI/CD minimal orienté sécurité
- **Bootstrap & onboarding sécurisé de la plateforme** (voir section dédiée)

Exclus

- Durcissement serveur et réseau (EPIC 2)
- Runtime IA et orchestration de modèles (EPIC 3, EPIC 6)
- Stockage fonctionnel des données IA (EPIC 4)
- Droits RGPD des personnes (EPIC 5)

---

4. Principes directeurs (non négociables)

- Privacy by design & by default
- Isolation stricte des tenants
- Aucune donnée sensible en clair dans les logs
- Aucun accès direct aux modèles IA
- Traçabilité systématique des accès sensibles
- Minimisation des données envoyées aux modèles IA

---

5. Architecture cible (vue logique)

- **Frontend** : Next.js (UI uniquement, aucune logique sensible)
- **Backend API** : services applicatifs sécurisés (Next.js Route Handlers / API)
- **Gateway LLM** : service interne unique pour tout appel IA
- **Security Core** : IAM, RBAC / ABAC, audit, chiffrement
- **Secrets Manager** : Vault ou équivalent

📌Toute interaction avec un modèle IA passe **obligatoirement** par la Gateway LLM.

---

6. Modèle multi-tenant & gouvernance des identités

6.1 Concepts clés

- **Tenant** : entité juridique et technique représentant un client (cabinet, clinique, organisation).
- **Utilisateur plateforme (Platform User)** :
- scope = `PLATFORM`
- pas de `tenant_id`
- rôle typique : **Superadmin plateforme**
- **Utilisateur tenant (Tenant User)** :
- scope = `TENANT`
- associé à un `tenant_id`
- rôles : Admin, User, Auditor, Support

L'isolation par tenant constitue une **frontière juridique et technique** non franchissable.

---

7. Bootstrap & onboarding initial (nouvelle section)

7.1 Objectif

Permettre l'**initialisation sécurisée et reproductible** de la plateforme sans exposer de surface d'attaque réseau.

Le bootstrap couvre : - la création du **premier superadmin plateforme**, - la création de **tenants métiers** (avocat, médecin, comptable, etc.), - la création de l'**administrateur du tenant** associé.

7.2 Modalités

- Le bootstrap est réalisé **exclusivement via CLI** (ligne de commande).
- **Aucun endpoint HTTP public** n'est autorisé pour ces opérations.
- Les commandes CLI appellent des **use-cases applicatifs**, jamais directement la base ou des providers.

7.3 Contraintes de sécurité (bloquantes)

- Création du superadmin **exécutable une seule fois** (lock applicatif ou flag persistant).
- Création de tenant **idempotente** (slug unique, erreurs explicites).
- Aucun mot de passe généré ou loggé en clair (activation ultérieure / reset sécurisé).
- Logs strictement RGPD-safe (événements + identifiants techniques uniquement).
- Émission systématique d'**audit events**.

📌Tant qu'aucune UI superadmin n'existe, la création de tenants est autorisée via CLI.

---

8. User Stories & exigences

US-1 — Architecture multi-tenant stricte

Je veux isoler strictement les données et traitements par tenant.

Exigences : - Chaque ressource est associée à un `tenant_id` - Aucun accès cross-tenant possible - Filtrage systématique des requêtes par tenant - Clés de chiffrement segmentées par tenant

---

US-2 — Authentification sécurisée (IAM)

Je veux une authentification standardisée et robuste.

Exigences : - OAuth2 / OIDC - MFA configurable par tenant - Sessions à durée limitée - Révocation immédiate possible

---

US-3 — Autorisation fine (RBAC / ABAC)

Je veux contrôler précisément les accès aux données et fonctionnalités.

Exigences : - Rôles globaux et tenant-scoped - Attributs dynamiques (tenant, métier, niveau de sensibilité) - Moteur de décision centralisé - Politiques déclaratives versionnées

---

US-4 — Gestion sécurisée des secrets

Je veux protéger l'ensemble des secrets applicatifs.

Exigences : - Aucun secret en clair dans le code ou la config versionnée - Gestionnaire de secrets dédié - Rotation des clés - Séparation stricte des rôles d'accès

---

US-5 — Journalisation RGPD-safe

Je veux journaliser sans exposer de données personnelles.

Exigences : - Logs orientés événements, jamais contenu - Identifiants anonymisés (hash / UUID) - Journalisation des accès sensibles - Rétention configurable - Logique append-only

---

US-6 — Gateway LLM (obligatoire)

📌**Rôle juridique et technique** : la Gateway LLM constitue une barrière obligatoire entre les données utilisateurs et tout modèle IA.

Fonctions : - Redaction et pseudonymisation - Filtrage des prompts - Application des règles RGPD - Allowlist de modèles autorisés - Journalisation RGPD-safe des appels IA

Interdictions : - Appels directs aux APIs IA depuis le frontend - Appels directs aux modèles depuis le code métier

---

US-7 — Sécurité applicative

Je veux réduire la surface d'attaque applicative.

Exigences : - Validation stricte des entrées (schemas) - Protection CSRF / XSS - Rate limiting applicatif - Headers de sécurité

US-8 — CI/CD orienté sécurité

Je veux détecter les failles le plus tôt possible.

Exigences : - Lint sécurité - Scan de secrets - Tests automatisés - Blocage du merge en cas de fail critique

---

9. Dépendances

- Aucun EPIC en amont
- Prérequis pour : EPIC 2, EPIC 3, EPIC 4, EPIC 5, EPIC 6, EPIC 7

---

10. Livrables

- Architecture IAM documentée
- Modèle multi-tenant formalisé
- Politiques RBAC / ABAC versionnées
- Gateway LLM opérationnelle
- Journalisation RGPD-safe active
- Procédure de bootstrap documentée
- Base de code prête pour audit

---

11. Risques & points de vigilance

- Mauvaise isolation tenant → **risque critique**
- Bypass de la Gateway LLM → perte de contrôle RGPD
- Logs trop verbeux → non-conformité
- Bootstrap mal sécurisé → compromission plateforme

---

12. Definition of Done (DoD)

- Isolation tenant validée par tests automatisés
- Aucun appel IA hors Gateway LLM
- Aucun secret exposé
- Logs conformes RGPD
- Bootstrap testé et non rejouable
- Checklist sécurité validée

Fin EPIC 1