# SOVERIA

SOVEREIGN COMPLIANCE OBSERVATORY FOR REGULATED AI

## Référentiel de conformité des systèmes

*d'intelligence artificielle en production*

| | |
|---|---|
| **Édition** | SOVERIA:2026 — Première publication : Avril 2026 |
| **Périmètre** | Systèmes IA en production dans l'Espace Économique Européen |
| **Alignement** | RGPD · EU AI Act 2024/1689 · ISO 27001:2022 · ISO 27701:2019 · OWASP LLM Top 10 · NIST AI RMF 1.0 |
| **Architecture** | 25 points de contrôle · 5 piliers thématiques · Score sur 100 |
| **Niveaux** | SOVERIA Observé · SOVERIA Conforme · SOVERIA Souverain |
| **Révision** | Annuelle (Q1) ou lors d'évolution réglementaire majeure |
| **Statut** | Document public — libre de citation avec attribution « SOVERIA:2026 par Vizidot » |
| **Protection** | Déposé INPI · Marque classes 42 et 45 |

# 01 — OBJET, PÉRIMÈTRE ET PRINCIPES FONDATEURS

## — 1.1 — Finalité du référentiel

SOVERIA a pour finalité de fournir aux organisations un cadre d'évaluation structuré, reproductible et aligné sur les exigences réglementaires applicables aux systèmes d'intelligence artificielle.

Il permet de :

- Évaluer objectivement le niveau de maturité d'une infrastructure IA en production selon 25 critères mesurables.
- Identifier les écarts de conformité vis-à-vis du RGPD et de l'EU AI Act avant qu'ils ne constituent un risque juridique ou opérationnel.
- Produire une documentation de conformité opposable, utilisable dans le cadre d'un audit client, d'un appel d'offres ou d'une démarche assurantielle.
- Planifier et prioriser les actions correctives selon un plan de remédiation structuré en niveaux de priorité.

## — 1.2 — Périmètre d'application

SOVERIA s'applique à tout système d'intelligence artificielle déployé en production ou en phase de pré-production dans l'Espace Économique Européen, qu'il soit un système propriétaire développé en interne, un service tiers intégré via API (OpenAI, Anthropic, Mistral, etc.), un système hybride, ou un système d'assistance à la décision ou de génération de contenu automatique.

### — 1.3 — Principes fondateurs

| | |
|---|---|
| **Reproductibilité** | Chaque point de contrôle est associé à une méthode de mesure définie — script automatique, vérification documentaire ou entretien structuré. Deux évaluateurs appliquant le même protocole obtiennent le même score. |
| **Proportionnalité** | Les exigences de SOVERIA sont proportionnées au niveau de risque du système évalué au sens de l'EU AI Act. |
| **Transparence** | Le présent référentiel est public. Les critères, le barème et la méthodologie sont accessibles sans restriction. |
| **Évolutivité** | SOVERIA est publié par édition annuelle, archivée publiquement. Les éditions antérieures restent valides pour les évaluations déjà réalisées. |
| **Souveraineté** | SOVERIA intègre des critères spécifiques à la localisation des données et à l'indépendance technologique vis-à-vis des opérateurs extra-européens. |

## 02 — ARCHITECTURE DU RÉFÉRENTIEL — LES 5 PILIERS

### — Structure

SOVERIA structure son évaluation en cinq piliers thématiques couvrant l'ensemble des dimensions critiques d'un système IA en production. Chaque pilier comprend cinq points de contrôle, pour un total de vingt-cinq critères d'évaluation.

| | |
|---|---|
| **A** | **Performance & Inférence**<br>Latence au premier token, gestion des pics de charge, stratégie de traitement par lots, plan de continuité et SLA IA.<br>5 points de contrôle · max 20 pts |
| **B** | **FinOps & Souveraineté Économique**<br>Maîtrise des coûts d'exploitation, traçabilité budgétaire par équipe et par cas d'usage, alertes de dépassement, stratégie d'optimisation.<br>5 points de contrôle · max 20 pts |
| **C** | **Conformité Réglementaire**<br>Localisation des données, registre des traitements, classification EU AI Act, droits des personnes concernées, rôle du DPO.<br>5 points de contrôle · max 20 pts |
| **D** | **Sécurité & Architecture**<br>Journalisation des inférences, contrôle d'accès par rôle, protection contre les injections de prompt, gateway IA unifiée, chiffrement.<br>5 points de contrôle · max 20 pts |
| **E** | **LLMOps & Industrialisation**<br>Pipeline d'évaluation automatisé, monitoring continu, versioning des modèles, validation humaine avant déploiement, mesure du ROI IA.<br>5 points de contrôle · max 20 pts |

### — Calcul du score global

Chaque point de contrôle est noté selon un barème à trois niveaux :

| | |
|---|---|
| **4 / 4 — Conforme** | Critère pleinement satisfait. Preuve documentée et vérifiable. |
| **2 / 4 — Partiel** | Critère partiellement satisfait. Actions correctives requises. |
| **0 / 4 — Absent** | Critère non satisfait ou non documenté. |

Le score de chaque pilier est la somme des scores de ses cinq points (maximum 20 points par pilier). Le score global est la somme des cinq piliers, exprimé sur 100.

## 03 — POINTS DE CONTRÔLE — LE RÉFÉRENTIEL COMPLET

Les vingt-cinq points de contrôle sont listés ci-dessous avec leur code, leur libellé officiel et les références réglementaires associées. Pour chaque point, le niveau CRITIQUE indique qu'un score de 0/4 constitue une non-conformité bloquante.

### Pilier A — Performance & Inférence

**A1 Latence au premier token (TTFT) < 800ms au percentile 95** — STANDARD

Vérifier que la latence mesurée au percentile 95 en conditions de charge normale est inférieure à 800ms. Preuves : rapports de monitoring, tableaux de bord de performance, tests de charge documentés.

**Références** : EU AI Act art. 9, 13 · NIST AI RMF 1.0

**A2 Gestion des pics de charge sans dégradation de service** — STANDARD

Architecture dimensionnée pour absorber les pics de charge sans dégradation mesurable du service. Preuves : résultats de tests de charge, plan de scalabilité, SLA documentés.

**Références** : EU AI Act art. 9 · NIST AI RMF 1.0

**A3 Stratégie de traitement par lots (batching) documentée et active** — STANDARD

Mise en œuvre d'une stratégie de batching réduisant la charge sur les endpoints IA pour les traitements non temps-réel. Preuves : documentation architecture, logs de traitement, indicateurs de performance.

**Références** : EU AI Act art. 9 · NIST AI RMF 1.0

**A4 Plan de continuité et procédure de bascule de modèle documentée** — VIGILANCE

Existence d'un plan de continuité opérationnelle incluant une procédure de bascule vers un modèle alternatif ou une instance de secours. Preuves : PCA documenté, test de bascule réalisé, RTO défini.

**Références** : EU AI Act art. 9, 13 · NIST AI RMF 1.0

A5 **Objectifs de niveau de service (SLA IA) formalisés et mesurés** **STANDARD**

SLA propres aux systèmes IA définis, communiqués aux équipes concernées et mesurés en continu. Preuves : document SLA signé, tableaux de bord de suivi, rapports mensuels.

**Références** : EU AI Act art. 9, 13 · NIST AI RMF 1.0

## Pilier B — FinOps & Souveraineté Économique

B1 **Coût par requête tracé avec granularité par utilisateur et par équipe** **STANDARD**

Instrumentation permettant d'attribuer chaque coût d'inférence à un utilisateur, une équipe ou un cas d'usage. Preuves : tableaux de bord FinOps, exports de facturation par tag, rapports d'allocation.

**Références** : EU AI Act art. 17 · NIST AI RMF 1.0

B2 **Budget IA annuel formalisé et suivi avec alertes de dépassement** **STANDARD**

Budget annuel alloué aux systèmes IA, approuvé formellement et suivi mensuellement. Alertes automatiques configurées. Preuves : document budgétaire validé, historique d'alertes, rapports de suivi.

**Références** : EU AI Act art. 17 · NIST AI RMF 1.0

B3 **Analyse comparative CAPEX vs OPEX documentée sur 24 mois** **STANDARD**

Analyse formalisée comparant les coûts d'hébergement souverain (CAPEX) aux coûts d'API cloud (OPEX) sur un horizon de 24 mois. Preuves : document d'analyse, hypothèses documentées, décision de gouvernance.

**Références** : EU AI Act art. 17 · NIST AI RMF 1.0

B4 **Alertes de dépassement budgétaire configurées à 70%, 90% et 100%** **STANDARD**

Alertes automatiques déclenchées à trois seuils du budget IA : 70%, 90% et 100%. Preuves : configuration des alertes, historique de déclenchement, procédure d'escalade documentée.

**Références** : EU AI Act art. 17 · NIST AI RMF 1.0

B5 **Stratégie d'optimisation des tokens documentée et appliquée** **STANDARD**

Stratégie formalisée de réduction de la consommation de tokens : compression des prompts, mise en cache, sélection du modèle adapté au cas d'usage. Preuves : documentation stratégique, résultats mesurés.

**Références** : EU AI Act art. 17 · NIST AI RMF 1.0

## Pilier C — Conformité Réglementaire

### C1 Localisation des données — zéro exfiltration hors Espace Économique Européen

**CRITIQUE**

Garantie contractuelle et technique que les données traitées par les systèmes IA ne transitent pas hors de l'EEE. Preuves : contrats cloud audités, localisation physique des instances, absence de transfert documentée.

**Références** : RGPD art. 46 · EU AI Act art. 10

### C2 Registre des activités de traitement IA tenu à jour (Art. 30 RGPD)

**CRITIQUE**

Registre des traitements incluant les systèmes IA, mis à jour à chaque évolution significative du système. Preuves : registre daté, validation DPO, historique de mise à jour.

**Références** : RGPD art. 30 · EU AI Act art. 12

### C3 Classification EU AI Act — niveau de risque identifié et documenté

**CRITIQUE**

Classification formelle du système selon l'EU AI Act (Risque Minimal, Limité, Haut, Inacceptable). Documentation de la méthode de classification et validation par le responsable juridique. Preuves : document de classification signé.

**Références** : EU AI Act art. 3, 6, Annexe III

### C4 Droits des personnes concernées implémentés et testés (Art. 15-17 RGPD)

**CRITIQUE**

Procédures opérationnelles permettant d'honorer les droits d'accès, de rectification et d'effacement dans un délai inférieur à 30 jours. Preuves : procédures documentées, test d'effacement réalisé, registre des demandes.

**Références** : RGPD art. 15-22 · EU AI Act art. 9

### C5 Délégué à la Protection des Données ou référent IA informé et impliqué

**VIGILANCE**

DPO ou référent IA consulté et impliqué dans le déploiement et les évolutions du système. Preuves : désignation CNIL enregistrée, compte-rendu de consultation, formation aux spécificités IA documentée.

**Références** : RGPD art. 37-39 · EU AI Act art. 9

## Pilier D — Sécurité & Architecture

### D1 Journaux d'inférence complets, horodatés, nominatifs et exportables

**CRITIQUE**

Chaque appel au système IA est enregistré avec horodatage, identifiant utilisateur, entrée et sortie. Logs immuables, exportables et conservés selon les exigences réglementaires. Preuves : échantillon de logs, politique de rétention.

**Références** : EU AI Act art. 12 · RGPD art. 30 · NIST AI RMF

### D2 Contrôle d'accès par rôle (RBAC) sur les endpoints IA

**CRITIQUE**

Accès aux endpoints IA strictement contrôlé par rôle. Aucun accès anonyme ou par défaut aux modèles en production. Preuves : matrice des accès, revue d'accès documentée, politique IAM.

**Références** : EU AI Act art. 9, 15 · ISO 27001 · OWASP LLM09

D3 **Protection active contre les attaques par injection de prompt** — CRITIQUE

Dispositifs de filtrage des entrées et des sorties pour détecter et bloquer les tentatives d'injection de prompt. Preuves : rapport de test d'injection, configuration du garde-fou, logs de blocage.

**Références** : EU AI Act art. 15 · OWASP LLM01, LLM02

D4 **Gateway IA unifiée permettant une bascule de modèle en moins de 48 heures** — VIGILANCE

Architecture de gateway unique centralisant tous les appels IA, permettant de basculer d'un fournisseur à un autre sans modification du code applicatif. Preuves : documentation architecture, test de bascule documenté.

**Références** : EU AI Act art. 13 · ISO 27001

D5 **Chiffrement en transit (TLS 1.3) et au repos documenté et attesté** — CRITIQUE

Chiffrement TLS 1.3 pour tous les flux en transit et chiffrement au repos pour toutes les données sensibles traitées par les systèmes IA. Preuves : audit de chiffrement, certificats, politique de gestion des clés.

**Références** : RGPD art. 25, 32 · EU AI Act art. 15 · ISO 27001 · OWASP LLM06

## Pilier E — LLMOps & Industrialisation

E1 **Pipeline d'évaluation automatisé bloquant avant tout déploiement en production** — VIGILANCE

Pipeline CI/CD incluant des tests automatisés de qualité et de sécurité du modèle, bloquant tout déploiement en production en cas d'échec. Preuves : configuration du pipeline, historique des blocages, métriques de qualité.

**Références** : EU AI Act art. 9, 15 · NIST AI RMF 1.0

E2 **Monitoring continu de la qualité des réponses en production** — VIGILANCE

Système de monitoring mesurant en continu la qualité des réponses du modèle en production : taux d'erreur, dérive sémantique, signaux utilisateurs. Preuves : tableaux de bord de monitoring, alertes configurées.

**Références** : EU AI Act art. 9, 12 · NIST AI RMF 1.0

E3 **Versioning des modèles et procédure de retour arrière documentée** — VIGILANCE

Chaque modèle déployé est versionné. Une procédure de rollback permettant de revenir à une version précédente en moins de 4 heures est documentée et testée. Preuves : registre de versions, test de rollback documenté.

**Références** : EU AI Act art. 12, 17 · ISO 27001

E4 **Procédure de validation humaine avant mise à jour de modèle ou de prompt** — STANDARD

Toute mise à jour de modèle ou de prompt système en production est soumise à une validation humaine formelle avant déploiement. Preuves : procédure documentée, historique des validations, rôles désignés.

**Références** : EU AI Act art. 14 · NIST AI RMF 1.0

| E5 **Retour sur investissement IA documenté et mesuré avec méthodologie définie** | STANDARD |
|---|---|

Méthodologie formalisée de calcul du ROI des systèmes IA, appliquée au moins annuellement. Preuves : document méthodologique, rapport ROI daté, indicateurs de valeur définis.

**Références** : EU AI Act art. 17 · NIST AI RMF 1.0

# 04 — NIVEAUX DE MATURITÉ SOVERIA

## — Trois seuils. Une progression.

SOVERIA définit trois niveaux de maturité correspondant à des seuils de score global. C'est l'organisation — en auto-évaluation ou avec l'appui d'un évaluateur tiers — qui calcule son niveau. SOVERIA fournit la grille de lecture, pas le verdict.

| Niveau | Score | Signification |
|---|---|---|
| Niveau I **Observé** | 0 – 69 / 100 | Infrastructure fonctionnelle avec failles identifiées. Le référentiel fournit un plan de remédiation structuré par niveau de priorité. Aucun certificat n'est associé à ce niveau. |
| Niveau II **Conforme** | 70 – 89 / 100 | Conformité réglementaire assurée. Aucun critère critique à 0/4. Niveau recommandé pour les organisations soumises à l'EU AI Act. |
| Niveau III **Souverain** | 90 – 100 / 100 | Excellence opérationnelle. Infrastructure IA industrielle, souveraine et pleinement documentée. Niveau de référence pour les ETI et organisations critiques. |

> Important : SOVERIA définit les niveaux et les critères — il ne délivre pas de labels lui-même. Les organisations souhaitant faire valider leur niveau par un tiers peuvent recourir à des évaluateurs indépendants s'appuyant sur le référentiel. Le standard reste gratuit et public quel que soit le parcours choisi.

# 05 — ALIGNEMENT RÉGLEMENTAIRE

## — Correspondance par pilier

SOVERIA est conçu comme un sur-ensemble opérationnel des obligations réglementaires applicables aux systèmes IA en Europe.

| PILIER SOVERIA | RÉGLEMENTATIONS COUVERTES | STANDARDS TECHNIQUES |
|---|---|---|
| **A — Performance & Inférence** | EU AI Act art. 9, 13 | NIST AI RMF 1.0 |
| **B — FinOps & Souveraineté Économique** | EU AI Act art. 17 | NIST AI RMF 1.0 |
| **C — Conformité Réglementaire** | RGPD art. 30, 15-22 · EU AI Act art. 3, 6, Annexe III | ISO 27701:2019 |
| **D — Sécurité & Architecture** | RGPD art. 25, 32 · EU AI Act art. 9, 15 | ISO 27001:2022 · OWASP LLM Top 10 · ENISA AI Cybersecurity |
| **E — LLMOps & Industrialisation** | EU AI Act art. 12, 14, 17 | ISO 27001:2022 · NIST AI RMF 1.0 |

# 06 — GOUVERNANCE DU RÉFÉRENTIEL

## — Architecture de gouvernance

La crédibilité de SOVERIA repose entièrement sur la transparence de sa gouvernance et l'indépendance de son Comité Éditorial.

| | |
|---|---|
| **Comité Éditorial** | Organe décisionnel composé de 5 à 7 membres indépendants. Ils valident les éditions annuelles du référentiel, arbitrent les désaccords et engagent publiquement leur crédibilité sur le contenu de SOVERIA. Le Comité est l'unique autorité éditoriale sur le référentiel. |
| **Secrétariat technique** | Assuré par Vizidot (Toulouse). Rôle strictement opérationnel : publication, hébergement, coordination logistique du Comité. Vizidot n'a pas de droit de veto sur les décisions éditoriales. |
| **Cycle de révision** | Édition annuelle publiée au Q1. Révision exceptionnelle possible en cas d'évolution réglementaire majeure. Chaque édition est archivée publiquement. Les évaluations réalisées sous une édition antérieure restent valides. |
| **Conflits d'intérêt** | Tout membre du Comité ayant un intérêt commercial direct dans une organisation évaluée déclare ce conflit avant délibération et s'abstient. Décisions à la majorité des membres non concernés. Délibérations archivées. |

## — Conditions d'utilisation

| | |
|---|---|
| **Usage autorisé (libre)** | Citation avec attribution obligatoire · Référencement dans la documentation interne · Formation et documentation pédagogique · Auto-évaluation autonome selon le référentiel |
| **Usage commercial** | L'utilisation commerciale de la marque SOVERIA (audits facturés à des tiers sous la marque, émission de certificats SOVERIA) est soumise à habilitation. Vizidot est l'unique autorité habilitée à délivrer les certifications SOVERIA et à habiliter des auditeurs tiers. Toute utilisation non autorisée constitue une violation de la marque déposée. |
| **Gouvernance interne** | La participation au Comité Éditorial est régie par une charte interne de gouvernance confidentielle. |