EUDAI Framework v1.3

Vos choix IA — en conscience. Conformité documentée.
Alternatives éclairées. Décisions souveraines.

PiaXel Nexus, projet EuTrustedIA.eu

2026-05-26

Table des matières

1 Avis juridique. à lire avant tout

EUDAI Framework (Cadre Européen de Doctrine IA) est un **référentiel doctrinal et opérationnel**. Il **n'est pas** un avis juridique individualisé.

EuTrustedIA et PiaXel Nexus ne sont **ni** un cabinet d'avocats, **ni** un cabinet de DPO délégué, **ni** un organisme habilité à délivrer une certification au sens du RGPD (Art. 42-43) ou de l'AI Act (Art. 43). L'éditeur ne se substitue à aucun de ces tiers.

EuTrustedIA documente la conformité ; elle ne la certifie pas. Tout livrable produit par nos outils (AIPD pré-remplie, fiche Article 50, registre des traitements) doit être **revu et signé** par un professionnel qualifié, DPO, avocat tech, ou expert vérifié de l'**Annuaire EuTrustedIA**, avant production de tout effet juridique.

Les recommandations de ce document sont **génériques** : elles ne tiennent pas compte de votre cas particulier, de votre secteur, de votre juridiction d'établissement principal, ni de l'état du droit en vigueur à la date de votre lecture.

L'éditeur décline toute responsabilité pour l'usage qui sera fait de ce document. Sa diffusion vous engage à respecter sa licence : **Creative Commons Attribution, Pas d'Utilisation Commerciale 4.0 International** (CC BY-NC 4.0).

2 Mission EuTrustedIA

> **« Vos choix IA — en conscience. »**
>
> *Conformité documentée. Alternatives éclairées. Décisions souveraines.*

Faire de l'IA souveraine un choix conscient.

Aucun entrepreneur ne devrait subir sa stack IA. Aucun ne devrait avancer à l'aveugle face au RGPD, à l'AI Act, à la souveraineté des données, à la dépendance fournisseur, aux transferts internationaux. Aucun ne devrait être prisonnier d'une idéologie — européanisme dogmatique d'un côté, fascination frontier de l'autre.

EuTrustedIA met à votre disposition **toutes les informations dont vous avez besoin** pour devenir **conscient et responsable** de vos décisions IA. Outils, fonctionnalités, origines, cadres législatifs, trade-offs : **nous éclairons, nous ne jugeons pas.**

EU first quand c'est pertinent. Pragmatique quand votre contexte l'exige. Transparent toujours.

Le but : que chaque entrepreneur EU fasse les bons choix — pour **ses** données, **son** produit, **ses** clients, **son** contexte.

3 Niveleur de terrain réglementaire — la 3ème dimension de la mission EuTrustedIA

> **« Vous ne devriez pas avoir à choisir entre conformité et compétitivité. Notre rôle : enlever l'overhead juridique pour que vous puissiez vous concentrer sur ce qui crée de la valeur — votre produit, vos clients, votre vision. »**
>
> *(Doctrine fondatrice EuTrustedIA, axe #3, acté 2026-05-14.)*

La réglementation IA européenne — RGPD, AI Act, EDPB, jurisprudence CJUE — est légitime, et nous n'en contestons ni l'esprit ni la nécessité. Elle protège les utilisateurs européens et structure un marché de l'IA qui, à défaut, dériverait. **Mais elle crée mécaniquement un coût fixe d'entrée.** Lire les textes, suivre les Opinions de l'EDPB, traduire l'AI Act en obligations applicables à votre cas, produire les livrables (AIPD, fiche Article 50, registre Art. 30, *Transfer Impact Assessment*) — cela demande un temps et une expertise juridique qui, ramenés au prix du marché, oscillent entre 1 500 et 5 000 € par audit chez un cabinet, plus la rétention d'un DPO. Pour un acteur établi qui dispose d'un service juridique interne, ce coût est absorbable. Pour un solopreneur IA EU qui démarre avec moins de 50 k€ de chiffre d'affaires annuel, il est prohibitif.

Le constat est structurel : **plus la réglementation est dense, plus elle favorise les incumbents** qui ont la capacité juridique de l'absorber, et désavantage ceux qui partent de zéro. *EUDAI nomme ce déséquilibre et lui répond.*

EUDAI est l'outil **pédagogique** de cet axe : un référentiel doctrinal public, sourcé sur les articles précis, traduit en obligations actionnables, mis à jour trimestriellement, accessible à un porteur de projet en autonomie. **Lire EUDAI, c'est la première étape pour ne plus subir l'overhead réglementaire.** La suite — POSITRONIA scanner, AIPD pré-remplie, Stack Recommender, Annuaire EuTrustedIA — outille concrètement la conformité à un prix solopreneur (29 à 99 €/mois), sans cabinet d'avocats et sans DPO délégué à 4 000 €/an.

Trois garde-fous encadrent cette posture : (1) elle est **pragmatique, jamais militante anti-régulation** — la régulation existe, on la rend gérable, on ne la combat pas ; (2) elle promet la **suppression d'un handicap structurel**, pas la compétitivité comme résultat — le produit, le marché et l'exécution restent de votre responsabilité ; (3) elle s'ancre sur les **solopreneurs EU réels** (vrais petits, 29 €/mois) et **pas sur le narratif** d'acteurs déjà bien dotés capitalistiquement.

Référence canonique : doctrine fondatrice triple-axe EuTrustedIA (auto-démontrable + éclairant pragmatique + niveleur de terrain réglementaire) — `feedback_mission_eclairant_pragmatique.md` (importance 10, mémoire persistante PiaXel) et ADR `Galaxy Spirit/80_PIAXEL_CORE/03_DECISIONS/2026-05-13__doctrine_eutrustedia_eclairant_souverain_pragmatique.md`.

4 Préambule. Un seul abonnement, deux moments de vie d'un projet IA

4.1 Que signifie EUDAI ?

EUDAI est l'acronyme de *European Union Doctrine on AI*, en français **Cadre Européen de Doctrine IA**. Le nom condense trois choix structurants qu'il faut comprendre avant d'entrer dans la doctrine elle-même.

European **U**nion. Ce cadre s'enracine dans le droit de l'Union européenne (RGPD, AI Act, EDPB, jurisprudence CJUE). Il ne prétend ni à une portée mondiale, ni à une équivalence avec les approches étatsuniennes (NIST AI RMF) ou britanniques (UK AI Safety Institute). Il revendique une fidélité opérationnelle au cadre légal européen, et il assume cette frontière.

Doctrine. Pas un référentiel d'audit fermé, pas une norme privée, pas une certification monnayée : une doctrine publique, applicable, contestable, et révisée trimestriellement à mesure que la jurisprudence européenne mûrit. Une doctrine est par nature ouverte à la critique, et elle s'enrichit des retours de la communauté qui l'utilise.

AI (*Artificial Intelligence*, en français **IA**). Le périmètre couvre les systèmes d'intelligence artificielle au sens de l'AI Act Art. 3.1, ce qui inclut les modèles de langage, les agents conversationnels, les systèmes de recommandation, les classifieurs, les générateurs de contenu, et les systèmes d'identification ou de catégorisation biométrique. Le RGPD s'applique en parallèle dès qu'un système IA traite des données à caractère personnel.

EUDAI a donc pour vocation de **traduire la conjugaison du RGPD et de l'AI Act en doctrine actionnable** pour les solopreneurs et micro-équipes IA européens, qui n'ont ni cabinet d'avocats ni DPO interne, et qui ont besoin d'un cadre stable, sourcé et auto-démontrable pour partir conformes ou se mettre en conformité.

EUDAI s'adresse à **deux moments de vie d'un projet IA**, traités par un **seul abonnement EuTrustedIA**. Vous bénéficiez indifféremment des deux modes selon le stade de votre projet, et vous pouvez même les utiliser en parallèle si vous gérez plusieurs projets à des stades différents.

4.2 Mode Audit & Conformité (post-build)

Vous avez déjà construit votre produit IA. Il tourne, il a des utilisateurs, et l'AI Act Art. 50 entre en vigueur le **2 août 2026**, vous voulez savoir où vous en êtes.

EuTrustedIA scanne, audite, et **livre les pièces** : AIPD pré-remplie destinée à être **signée par un DPO partenaire**, fiche **Article 50** prête pour la CNIL, registre des traitements à jour, recommandations de remédiation hiérarchisées.

> *Déclencheur marché : 2026-08-02. Promesse : « Vous avez bâti, on documente la conformité de ce qui est. »*

4.3 Mode Lancement Conforme (pre-build)

Vous n'avez pas encore commencé. C'est le meilleur moment de votre vie pour rencontrer EUDAI.

Avant la première ligne de code, le premier prompt système, le premier choix de fournisseur, vous obtenez : une **auto-évaluation EUDAI** sur 12 axes pre-build, suivie d'un **POSITRONIA Blueprint** (Diagnostic Pré-build, audit de votre cahier des charges, pas du code), d'un **Stack Recommender** (Recommandeur Souverain EU, recommandation infra + IA 100 % EU avec 3 alternatives par couche), d'une **AIPD pré-remplie sectorielle**, et de **3 voies pour exécuter** : DIY, FORMATION, AVANTAGES.

> *Déclencheur marché : moment où le porteur de projet structure son idée. Promesse : « Vous lancez, on vous aide à partir conforme, pas à colmater après. »*

4.4 Pourquoi un seul abonnement couvre les deux modes

Parce que la conformité IA est **un cycle**, pas un événement :

- on **lance** conformément (mode Lancement Conforme, mois 0 à 6),
- on **scale** en re-scannant (mode Audit & Conformité, scan annuel),
- on **prouve** au régulateur, à un investisseur, à un client B2B (livrables Audit & Conformité renforcés).

Un porteur capté en **LANCE-TOI à 49 €** (ticket d'entrée pre-build one-shot) peut devenir un abonné **SOLO à 29 €/mois** dès qu'il commence à construire, puis monter en **GENESIS à 69 €/mois** quand il veut s'engager dans le parcours d'autonomie souveraine, puis basculer en **AVANTAGES à 99 €/mois** pour activer le Club Deal partenaires et les rendez-vous remisés sur l'Annuaire EuTrustedIA, puis évoluer en **ENTREPRISE sur devis** à mesure qu'il passe à l'échelle ou qu'il gère un portefeuille de projets multi-équipes. **EUDAI n'est pas un audit ponctuel : c'est un cadre qui vous accompagne du premier croquis au passage à l'échelle, sans rupture de continuité entre pre-build et post-build.**

4.5 Trois niveaux d'usage IA, et lequel vous concerne

Avant d'entrer dans la doctrine, il est important de distinguer **trois niveaux d'usage IA** qui n'engagent ni les mêmes obligations RGPD, ni les mêmes obligations AI Act. Beaucoup de solopreneurs confondent ces niveaux et, selon les cas, s'angoissent à tort ou se croient à tort exonérés. Le périmètre du présent document et celui de POSITRONIA visent prioritairement le **niveau 3**.

Niveau 1, usage personnel privé. Vous utilisez Claude, ChatGPT ou Mistral pour rédiger un courriel à un proche, traduire une recette, organiser vos vacances ou pratiquer une langue. Aucun lien avec une activité professionnelle. Vos seules données personnelles sont traitées, et la base légale est votre propre consentement implicite à utiliser le service. Le RGPD, dans sa dimension *responsable de traitement*, ne s'applique pas. L'AI Act ne s'applique pas non plus dans la qualification de fournisseur ou de déployeur. Restent les conditions générales du service que vous utilisez. Ce niveau n'est pas le périmètre EUDAI.

Niveau 2, usage professionnel pour soi-même (outillage interne). Vous êtes solopreneur, indépendant ou micro-entreprise, et vous utilisez un assistant IA pour bâtir votre produit, rédiger vos courriels commerciaux, structurer votre documentation interne ou écrire votre code. Le système IA est **votre outil de travail**, il n'est **pas exposé à vos clients ou à vos salariés**. Vous restez responsable du traitement RGPD pour les données personnelles de vos prospects, clients ou fournisseurs que vous traitez par ailleurs (registre Art. 30, base légale Art. 6, sécurité Art. 32, etc.), et vos sous-traitants IA doivent satisfaire les obligations Art. 28 (DPA signé) et Art. 44-49 (transferts hors UE encadrés) si vous leur soumettez des données personnelles. L'AI Act, lui, ne fait pas peser sur vous d'obligations de fournisseur ou de déployeur tant que vous ne mettez pas le système IA au service de tiers. Le niveau 2 est un usage légitime, à condition que la traçabilité fournisseur (DPA, CCT, juridiction d'établissement) soit en ordre.

Niveau 3, système IA mis au service de tiers (clients, salariés ou public). Vous intégrez un système IA dans votre produit, votre site, votre application, votre service client, votre processus de recrutement ou votre flux interne ouvert à des salariés. Le système IA produit alors des sorties qui touchent **directement** des personnes autres que vous. Vous devenez **déployeur** au sens AI Act, et potentiellement **fournisseur** si vous combinez, fine-tunez ou redistribuez un modèle. Les obligations s'empilent : transparence Art. 50 (marquage des contenus générés), surveillance humaine Art. 14 si haut risque, AIPD au sens RGPD Art. 35, registre, base légale du traitement vis-à-vis de vos utilisateurs finaux, notice Art. 13-14, droit d'opposition Art. 22 si décision automatisée à effet juridique. **C'est ce niveau 3 qui constitue le périmètre central d'EUDAI et de POSITRONIA.**

Cas d'école, l'éditeur du présent document. PiaXel Nexus utilise l'assistant IA Claude (Anthropic, US) pour produire le code de son SaaS, structurer sa documentation interne et rédiger ses propres documents publics, dont celui que vous lisez. C'est un usage de **niveau 2** : Claude est une dépendance interne de développement, traçable contractuellement (DPA + DPF), et aucune donnée personnelle de tiers ne lui est soumise. À l'inverse, l'application **POSITRONIA** (la plateforme EuTrustedIA exposée aux abonnés payants) tourne sur une **infrastructure LLM EU souveraine vérifiable** — modèles open-source (Mistral Nemo, Mixtral, LLaMA) hébergés chez **OVH AI Endpoints ⊠⊠**, **Scaleway Generative APIs ⊠⊠** ou **Infomaniak AI ⊠⊠** selon arbitrage opérationnel publié dans notre LEDGER. Elle relève du **niveau 3** : un client final paie pour utiliser un système IA et reçoit une recom-

mandation produite par ce système — la souveraineté EU y devient obligatoire par construction. La doctrine PiaXel Nexus impose de distinguer clairement les deux niveaux et de choisir le fournisseur LLM en conséquence : souveraineté EU obligatoire au niveau 3, traçabilité contractuelle au niveau 2. **Note transparente** : nous avons écarté Mistral Cloud API (`mistral.ai/api`) au tier Standard depuis que Mistral a ajouté les USA aux processing locations via GCP en février 2026 sans notification préalable (plainte CNIL en cours). Mistral Compute (datacenter Essonne ▯▯, déploiement progressif 2026 H2) sera évalué dès disponibilité. Cette décision est documentée dans notre ADR `2026-05-13__doctrine_eutrustedia_eclairant_souverain_pragmatique.md`.

Cette distinction n'est ni un détail juridique, ni une coquetterie philosophique, c'est l'architecture mentale qui permet de **dimensionner correctement vos obligations**. Trop de solopreneurs IA pensent à tort qu'utiliser un assistant LLM pour écrire leurs propres prompts les expose aux obligations Art. 50 ou Art. 35, alors que c'est l'usage qu'ils font de ce LLM **pour leurs clients** qui les y expose, pas l'usage qu'ils en font pour eux-mêmes. Inversement, exposer un agent IA à des utilisateurs finaux **sans aucune notice de transparence** est trop souvent banalisé, alors que c'est précisément ce que l'AI Act vient sanctionner à partir du **2 août 2026**.

5 Partie 1. Pourquoi EUDAI ?

5.1 1.1 Le vide doctrinal entre RGPD et AI Act

L'Europe dispose de deux textes-phares sur l'IA : le **RGPD** (Règlement (UE) 2016/679, applicable depuis mai 2018) et l'**AI Act** (Règlement (UE) 2024/1689, déploiement échelonné 2024-2027).

Sur le papier, c'est complet. Dans la pratique d'un solopreneur IA qui assemble un agent conversationnel un dimanche soir, ces textes posent **trois problèmes opérationnels majeurs** :

1. **Ils ne se parlent pas explicitement.** Le RGPD régit les données personnelles ; l'AI Act régit les systèmes d'IA. Quand votre agent traite des données personnelles **dans** un système d'IA d'usage général (*general-purpose AI*), vous tombez sous les deux, sans qu'aucun des deux textes ne vous dise dans quel ordre les appliquer.
2. **Ils sont pensés pour l'entreprise structurée**, dotée d'un DPO, d'un service juridique, et d'une équipe sécurité. Pas pour un porteur seul, pas pour un projet à 49 € de budget mensuel d'infrastructure.
3. **Ils sont en mouvement.** L'AI Act Art. 50 (transparence) entre en vigueur le **2 août 2026**, l'EDPB publie régulièrement des Opinions précisantes (Opinion 28/2024 sur les modèles d'IA et l'anonymisation des données d'entraînement, par exemple), et les autorités nationales, CNIL en tête, publient leurs propres recommandations qui font autorité de fait.

EUDAI n'est pas un sur-texte qui prétend remplacer le droit. C'est une **traduction opérationnelle** : un cadre stable, applicable demain matin, sourcé sur les articles précis, mis à jour trimestriellement, et adapté à votre stade, pre-build ou post-build.

5.2 1.2 Le constat. 10 millions de solopreneurs IA EU sans doctrine actionnable

Une estimation prudente : entre **5 et 10 millions** de personnes en Union européenne lancent ou opèrent aujourd'hui un projet IA en solo ou en micro-équipe (≤ 5 personnes). Indépendants, *bootstrappers*, freelances en transition, étudiants entrepreneurs, salariés en projet annexe.

Ils partagent **trois caractéristiques structurelles** :

— **Pas de DPO interne.** Le coût d'un DPO délégué (1 500 à 4 000 € par an) est hors de portée pour un projet à revenu inférieur à 50 k€ par an.

— **Pas de service juridique.** Une consultation chez un avocat tech compétent en IA et RGPD se facture **300 à 600 € de l'heure**, et il en faut généralement 5 à 15 heures pour cadrer un projet.
— **Pas de conseil stratégique en conformité dès la conception.** Les *Big 4*, Naaia, Trustia, Witty Works, OneTrust visent des clients à six chiffres. Pour le solopreneur, le marché est **vide**.

Pendant ce temps, le risque réglementaire monte :

— **Sanctions RGPD** : jusqu'à **20 M€** ou **4 % du chiffre d'affaires mondial** (le plus élevé). Dans la pratique récente, la CNIL a sanctionné plusieurs micro-acteurs à des montants compris entre **3 000 et 50 000 €**, destructeurs pour un solopreneur.
— **Sanctions AI Act** : jusqu'à **35 M€** ou **7 % du CA mondial** pour les pratiques interdites (Art. 5), **15 M€** ou **3 %** pour la plupart des autres manquements (Art. 99).
— **Risque réputationnel** : un signalement par un utilisateur sur un canal public peut détruire la traction commerciale d'un produit en quelques heures.

Le solopreneur IA EU est aujourd'hui dans une situation paradoxale : il **construit** des systèmes qu'une équipe de vingt personnes aurait piloté il y a cinq ans, mais il n'a **aucun outil** pour les rendre conformes. **EUDAI vise à combler ce vide.**

5.3 1.3 Au-delà de l'Article 50. la carte des articles qui frappent réellement

L'AI Act Art. 50 (transparence des contenus générés par IA) bénéficie d'une visibilité médiatique forte parce qu'il entre en vigueur le **2 août 2026** et concerne quasiment tous les solopreneurs déployant de l'IA générative. C'est un **point d'attention urgent**.

Mais c'est aussi un piège. Un solopreneur qui se met en conformité avec le seul Art. 50, en ignorant le reste, fabrique une **bombe à retardement juridique**. Les vraies sources de risque, dans l'ordre d'impact pour un projet IA solo, sont les suivantes.

5.3.1 1.3.1 RGPD, le marteau de tous les jours

Article	Sujet	Quand cela devient critique
Art. 5	Principes (minimisation, limitation de conservation, exactitude)	Toujours. C'est la base de toute défense.
Art. 6	Bases légales du traitement	**Choisir consentement contre intérêt légitime de travers = nullité du traitement.**
Art. 9	Catégories particulières (santé, opinions, biométrie, vie sexuelle, données de syndicat)	Si votre agent IA traite ces données → quasi-impossible sans consentement explicite.

Article	Sujet	Quand cela devient critique
Art. 22	**Décision automatisée et profilage**	**Critique pour l'IA** : si une décision IA produit un effet juridique ou similaire (RH, crédit, accès à un service) → encadrement strict + droit d'opposition humaine.
Art. 25	**Protection des données dès la conception et par défaut**	C'est exactement le périmètre de notre mode *Lancement Conforme*.
Art. 28	**Sous-traitants**	Pas de contrat de sous-traitance (DPA) signé avec votre fournisseur LLM (Mistral, OpenAI, Anthropic, etc.) = **violation pure et simple**.
Art. 30	Registre des traitements	Obligatoire dès traitement régulier de données sensibles → 90 % des solopreneurs IA sont concernés.
Art. 32	Sécurité du traitement	Chiffrement, MFA, sauvegardes, gestion des incidents.
Art. 33-34	**Notification de violation sous 72 h**	Une fuite de données et vous avez **72 heures** pour notifier la CNIL, sinon amende.
Art. 35	**AIPD obligatoire** (analyse d'impact relative à la protection des données)	Large échelle, IA, données sensibles → solopreneur IA quasi toujours concerné.
Art. 44-49	**Transferts hors UE**	Si vous utilisez OpenAI, Anthropic, Google = transfert vers les États-Unis → clauses contractuelles types (CCT), DPA, *Transfer Impact Assessment* obligatoires.

5.3.2 1.3.2 AI Act, le marteau qui arrive

Article	Sujet	Quand cela devient critique
Art. 5	**Pratiques interdites**	Manipulation subliminale, notation sociale, reconnaissance d'émotion en milieu professionnel ou éducatif, catégorisation biométrique → **votre produit est purement illégal si vous tombez dedans.**
Art. 6 + Annexe III	**Classification à haut risque**	RH (tri de CV), éducation (notation), crédit, santé, justice, infrastructure critique → si oui, tout change.
Art. 9-15	Obligations à haut risque	Qualité des données, traçabilité, explicabilité, surveillance humaine, robustesse, cybersécurité.
Art. 10	Qualité des données d'entraînement	Si vous fine-tunez un modèle.
Art. 13-14	Transparence vis-à-vis des déployeurs + surveillance humaine	Si système classé à haut risque.
Art. 50	**Transparence vis-à-vis des utilisateurs finaux** (chatbots, deepfakes, contenus générés par IA)	Quasi tous les déployeurs. **Déclencheur 2026-08-02.**
Art. 51-55	**Modèles d'IA à usage général (GPAI)**	Si vous diffusez un modèle ou affinez un modèle de fondation.

5.3.3 1.3.3 Carte par stade de projet, *« quand m'inquiéter de quel article ? »*

```
PRE-BUILD (avant la première ligne de code)
  └─ RGPD Art. 25 (conception) + Art. 6 (base légale) + Art. 35 (AIPD)
  └─ AI Act Art. 5 (pratiques interdites) + Art. 6 + Annexe III (classification)

LANCEMENT (mise en service)
  └─ RGPD Art. 13-14 (information) + Art. 28 (sous-traitants) + Art. 30 (registre)
   └─ RGPD Art. 32 (sécurité) + Art. 44-49 (transferts hors UE)
```

```
  └─ AI Act Art. 50 (marquage transparence)

OPÉRATION (run continu)
  └─ RGPD Art. 22 (décision automatisée) + Art. 33-34 (notif violation 72 h)
  └─ AI Act Art. 13-14 (si haut risque)

PASSAGE À L'ÉCHELLE (croissance)
  └─ RGPD Art. 35 (re-AIPD si périmètre change)
  └─ AI Act Art. 9-15 (obligations haut risque si applicables)
  └─ AI Act Art. 51-55 (si vous devenez fournisseur GPAI)
```

C'est cette carte que les Parties 2 et 3 d'EUDAI rendent opérationnelle, pilier par pilier, et que la checklist en 25 points (§ 3.2) traduit en actions concrètes.

5.4 1.4 La doctrine en une phrase

> ***« Si on vend de la conformité, on doit être exemplaire. »***
>
> ***« Le vrai sujet, c'est devenir conscient et responsable — donner toutes les informations pour faire les bons choix. »*** (Laurent SOUHY, fondateur PiaXel Nexus, 2026-05-12)

Tout EUDAI découle de la conjonction de ces deux phrases.

La première dit que nous sommes exemplaires de ce que nous prêchons. Concrètement, cela signifie qu'**EuTrustedIA s'applique à elle-même**, en premier et en public, **chacune** des recommandations du présent document. Stack majoritairement EU souveraine (trajectoire Phase A → Phase C documentée en § 2.1.3). Méthodologie publique. Jeu de données d'évaluation versionné public (`eutrustedia/sentinel-bench`). LEDGER (registre append-only horodaté) public de toutes les décisions techniques. AIPD interne disponible à l'inspection. Toutes les sorties de nos LLM marquées au sens de l'**AI Act Art. 50**, y compris les recommandations de ce document, là où elles sont *aidées par LLM* (et c'est dit explicitement, voir Partie 4 *Disclaimers techniques*).

La seconde dit que nous éclairons, nous ne jugeons pas. Notre rôle n'est pas de condamner les choix non-EU ni de prescrire une seule route. C'est de **mettre à votre disposition toutes les informations** dont vous avez besoin pour décider — selon vos données, votre produit, vos clients, votre contexte légal. EU first comme **défaut recommandé**, jamais comme **dogme**. Pragmatique non-manichéen.

C'est ce que nous appelons la doctrine **« auto-démontrable + éclairante »**. Vérifiables sur ce que nous prêchons (auto-démontrable) ET transparents sur les trade-offs (éclairant). Un éclairant a plus d'autorité qu'un militant — il sait montrer pourquoi telle option est meilleure quand elle l'est, ET pourquoi les options moins idéales sont parfois acceptables. C'est plus crédible B2B sophistiqué.

Cette approche rejoint la notion d'*Ethics by Evolution* proposée par Jérôme Béranger (chercheur associé INSERM Université Toulouse 3, Institut EuropIA) et Fatima Ait Thami (GoodAlgo) dans la revue Polytechnique Insights du 21 avril 2026. *Ethics by Evolution* prolonge l'approche *Ethics by Design* en exigeant que les critères et les indicateurs éthiques soient adaptés tout au long du cycle de vie d'un

système d'IA, pas seulement à sa conception. EuTrustedIA pratique cela depuis le premier jour, par trois mécanismes concrets : un *signal layer* refreshable trimestriel qui aligne les catégories AI Act sur la jurisprudence européenne au fil de sa publication, des snapshots de jeux de données d'évaluation versionnés Git et tagués (sentinel-bench publié et incrémenté de version en version), et un LEDGER public horodaté de toutes les décisions techniques structurelles, accessible sur `eutrustedia.eu/audit/ledger`. Notre doctrine n'est donc pas un slogan figé. C'est un cadre vivant qui évolue avec l'état du droit et de la recherche.

5.5 1.5 Les 5 piliers EUDAI

EUDAI se déploie sur **cinq piliers**. Chacun est **traduisible en obligations RGPD/AI Act précises**, **vérifiable** (POSITRONIA scanner ou auto-évaluation), et **livrable** (AIPD, fiche Art. 50, rapport de diagnostic pré-build).

Chaque pilier s'enracine dans **un bouquet d'articles**, pas un seul. C'est la conséquence directe du § 1.3 ci-dessus.

#	Pilier	Articles principaux	Question solopreneur résolue
1	**Souveraineté radicale**	RGPD Art. 28, 44-49, AI Act Art. 25 (BYOK)	*« Sur quel cloud, quel LLM, quelle base je m'appuie sans dépendre des États-Unis ou de la Chine ? »*
2	**Conformité auto-démontrable**	RGPD Art. 5, 24, 30, AI Act Art. 12 (logs)	*« Comment je prouve à un client B2B, à un investisseur, à un régulateur, que je suis sérieux ? »*
3	**Humain dans la boucle final**	RGPD Art. 22, AI Act Art. 14 (surveillance humaine)	*« Qui signe à la fin ? Qui prend la responsabilité juridique ? »*
4	**Transparence des données d'entraînement**	RGPD Art. 5, 6, 9, 35, AI Act Art. 10, EDPB Opinion 28/2024	*« Mon modèle a été entraîné comment, et est-ce que c'est légal ? »*

#	Pilier	Articles principaux	Question solopreneur résolue
5	**Anti-deepfake et anti-empoisonnement**	RGPD Art. 15 (entrée), AI Act Art. 50 (sortie)	*« Comment éviter que mes outputs soient pris pour des fakes, et comment me protéger contre les données empoisonnées en amont ? »*

Les Parties 2 à 4 développent chacun de ces piliers, fournissent un arbre de décision pre-build (Partie 3), une checklist 25 points opérationnelle (Partie 3), une présentation du Stack Recommender et du tunnel à 3 voies (Partie 3), et présentent les 4 plans tarifaires d'accompagnement (Partie 4). Chaque pilier sera également décliné en module vidéo de formation dédié, accessible via le Plan FORMATION ou GENESIS, pour les porteurs qui veulent passer de la doctrine écrite à la mise en œuvre guidée.

5.6 1.6 LLM Fallacy / Capability Divergence — fondation cognitive de la posture EUDAI

> *Cette section est la fondation cognitive d'EUDAI. Elle explique mécaniquement pourquoi le disclaimer juridique de la page d'ouverture — « EuTrustedIA documente la conformité ; elle ne la certifie pas » — n'est pas une précaution légale de confort, mais un fait cognitif documenté par la recherche académique.*

5.6.1 1.6.1 Le phénomène : définition formelle

La **capability divergence** (ΔC) est l'écart documenté entre la compétence qu'un output LLM produit *en apparence* et la compétence sous-jacente *réellement* détenue par l'utilisateur.

> « The LLM fallacy is defined as a cognitive attribution error in which individuals misinterpret LLM-assisted outputs as evidence of their own independent competence, producing a systematic divergence between perceived and actual capability. »
>
> — Kim, H., Yu, H., & Yi, H. (2026). *The LLM Fallacy : Misattribution in AI-Assisted Cognitive Workflows.* arXiv :2604.14807v1 [cs.AI], 16 Apr 2026. ddai Inc.

Trois conditions sont nécessaires pour que la LLM Fallacy se déclenche :

1. La tâche implique une **génération d'output médiatisée par LLM** qui exigerait sinon une expertise de domaine.

2. L'interaction est **suffisamment fluide** pour que la frontière humain/machine ne soit pas perçue.
3. L'output présente un **niveau de cohérence** typiquement associé à une performance humaine qualifiée.

Quand ces trois conditions sont réunies, l'utilisateur s'attribue la compétence produite par le système — et non la sienne. C'est le mécanisme fondamental.

5.6.2 1.6.2 Les trois propriétés LLM qui amplifient la divergence

Le papier Kim/Yu/Yi formalise trois propriétés de l'interaction LLM qui créent ensemble la condition de déclenchement :

Propriété	Définition	Effet cognitif
Opacity	Le processus de raisonnement du modèle est opaque — l'utilisateur voit l'output, pas le raisonnement	L'utilisateur ne peut pas distinguer sa contribution de celle du modèle
Fluency	L'output présente la prose et la cohérence d'un expert qualifié	L'output *sonne* compétent — ce qui le fait percevoir comme preuve de compétence
Interactional Immediacy	Le cycle de réponse est quasi-instantané et conversationnel	La frontière humain/machine s'efface ; l'utilisateur vit l'échange comme une pensée co-produite

La chaîne causale formelle (Figure 1 du papier) est la suivante :

```
Propriétés LLM [Opacity + Fluency + Interactional Immediacy]
  ↓
Médiation cognitive [Attribution Ambiguity + Cognitive Outsourcing]
  ↓
Misattribution (l'utilisateur s'attribue l'output)
  ↓
Capability Divergence (ΔC = gap compétence perçue / compétence réelle)
```

5.6.3 1.6.3 Distinction critique avec les concepts proches

La LLM Fallacy est souvent confondue avec trois concepts adjacents. La distinction est fondamentale pour comprendre pourquoi les réponses habituelles (meilleure interface, meilleurs garde-fous) ne la résolvent pas :

Concept	Niveau d'opération	Différence avec la LLM Fallacy
Hallucination	Qualité de l'output système	La LLM Fallacy persiste même quand l'output est factuellement **correct**
Automation bias	Exécution de la tâche (sur-reliance)	Opère sur la confiance dans l'outil, pas sur l'auto-attribution de compétence
Cognitive offloading	Exécution de la tâche (délégation d'effort)	Opère sur la réduction de charge mentale, pas sur la perception de soi
LLM Fallacy	**Auto-perception et attribution de compétence**	Opère sur l'identité cognitive — *qui je crois être* après avoir utilisé le LLM

L'implication pratique est décisive : améliorer la précision du LLM (réduire les hallucinations) ne résout pas la LLM Fallacy. Un output parfaitement correct peut déclencher la même divergence de compétence perçue.

5.6.4 1.6.4 Le domaine « Professional Signaling » — le plus critique pour EuTrustedIA

Le papier Kim/Yu/Yi identifie six domaines de manifestation de la LLM Fallacy. Le sixième — le **domaine professionnel (signaling)** — est le plus critique pour l'écosystème EuTrustedIA :

> *L'utilisateur déclare des compétences basées sur des outputs assistés par LLM.*

C'est exactement la situation du solopreneur IA qui a demandé à ChatGPT de rédiger son AIPD, qui a obtenu un document bien structuré et fluent, et qui pense désormais **avoir fait sa conformité AI Act**. Il a produit un brouillon. Il a capturé l'output de quelqu'un d'autre — le modèle. Il n'a pas, pour autant, acquis la compétence juridique que ce brouillon simule.

Le risque est réel et documenté : le papier argumente que la LLM Fallacy affecte les **systèmes d'évaluation institutionnels** (recrutement, certification, audit), pas seulement les individus. Les outputs LLM peuvent satisfaire des critères formels **sans que la compétence sous-jacente existe**. La relation performance ⇔ compétence s'affaiblit systématiquement.

5.6.5 1.6.5 Trois implications doctrinales pour EUDAI v1.3

La LLM Fallacy n'est pas un risque abstrait. Elle produit trois implications concrètes sur la doctrine et l'offre EuTrustedIA.

Implication 1 — L'Annuaire EuTrustedIA n'est pas un service premium optionnel

Combler ΔC nécessite un professionnel qui engage sa responsabilité. POSITRONIA-CORE détecte l'écart technique — la distance entre l'état du code/de la configuration et les exigences réglementaires. EUDAI structure la documentation et produit des brouillons de livrables (AIPD, fiche Article 50, registre Art. 30). Mais **seul un expert vérifié de l'Annuaire EuTrustedIA peut signer, arbitrer et engager** — parce que la signature engage une responsabilité professionnelle que l'IA ne détient pas et ne peut pas simuler.

Ce n'est pas un choix marketing de monter en gamme : c'est la conséquence directe de la capability divergence. Le Plan AVANTAGES à 99 €/mois — qui donne accès aux experts vérifiés de l'Annuaire avec remise — trouve ici sa justification **cognitive**, pas seulement commerciale.

Implication 2 — Le différenciateur face aux concurrents DIY

Snyk, OneTrust, Vanta, DataGuard vendent implicitement l'autonomie : *« scannez, vérifiez, vous êtes conformes. »* Ils produisent des dashboards et des rapports qui *ressemblent* à de la conformité — et qui déclenchent exactement la LLM Fallacy dans le domaine Professional Signaling.

EuTrustedIA est honnête sur la capability divergence. La posture est explicite : tout scanner automatique souffre structurellement de la LLM Fallacy. L'output de POSITRONIA est un brouillon structuré, pas une décision. L'écart entre les deux s'appelle capability divergence. L'antidote s'appelle l'Annuaire EuTrustedIA.

Concurrent	Promesse implicite	Position face à la LLM Fallacy
Snyk	« Votre sécurité est gérée »	Output = scan automatisé, pas arbitrage expert
OneTrust	« Votre conformité est assurée »	Dashboard ≠ responsabilité engagée
Vanta	« Certifié en quelques clics »	Certification SOC2 ≠ conformité AI Act/RGPD
EuTrustedIA	**« Nous documentons, l'expert valide »**	**Seul acteur honnête sur la capability divergence**

EuTrustedIA est le **seul acteur** qui dit explicitement *« l'IA ne suffit pas »* tout en proposant le pipeline complet (outil de documentation + annuaire de professionnels). Ce n'est pas une faiblesse — c'est de la crédibilité B2B face à des interlocuteurs sophistiqués (DPO, avocats tech, responsables conformité).

Implication 3 — La posture éditoriale anti-FUD, fondée sur la lucidité cognitive

EuTrustedIA ne vend pas la peur de l'AI Act. Elle vend la lucidité : comprendre pourquoi l'IA seule ne suffit jamais pour des sujets à responsabilité engagée.

Cette posture éditoriale interdit de produire du contenu de type *« comment utiliser ChatGPT pour votre conformité »* — ce serait alimenter exactement la LLM Fallacy que l'on combat. Elle impose en revanche d'expliquer, concrètement et sans alarmisme, comment le Professional Signaling fonctionne et pourquoi le brouillon n'est pas la décision.

Le fil éditorial : *« Vous avez un beau rapport. Voici pourquoi ce n'est pas encore de la conformité — et voici la marche suivante. »* Substance + factualité. Pas de FUD. Pas d'alarmisme sur les amendes. La réglementation existe ; notre rôle est de la rendre gérable, pas de l'instrumentaliser.

5.6.6 1.6.6 Ce que cela change dans les livrables EUDAI

Tous les livrables produits par POSITRONIA-CORE et par EUDAI portent, depuis cette version v1.3, un marquage explicite cohérent avec la doctrine capability divergence :

- **Badge obligatoire** sur chaque livrable généré (AIPD pré-remplie, fiche Article 50, registre Art. 30) : `BROUILLON — à réviser et signer par un DPO ou avocat qualifié avant tout effet juridique`
- **Métadonnées de document** systématiques : `status: draft | requires_professional_review: true | generated_by: POSITRONIA-CORE`
- **Lien vers l'Annuaire EuTrustedIA** dans chaque livrable : voie directe vers un professionnel pouvant combler ΔC
- **Page dédiée** (à venir) : `/pourquoi-positronia-ne-remplace-pas-votre-avocat` — vulgarisation des 3 mécanismes LLM Fallacy (fluency, opacity, attribution ambiguity) en langage non-technique, avec CTA Annuaire

Ce marquage n'est pas une faiblesse produit à minimiser. C'est une proposition de valeur explicite : *« nous sommes honnêtes sur ce que l'IA peut et ne peut pas faire. »* La transparence sur la capability divergence est elle-même un argument B2B différenciant face à des interlocuteurs qui ont déjà été déçus par des outils qui promettaient l'autonomie complète.

Référence académique : Kim, H., Yu, H., & Yi, H. (2026). *The LLM Fallacy : Misattribution in AI-Assisted Cognitive Workflows.* arXiv :2604.14807v1 [cs.AI], 16 Apr 2026. ddai Inc. — paper fondateur de cette section doctrinale. Consulté via vulgarisation et application au domaine de la conformité juridique.

6 Partie 2. Les 5 piliers EUDAI

6.1 2.0 *« Avant de commencer »*. l'auto-évaluation 12 axes pre-build

Le pilier le plus rentable de tout EUDAI s'applique **avant** la première ligne de code : **RGPD Art. 25** (*« Protection des données dès la conception et par défaut »*) et **AI Act Art. 25** (*« obligations dans la chaîne de valeur »*) imposent que la conformité soit **conçue dans l'architecture**, pas plaquée après coup.

Concrètement, cela signifie qu'**avant** d'écrire le premier prompt système, **avant** de signer avec un fournisseur de LLM, **avant** d'ouvrir un compte sur un cloud, le porteur de projet IA répond à **12 questions structurantes**. Chacune éclaire un risque réglementaire spécifique, et déclenche un **drapeau** quand la réponse est problématique.

Cette auto-évaluation est intégrée au ticket **LANCE-TOI 49 € unique** ainsi qu'aux abonnements **SOLO**, **GENESIS**, **AVANTAGES** et **ENTREPRISE** (cf. Préambule, et Partie 4 plans tarifaires).

6.1.1 2.0.1 Les 12 axes, questions et drapeaux

#	Axe	Question structurante	Drapeau rouge
1	**Cas d'usage IA**	Mon système fait : chatbot conversationnel ? agent autonome ? classification ? génération de contenu ? recommandation ? notation de personnes ?	Notation de personnes → **Art. 5 ou Annexe III** très probable
2	**Public cible**	Mes utilisateurs finaux sont : employés internes ? clients adultes ? mineurs ? public général ? personnes vulnérables ?	Mineurs ou personnes vulnérables → **AIPD obligatoire** + **AI Act Art. 5.1.b**

#	Axe	Question structurante	Drapeau rouge
3	**Type de données**	Je traite : aucune donnée personnelle ? données pseudonymisées ? données personnelles classiques ? données *catégories particulières* (santé, opinions, biométrie, vie sexuelle, syndic) ?	Catégories particulières → **RGPD Art. 9** + consentement explicite quasi obligatoire
4	**Modèle IA**	J'utilise : un LLM API (Mistral, OpenAI, Anthropic, …) ? un modèle open-weight self-hébergé ? un modèle entraîné par moi ? un agent multi-modèles ?	Modèle entraîné par moi sur données personnelles → **AIPD obligatoire** + **AI Act Art. 10**
5	**Hébergement**	Mon infrastructure est : 100 % EU souverain ? EU-friendly avec dépendances US ? US ? inconnu ?	US ou inconnu → **RGPD Art. 44-49** + Transfer Impact Assessment obligatoire
6	**Base légale RGPD**	Mon traitement repose sur : consentement Art. 6.1.a ? contrat Art. 6.1.b ? obligation légale Art. 6.1.c ? intérêt vital Art. 6.1.d ? mission service public Art. 6.1.e ? intérêt légitime Art. 6.1.f ?	Pas de réponse claire → **violation pure** dès le premier traitement
7	**Décision automatisée**	Mon système prend une décision qui produit un effet juridique ou similaire sur la personne (RH, crédit, accès service, sanction) ?	OUI → **RGPD Art. 22** + droit d'opposition + intervention humaine obligatoire

#	Axe	Question structurante	Drapeau rouge
8	**Stade entraînement**	J'utilise : un modèle pré-entraîné tel quel ? un fine-tune léger (LoRA, instruct) ? un entraînement complet sur mes données ?	Entraînement complet → **AI Act Art. 10** qualité des données + **EDPB Opinion 28/2024** anonymisation
9	**Volume utilisateurs**	Sur 12 mois prévus : < 100 ? 100 à 10 000 ? 10 000 à 1 M ? > 1 M ?	> 10 000 → **AIPD très probablement obligatoire** (large échelle Art. 35)
10	**Géographie utilisateurs**	Mes utilisateurs sont : France uniquement ? UE uniquement ? UE + monde ?	Hors UE → **transferts Art. 44-49** + DPA fournisseur LLM crucial
11	**Classification haut risque**	Mon cas d'usage tombe-t-il dans l'**Annexe III** (RH, éducation, crédit, santé, justice, infrastructure critique, biométrie d'identification) ?	OUI → **AI Act Art. 6 + 9-15** = obligations massives (qualité données, traçabilité, surveillance humaine, robustesse, cybersec)
12	**Transparence Art. 50**	Mon système : interagit avec un humain (chatbot) ? génère du contenu (texte/image/audio/vidéo) ? produit du *deepfake* ou du contenu manipulé ?	OUI → **AI Act Art. 50** + obligation de marquage à partir du **2026-08-02**

6.1.2 2.0.2 Comment l'auto-évaluation génère un *POSITRONIA Blueprint* (Diagnostic Pré-build)

Une fois les 12 axes renseignés, l'outil EUDAI produit un **POSITRONIA Blueprint** structuré en 5 sections :

1. **Risques rouges**, articles RGPD/AI Act déclenchés et niveau de criticité

2. **Choix corrects pré-validés**, pour chaque axe, alternatives qui éliminent le risque (avec catalogue **Stack Recommender**)
3. **AIPD pré-remplie sectorielle**, modèle d'analyse d'impact relative à la protection des données, généré pour le secteur du porteur (RH, santé, edtech, fintech, généraliste)
4. **Marquages Article 50 préparés**, kit de démarrage si concerné par Axe 12
5. **Recommandation de voie** : DIY (gratuit après pack) / FORMATION (Plan GENESIS 69 €/mois) / AVANTAGES (Plan AVANTAGES 99 €/mois avec Club Deal partenaires et rendez-vous remisés sur l'Annuaire), cf. Partie 3

> *Le Pilier 0 résout 70 % des erreurs structurelles **avant** qu'elles ne deviennent dette technique ou contentieux. Le coût de remédiation pre-build est en moyenne 5 à 10 fois inférieur au coût de remédiation post-build (estimation interne EuTrustedIA basée sur audit DirStarter + retours des 12 premiers experts contactés Phase 1).*

6.2 2.1 Pilier 1. Souveraineté radicale (à la racine — étymologique, *radix*)

> **Note terminologique** : *« radicale »* ici prend son sens étymologique latin *radix* (racine), pas le sens politique d'extrémisme. Souveraineté **dès la conception**, **à la racine** de l'architecture — pas dogmatique ni militante. La doctrine EUDAI v1.2 reformule ce pilier en posture **éclairante pragmatique** : EU first comme défaut recommandé, jamais comme interdit absolu.

6.2.1 2.1.1 La promesse au solopreneur

> *« Je veux construire mon produit IA sans avoir à choisir entre la facilité (tout chez OpenAI ou AWS) et la dépendance géopolitique — ni à subir un dogme. Comment ? »*

EUDAI répond avec une **doctrine éclairante en 3 routes graduées**, à choisir selon votre contexte (volume données, sensibilité, budget, charge sysops acceptable, exposition légale) :

- **Route A — Compliant-avec-votre-vendor actuel** (frontier US Anthropic/OpenAI/Google) : si vous êtes déjà sur Claude/GPT-5.5/Gemini, vous restez compliant via DPF (Data Privacy Framework EU-US 2023 + SCC Art. 46 + DPA + AIPD Art. 35 + marquage Art. 50). Trade-off : perf frontier max, dépendance vendor US, DPF challenged en justice (Schrems III en préparation).
- **Route B — Hybride dual-régime** : routing par sensibilité de donnée — frontier US autorisé pour données non-personnelles / anonymisées (brainstorming, recherche publique), EU souverain hosted pour données PII / sensibles / clients B2B. Trade-off : complexité architecturale, risque routing erroné.
- **Route C — EU souverain hosted** (recommandée par défaut) : modèles open-source (Mistral Nemo, Mixtral, LLaMA) hébergés chez **OVH AI Endpoints ⊠⊠**, **Scaleway Generative APIs ⊠⊠** ou **Infomaniak AI ⊠⊠**. Souveraineté EU pure, juridiction sans CLOUD Act, pricing pay-per-token. Trade-off : perf -5/-10 pts vs frontier US sur reasoning créatif (négligeable pour scoring conformité structuré).
- **Route D — Self-hosted air-gappé** : modèle GGUF open-weight (Mistral, Mixtral, LLaMA) tournant sur votre PC ou serveur bare-metal EU dédié, via llama.cpp ou vLLM. Souveraineté maximale absolue. Trade-off : charge sysops (CUDA drivers, monitoring), hardware CapEx, perf hardware-bounded.

Le principe **BYOK (Apportez votre propre clé)** reste **fortement recommandé** pour toutes les routes : vous restez propriétaire de vos secrets cryptographiques, votre fournisseur LLM ne peut pas utiliser vos requêtes pour entraîner ses modèles, et vous pouvez révoquer l'accès à tout moment. POSITRONIA auditera votre stack quelle que soit la route choisie et produira pour chaque scorer un rapport assorti des **trade-offs documentés** correspondant à votre route effective.

6.2.2 2.1.2 Articles fondement

RGPD Art. 28, sous-traitants. Tout fournisseur (LLM, cloud, base de données, vector store) qui traite vos données personnelles pour votre compte est un **sous-traitant** au sens RGPD. Il vous faut, **avant**

le premier traitement :

- un **contrat de sous-traitance écrit** (DPA), clauses obligatoires Art. 28.3 ;
- l'**identification précise** du périmètre de traitement et des finalités ;
- la **liste des sous-traitants ultérieurs** (AWS, GCP, Azure utilisés par le fournisseur LLM, etc.) avec droit d'opposition.

> *Pas de DPA signé avec votre fournisseur LLM = violation pure dès le premier appel API.*

RGPD Art. 44-49, transferts hors UE. Si vos données personnelles transitent vers un sous-traitant établi aux États-Unis, en Inde, ou dans tout pays sans décision d'adéquation européenne, vous devez :

- mettre en place des **clauses contractuelles types (CCT)** validées par la Commission européenne (décision (UE) 2021/914) ;
- conduire un ***Transfer Impact Assessment*** (TIA), analyse documentée du risque local, références à *Schrems II* (CJUE C-311/18) ;
- évaluer les **mesures supplémentaires** (chiffrement end-to-end, pseudonymisation, séparation des clés).

> *OpenAI et Anthropic sont domiciliés aux États-Unis. Une utilisation en production Phase B sans DPA + CCT + TIA = risque de sanction CNIL automatique.*

AI Act Art. 25, obligations dans la chaîne de valeur. Les fournisseurs et les déployeurs ont l'obligation de **collaborer** dans la chaîne de valeur IA pour assurer la conformité. Concrètement, vous devez pouvoir **démontrer** d'où viennent les modèles, les données, les guards.

6.2.3 2.1.3 Application EuTrustedIA, auto-démontrable (MAJ 2026-05-13)

Notre stack actuelle n'est pas une recommandation universelle. C'est notre application opérationnelle des critères de souveraineté à la date de rédaction. Chaque ligne ci-dessous est revisitable trimestriellement par un audit Stack Recommender (cf. § 3.3). **Décisions techniques Phase A actées 2026-05-13** : nous assumons publiquement un compromis transitoire « majoritairement européen » avec migration Phase C 100 % souveraine, dans l'esprit auto-démontrable qui exige de ne pas dissimuler les choix.

MAJ 2026-05-13 : la ligne LLM frontière a été repivotée suite à la découverte que Mistral a ajouté les USA aux processing locations via GCP en février 2026 sans notification préalable (plainte CNIL en cours). Notre route LLM passe par des **endpoints EU souverains hosted** (OVH AI Endpoints □□, Scaleway Generative APIs □□, Infomaniak AI □□) qui hébergent des modèles open-source. Mistral Cloud API au tier Standard est désormais hors de notre stack production par défaut. Mistral Compute (datacenter Essonne □□, déploiement progressif 2026 H2) sera évalué dès disponibilité.

Couche	Critère exigé	Application EuTrustedIA Phase A (go-live 2026-05-30)	Phase C (migration)
Cloud, hébergement applicatif	Établi UE/EEE/Suisse, certifié ISO 27001, juridiction connue, possibilité de self-host	**Vercel + DPA EU + data region Frankfurt ⚠⚠ RGPD-OK** (compromis transitoire assumé pour go-live rapide)	→ **Infomaniak Public Cloud ⚠⚠**
Base relationnelle	OSS, sans lock-in fournisseur	**Neon EU region ⚠⚠ RGPD-OK** (Postgres OSS managé, data EU)	→ **Infomaniak Postgres ⚠⚠**
Secrets management	Externe au hosting, juridiction EU connue	**Infisical Cloud EU Frankfurt ⚠⚠** (défense en profondeur post-incident Vercel avril 2026)	→ **Infisical self-host Infomaniak ⚠⚠**
Paiement	EU-natif, frais SEPA, DPA RGPD natif	**Mollie ⚠⚠** (PSP unique)	reste
Mail transactionnel	EU établi, RGPD-natif	**Brevo ⚠⚠** (ex-Sendinblue)	reste
Webinaires	EU établi	**kMeet Infomaniak ⚠⚠** (kSuite Business, manuel Phase A → API Phase B)	reste
LLM frontière (MAJ 2026-05-13)	**Endpoint hébergé EU pure, juridiction sans CLOUD Act, modèles open-source, pricing pay-per-token, BYOK fortement recommandé**	**OVH AI Endpoints ⚠⚠** OU **Scaleway Generative APIs ⚠⚠** OU **Infomaniak AI ⚠⚠** (arbitrage final acté dans ADR `2026-05-13`). Modèles : Mistral Nemo, Mixtral 8x22B, LLaMA 3.1/3.3. **Mistral Cloud API tier Standard ÉVICTÉ par défaut** suite GCP US processing Feb 2026.	Mistral Compute (datacenter Essonne ⚠⚠) si déploiement Q3/Q4 2026 effectif

Couche	Critère exigé	Application EuTrustedIA Phase A (go-live 2026-05-30)	Phase C (migration)
LLM open-weight self-hébergé (route D air-gappé)	Modèle ouvert, licence permissive, audit possible	Mistral open-weight (Large 2, Mixtral, Nemo), LLaMA 3.1 (origine US Meta, OK self-host EU pour POC, prudence en production critique)	reste
Embeddings	OSS ou EU établi, self-hostable	sentence-transformers OSS, Mistral Embed	reste
Vector store	EU établi ou OSS pur	Qdrant (origine FR/Berlin), pgvector OSS	reste
Guards / safety	OSS Apache 2.0, self-host EU	NeMo Guardrails (Apache 2.0), Mistral Moderation API, Garak (OSS adversarial)	reste
Marquage Art. 50	Standard ouvert, pas de SaaS US obligatoire	Solution maison + standard C2PA	reste
Eval framework	OSS, données stockées en EU souverain	Promptfoo OSS + scorers Python EuTrustedIA + storage PostgreSQL	reste

Storytelling go-live (MAJ 2026-05-13) : *« Stack majoritairement européenne : Mollie ✅, Brevo ✅, kMeet Infomaniak ✅, LLM frontière sur OVH/Scaleway/Infomaniak (modèles open-source EU hosted). Hébergement applicatif Vercel sous DPA RGPD (data region Frankfurt, compromis transitoire Phase A). Migration Phase C vers infrastructure 100 % souveraine. »*

Note transparente sur le LLM frontière : nous avons écarté Mistral Cloud API au tier Standard depuis février 2026 (transferts USA via GCP non notifiés, plainte CNIL en cours). Notre décision est documentée dans l'ADR transverse PiaXel `2026-05-13__doctrine_eutrustedia_eclairant_souverain_pragma` (LEDGER public `eutrustedia.eu/audit/ledger`). Pour vous : si vous utilisez Mistral Cloud API, vous restez compliant en activant le tier Enterprise + opt-out transfers + DPA + AIPD Art. 35 (Route A) ; OU vous switchez vers la Route C (EU hosted endpoint). Nous éclairons les deux options, nous ne jugeons pas.

Source détaillée : `docs/build-journal/2026-05-06__stack-tech-foundation.md`.

6.2.4 2.1.4 Détection POSITRONIA, drapeaux rouges

POSITRONIA n'analyse pas le code source applicatif du client en V1. Il produit son rapport de souveraineté à partir de trois sources non intrusives :

- le cahier des charges du client (PRD, architecture documentée, schémas de flux) ;
- les fichiers de configuration et de déclaration d'infrastructure (variables d'environnement non secrètes, fichiers Docker ou Terraform, exports n8n ou Zapier) ;
- l'inventaire déclaré des sous-traitants (LLM, cloud, base, vector store, guards) que le client renseigne lors de l'auto-évaluation 12 axes.

À partir de ces sources, POSITRONIA émet trois niveaux de drapeau :

- **Critique** : mono-vendor US (par exemple, toute la stack sur AWS sans abstraction infrastructure), recommandation de refonte.
- **Avertissement** : présence d'un fournisseur US sans DPA signé, ou sans TIA documenté.
- **OK** : stack 100 % EU avec au moins deux alternatives par couche critique.

Chaque drapeau pointe l'article violé (Art. 28 ou Art. 44-49) et propose trois alternatives EU issues du catalogue Stack Recommender (cf. § 3.3).

6.2.5 2.1.5 Livrable client

- **Rapport souveraineté PDF** signé par votre DPO partenaire (Annuaire EuTrustedIA)
- **Tableau d'équivalences EU** par couche actuelle (ce que vous utilisez aujourd'hui → 3 alternatives EU recommandées + leur licence + leur coût indicatif)
- **Modèle de DPA générique** avec clauses Art. 28 et CCT pré-renseignées (à co-signer avec chaque sous-traitant)

6.3 2.2 Pilier 2. Conformité auto-démontrable

6.3.1 2.2.1 La promesse au solopreneur

> *« Comment je prouve à un client B2B exigeant, à un investisseur, à un régulateur, que je suis sérieux sur la conformité, sans embaucher un cabinet à 50 000 € ? »*

EUDAI répond : en construisant un **dossier de preuve permanent**, vivant et public, qui démontre la conformité **par les artefacts** plutôt que par les déclarations.

6.3.2 2.2.2 Articles fondement

RGPD Art. 5.2, principe de responsabilité. Le responsable de traitement *« est tenu d'être en mesure de démontrer »* le respect des principes de l'Art. 5. Pas *« de respecter »*, *« de démontrer »*. L'écart est crucial : démontrer = produire des artefacts vérifiables.

RGPD Art. 24, obligation du responsable. Le responsable doit mettre en œuvre des *« mesures techniques et organisationnelles appropriées pour démontrer que le traitement est effectué conformément »*. La démonstration est l'obligation centrale.

RGPD Art. 30, registre des traitements. Tenu à jour, contenant 8 mentions obligatoires, opposable à la CNIL en cas de contrôle.

AI Act Art. 12, tenue de registres. Pour les systèmes IA à haut risque : *« journaux des opérations »* tenus tout au long du cycle de vie. Pour les autres : recommandé fortement.

AI Act Art. 17, système de management de la qualité. Pour les fournisseurs de systèmes haut risque, mise en place d'un système qualité documenté.

6.3.3 2.2.3 Application EuTrustedIA, auto-démontrable au sens fort

> *« Si on vend de la conformité, on doit être exemplaire. »* (Doctrine page 1)

EuTrustedIA matérialise ce principe par **six artefacts publics permanents** :

1. LEDGER append-only horodaté. Chaque décision technique structurelle (intégration d'un OSS tiers, choix d'architecture, modification de scope, incident sécurité) est inscrite dans un journal SHA-256-chaîné dont **toute modification rétroactive est détectable**. Public, accessible à `eutrustedia.eu/audit/ledger`.

2. Méthodologie publique. Le cadre EUDAI lui-même est ouvert (CC BY-NC 4.0). Les règles POSITRONIA YAML sont versionnées Git public. Les décisions sont des **ADR** (*Architecture Decision Records*) datés et signés.

3. Banc d'essai versionné public, `eutrustedia/sentinel-bench`.

Phase	Taille	Stratification	IC accuracy publié
A (mai-août 2026)	50 exemples synthétiques curés	baseline interne	±10 %
B (août 2026, go-live public)	**125 exemples stratifiés**	18 articles RGPD/AI Act × 4 stades de projet × 3 typologies + buffer cas borderline	**±6 %**
C+ (à partir de Q4 2026)	200-500 exemples	enrichissement par cas clients réels anonymisés (consentement explicite RGPD Art. 6.1.a)	±3-5 %

Toute mesure d'accuracy publiée mentionne **la version du banc**, **le modèle évalué**, et **l'intervalle de confiance**. Pas de chiffre nu.

À partir de la Phase B, le banc respecte aussi la séparation train, validation et test (60 % / 20 % / 20 %) imposée par notre doctrine transverse PiaXel Nexus sur les datasets (principe 9, séparation obligatoire dès 100 cas). Le sous-ensemble de test reste isolé pendant tout le cycle de développement et n'est utilisé que pour la mesure finale publiée. Cela évite que le score communiqué au marché soit en réalité un score de fit sur les cas qui ont servi à calibrer les prompts. C'est le seul moyen sérieux de revendiquer une mesure de généralisation, et c'est ce que les acteurs SaaS opaques comme Vanta, Drata ou OneTrust ne peuvent pas démontrer sur leurs propres benchmarks fermés.

4. AIPD interne. EuTrustedIA conduit sa propre AIPD (au sens RGPD Art. 35) sur le traitement de ses prospects et clients. Disponible à inspection sur demande motivée. Mise à jour à chaque changement de périmètre.

5. Marquages AI Act Art. 50 sur nos propres outputs. Toute recommandation de ce document, de notre site, de nos outils, *aidée par LLM* est explicitement marquée comme telle. Pas de tromperie sur l'origine humaine vs IA d'un texte produit par EuTrustedIA.

6. Cybersec 5-tests publics. Avant l'intégration de tout OSS tiers (Semgrep, Trivy, gitleaks, NeMo Guardrails, etc.), EuTrustedIA conduit 5 tests cybersec documentés et archive le rapport dans `docs/AUDIT/CYBERSEC/REPORTS/`.

6.3.4 2.2.4 Détection POSITRONIA, chez le client

POSITRONIA scanne le projet du client à la recherche d'**artefacts de démonstrabilité** :

Présence	Signal
Registre Art. 30 tenu et à jour	**OK**
Journaux d'opérations IA conservés ≥ 6 mois	**OK**
AIPD documentée signée	**OK**
ADR ou équivalent pour décisions techniques	**Attention** (recommandé, pas obligatoire)
Politique de gestion des violations sous 72 h	**OK** (RGPD Art. 33)
Rien de tout ce qui précède	**Critique** violation Art. 5.2 + Art. 24

6.3.5 2.2.5 Livrable client

- **Modèle de LEDGER** prêt à instancier (script Python signature SHA-256)
- **Modèle d'AIPD** sectoriel (RH, santé, edtech, fintech, généraliste)
- **Checklist auto-démontrabilité 12 points** opérationnelle
- **Politique de violation 72 h** rédigée + procédure de notification CNIL

6.4 2.3 Pilier 3. Humain dans la boucle final

6.4.1 2.3.1 La promesse au solopreneur

> *« Si POSITRONIA scanne mon code et me dit qu'il est OK, est-ce que je peux mettre en production avec ce seul rapport ? »*

Non. EUDAI tient une position non négociable : POSITRONIA est un **outil de diagnostic**, pas un signataire. La validation juridique passe **toujours** par un expert vérifié de l'**Annuaire EuTrustedIA**.

6.4.2 2.3.2 Articles fondement

RGPD Art. 22, décision automatisée et profilage. *« La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative. »*

Trois implications :

- les décisions à effet juridique requièrent **intervention humaine effective** (pas un *rubber stamping*) ;
- la personne a **droit d'opposition** et droit d'obtenir une **explication** ;
- des **catégories particulières** (Art. 9) traitées en décision auto sont quasi-toujours interdites sauf consentement explicite.

AI Act Art. 14, surveillance humaine pour systèmes haut risque. Les systèmes haut risque doivent être *« conçus et développés de manière à pouvoir faire l'objet d'une surveillance effective par des personnes physiques pendant la période d'utilisation »*. Quatre obligations spécifiques : compréhension capacités/limites, vigilance face aux biais d'automatisation, interprétation correcte des sorties, capacité à passer outre la décision.

AI Act Art. 26, obligations des déployeurs. Le déployeur d'un système haut risque attribue la surveillance humaine à des personnes formées, compétentes, et autorisées.

6.4.3 2.3.3 Application EuTrustedIA, pourquoi nos livrables sont revus, pas émis

Concrètement, voici ce qui se passe quand un client utilise notre mode *Audit & Conformité* (post-build) :

```
1. Client lance un scan POSITRONIA
2. POSITRONIA produit un rapport technique + AIPD pré-remplie + fiche Art. 50
3. Le rapport est transmis à un expert vérifié de l'Annuaire EuTrustedIA
   (DPO délégué, avocat tech, consultant AI Act selon le cas)
4. L'expert REVOIT le rapport, le complète, le signe en son nom
5. Le client reçoit un livrable signé qui engage l'expert,
   pas EuTrustedIA en tant que plateforme
```

Ce schéma protège **le client** (livrable opposable, signataire identifié et qualifié) et **EuTrustedIA** (pas de risque de qualification d'usurpation de mécanisme de certification, cf. Avis juridique page 1).

6.4.4 2.3.4 Détection POSITRONIA, chez le client

POSITRONIA cherche, dans le périmètre fonctionnel du client :

Cas détecté	Action recommandée
Décision automatisée à effet juridique sans intervention humaine	**Critique** Critique, Art. 22 violé. Nécessite *human-in-the-loop* obligatoire
Système classé haut risque (Annexe III) sans surveillance humaine documentée	**Critique** Art. 14 violé
Profilage de personnes vulnérables (mineurs, personnes handicapées)	**Critique** Risque cumulé Art. 22 + Art. 5.1.b AI Act
Décision automatisée avec **mention** d'opposition humaine, mais sans procédure réelle	**Attention** *Rubber stamping*, non conforme à la jurisprudence EDPB Guidelines 4/2017

6.4.5 2.3.5 Livrable client

- **Matrice « où mettre l'humain »** par type de décision (admission, scoring, modération, sanction, recommandation)
- **Procédure standardisée d'intervention humaine** (qui, quand, sous quels critères, avec quel délai)
- **Modèle de notification à la personne** (droit d'opposition + contact intervenant humain) conforme RGPD Art. 13-14

6.5 2.4 Pilier 4. Transparence des données d'entraînement

6.5.1 2.4.1 La promesse au solopreneur

> *« Mon modèle a été entraîné comment, sur quelles données, et est-ce que c'est légal pour ce que je veux en faire ? »*

EUDAI introduit un *« AI Training Hygiene Check »* (CO-035) : une procédure structurée pour interroger la **provenance**, **la base légale**, et **la légitimité d'usage** des données d'entraînement de tout modèle utilisé en production.

6.5.2 2.4.2 Articles fondement

RGPD Art. 5.1.a, loyauté et transparence. *« Les données à caractère personnel sont traitées de manière licite, loyale et transparente. »* Pour un modèle entraîné sur du *web scraping* sans consentement, la loyauté est sérieusement questionnée.

RGPD Art. 6, base légale. Six bases légales possibles. Pour des données d'entraînement non sollicitées, la base la plus invoquée par les fournisseurs LLM est *« intérêt légitime »* (Art. 6.1.f), base **fragile**, contestable au cas par cas, et qui ne tient pas pour les catégories particulières Art. 9.

RGPD Art. 9, catégories particulières. Données de santé, opinions politiques, convictions religieuses, vie sexuelle, syndic, biométrie d'identification, données génétiques. **Interdiction de principe** sauf exceptions strictes (consentement explicite, finalité médicale, intérêt public majeur).

RGPD Art. 35, AIPD obligatoire pour traitement à risque élevé. Un modèle entraîné sur grande échelle de données personnelles **est** un traitement à risque élevé.

AI Act Art. 10, qualité des données pour systèmes haut risque. Données d'entraînement, validation, test : pertinentes, représentatives, exemptes d'erreurs, complètes, prenant en compte les caractéristiques du contexte.

EDPB Opinion 28/2024 (octobre 2024), modèles IA et anonymisation. Réponse formelle aux questions soulevées par l'autorité irlandaise. Trois enseignements majeurs :

1. Un modèle peut être *« anonyme »* au sens RGPD si l'extraction de données personnelles individuelles n'est pas raisonnablement possible. Mais l'**inversion** d'anonymat (memorization attack) est un risque réel, à tester.
2. La doctrine *« données publiquement accessibles »* ne crée **pas** de base légale automatique pour ré-utilisation à grande échelle dans un entraînement IA commercial.
3. Le déployeur d'un modèle hérite des problèmes de l'entraînement amont, **ce n'est pas le problème de l'autre**.

6.5.3 2.4.3 Application EuTrustedIA, auto-démontrable

À la date de rédaction, EuTrustedIA n'entraîne pas de modèle de fondation. Nous utilisons exclusivement des modèles existants (Mistral, etc.) en mode inférence, sans fine-tuning sur nos données

client.

Concrètement, cela signifie qu'à ce jour :

— pas de risque Art. 5.1.a sur l'entraînement (nous n'entraînons rien) ;
— le risque demeure chez le fournisseur LLM (Mistral), nous nous reposons sur leur AIPD et leurs CCT ;
— si un client fine-tune un modèle via POSITRONIA ou EuTrustedIA, nous documentons la procédure et exigeons une AIPD client signée par son DPO.

Biais des modèles utilisés en inférence. Nous ne sommes pas neutres pour autant. Mistral, et plus généralement tout modèle de fondation que nous utilisons en inférence, porte des biais hérités de son entraînement. Nous n'en sommes pas les auteurs, mais nous sommes responsables au regard de nos clients de l'usage que nous en faisons. Nous maintenons donc une page de transparence publique, accessible sur `eutrustedia.eu/transparence-modeles`, qui liste pour chaque modèle utilisé : ses biais documentés par le fournisseur ou par la recherche académique, les tests de biais que nous appliquons sur POSITRONIA Bench (décomposition par secteur, par genre, par longueur de prompt, par langue), et les écarts mesurés. Si un écart entre sous-populations dépasse 15 %, nous l'investiguons et nous l'annonçons. Cette page V0 est publiée en même temps que le ship POSITRONIA CORE Phase A.

Cap futur transparent. À mesure que la base utilisateurs grandit, nous prévoyons d'enrichir nos jeux de données d'évaluation (POSITRONIA Bench notamment) à partir de cas réels, mais uniquement sous quatre conditions cumulatives, qui seront documentées publiquement avant tout usage. Premièrement, consentement explicite, libre, éclairé et révocable de l'utilisateur (RGPD Art. 6.1.a, pas d'opt-out déguisé). Deuxièmement, anonymisation forte testée par trois techniques nommées et documentées : *membership inference attack* (peut-on déterminer qu'un utilisateur précis appartient au dataset en interrogeant le modèle entraîné dessus ?), *extraction attack* (peut-on extraire un texte d'entraînement verbatim en sondant le modèle ?), *prompt injection probing* (peut-on faire ressortir des fragments de cas par injection contrôlée ?). Pour chaque test, nous documentons la métrique, le seuil acceptable, le résultat obtenu et la date du test, conformément à EDPB Opinion 28/2024. Troisièmement, durée de conservation limitée et purge automatique au-delà. Quatrièmement, AIPD interne mise à jour avant chaque évolution du périmètre. Tant que ces conditions ne sont pas verrouillées, le bench reste 100 % synthétique. Cette mention est volontaire et engage EuTrustedIA, conformément au pilier *« auto-démontrable »* qui exige la transparence sur les évolutions futures, pas seulement sur l'état présent.

Reproductibilité bit-à-bit. Tous nos verdicts POSITRONIA sont produits par défaut en précision FP32, choix de calcul qui maximise la reproductibilité et la stabilité numérique entre deux exécutions. Chaque snapshot de scan est signé SHA-256 et horodaté. Cela permet à un auditeur, à un régulateur, ou à un journaliste tech de re-vérifier nos mesures à la virgule près sur la même version Git du code, du dataset et du modèle utilisé. Cette reproductibilité bit-à-bit est une promesse contraignante, gravée dans notre doctrine technique transverse PiaXel Nexus (`DOCTRINE_DATASETS_PIAXEL.md`, principe 5).

6.5.4 2.4.4 Détection POSITRONIA, chez le client

POSITRONIA détecte, dans les configurations et la documentation du client (cahier des charges, schémas d'architecture, inventaire déclaré des datasets), les patterns suivants :

Pattern détecté	Verdict
Fine-tuning sur dataset *Common Crawl* sans filtrage	**Critique** Risque massif Art. 5.1.a + Art. 6
Fine-tuning sur dataset *LAION* (images, contesté multiple fois en justice)	**Critique** Risque réputationnel + juridique
Fine-tuning sur dataset client **sans** consentement explicite Art. 6.1.a	**Critique** Violation pure
Utilisation d'un modèle (Mistral, OpenAI, …) **sans** AIPD documentée côté client	**Attention** AIPD à produire
Anonymisation des données d'entraînement par seul *suppression de noms*	**Attention** Insuffisant, EDPB exige tests d'inversion d'anonymat
Distillation d'un modèle commercial (Mistral, OpenAI, etc.) sans vérification CGU du fournisseur amont	**Attention** Risque contractuel et juridique. Vérifier explicitement les conditions générales du fournisseur amont avant tout déploiement, certaines licences interdisent la distillation.
Documentation transparente de la provenance des données	**OK**

6.5.5 2.4.5 Livrable client, *AI Training Hygiene Report*

Pour chaque scan, le client reçoit :

- **Inventaire des données utilisées** en entraînement / fine-tuning / inference (avec leur provenance déclarée)
- **Analyse base légale** par type de données (Art. 6 + Art. 9 si applicable)
- **Recommandations de remédiation** avec catalogue de datasets EU-friendly (Pléiades, Croissant, OSS curés)
- **Modèle de notice de transparence** vis-à-vis des utilisateurs finaux (RGPD Art. 13-14 + AI Act Art. 50)

6.6 2.5 Pilier 5. Anti-deepfake et anti-empoisonnement

6.6.1 2.5.1 La promesse au solopreneur

> *« Comment éviter que les outputs de mon IA soient pris pour du contenu humain authentique, et comment me protéger contre les données malveillantes qu'on pourrait pousser dans mon modèle ? »*

EUDAI traite les deux extrémités du même problème : la **sortie** (marquage Art. 50, lutte contre les *deepfakes*) et l'**entrée** (anti-empoisonnement, anti-injection).

6.6.2 2.5.2 Articles fondement

Sortie, AI Act Art. 50. Quatre obligations distinctes :

1. **Art. 50.1**, système IA conversationnel : informer l'utilisateur qu'il interagit avec une IA, sauf évidence contextuelle.
2. **Art. 50.2**, fournisseur de contenu IA générique : marquer le contenu comme généré par IA dans un format lisible par machine (watermark technique, métadonnées C2PA, etc.).
3. **Art. 50.3**, fournisseur de système d'identification biométrique des émotions ou de catégorisation biométrique : informer les personnes concernées.
4. **Art. 50.4**, déployeur de *deepfake* : divulguer que le contenu est artificiellement généré ou manipulé.

Entrée, RGPD Art. 15 : droit d'accès aux données. Si vos données d'entraînement contiennent des données personnelles que vous n'avez pas le droit d'utiliser, la personne peut demander accès et opposition. **Cas concret** : un artiste qui découvre ses œuvres dans le dataset d'un modèle commercial peut faire valoir son Art. 15.

Entrée, AI Act Art. 5.2.a : interdiction de techniques subliminales ou délibérément manipulatrices visant à altérer substantiellement le comportement d'une personne. Couvre les **prompt-injections** malveillantes adressées à des utilisateurs finaux.

6.6.3 2.5.3 Application EuTrustedIA, auto-démontrable

Côté sortie :

— Toutes les sorties de notre site, de nos outils, de nos emails *aidées par LLM* sont marquées comme telles. Pas seulement à la première mention, sur **chaque artefact** produit (rapport scan, recommandation, fiche AIPD pré-remplie, contenu de blog).
— Format technique : métadonnées C2PA Coalition pour les images générées (à venir Phase B), avertissement textuel explicite pour les textes (*« Recommandation aidée par LLM Mistral, revue par l'équipe humaine PiaXel Nexus »*).
— Doctrine **PiaXel Nexus CO-031** : marquage entrée + sortie systématique sur chaque flux IA.

Côté entrée :

— POSITRONIA lui-même tourne avec **POSITRONIA-Observe Pro** (détection runtime injection/anomalies, Observe-only) + **Mistral Moderation API** (guard de modération) en série pour filtrer les prompts malveillants.
— Tests **Garak** (OSS adversarial testing) trimestriels documentés sur POSITRONIA pour détecter les régressions de robustesse.

6.6.4 2.5.4 Détection POSITRONIA, chez le client

Pattern détecté	Verdict
Système conversationnel IA sans annonce explicite à l'utilisateur	**Critique** Art. 50.1 violé
Génération de contenu IA (texte, image, audio, vidéo) sans marquage	**Critique** Art. 50.2 violé (à partir 2026-08-02)
Deepfake manipulé sans divulgation	**Critique** Art. 50.4 violé + risque pénal selon usage
Pipeline IA sans guard d'entrée (prompt-injection non filtrée)	**Attention** Risque sécuritaire élevé + Art. 5.2.a si exploité
Pas de tests adversariaux documentés	**Attention** Recommandation forte (pas obligation pure)
Marquage C2PA / SynthID / watermark textuel implémenté	**OK**

> **Cas concret 2026, la démocratisation du voice-clone non Art. 50.** Le 4 mai 2026, xAI a publié une API publique de voice-cloning intégrée à Grok. Cinq secondes d'audio, plus une passphrase de consentement, suffisent pour répliquer une voix. La passphrase vérifie qui clone, mais elle ne marque pas la sortie audio comme synthétique. Le distinguo doctrinal qu'EUDAI grave ici, c'est que *consentement n'est pas provenance*. La passphrase prouve qu'un consentement existe au moment du clone, elle ne prouve pas que la sortie générée porte la marque *« contenu synthétique »* exigée par l'AI Act Art. 50. Conséquence pour un solopreneur qui intègre cette API dans son produit B2B sans sur-couche de marquage : il expose son client final à un deepfake CEO ou à un deepfake support sans alibi Art. 50, et donc sans défense crédible si l'usage tourne mal. POSITRONIA détecte cette exposition par scorer dédié et propose la mitigation, soit un basculement vers un moteur self-host EU type Coqui TTS avec watermark audio, soit une procédure de vérification interne qui ajoute un marquage Art. 50 systématique avant diffusion.

6.6.5 2.5.5 Livrable client, *Kit de marquage Art. 50 démarrage*

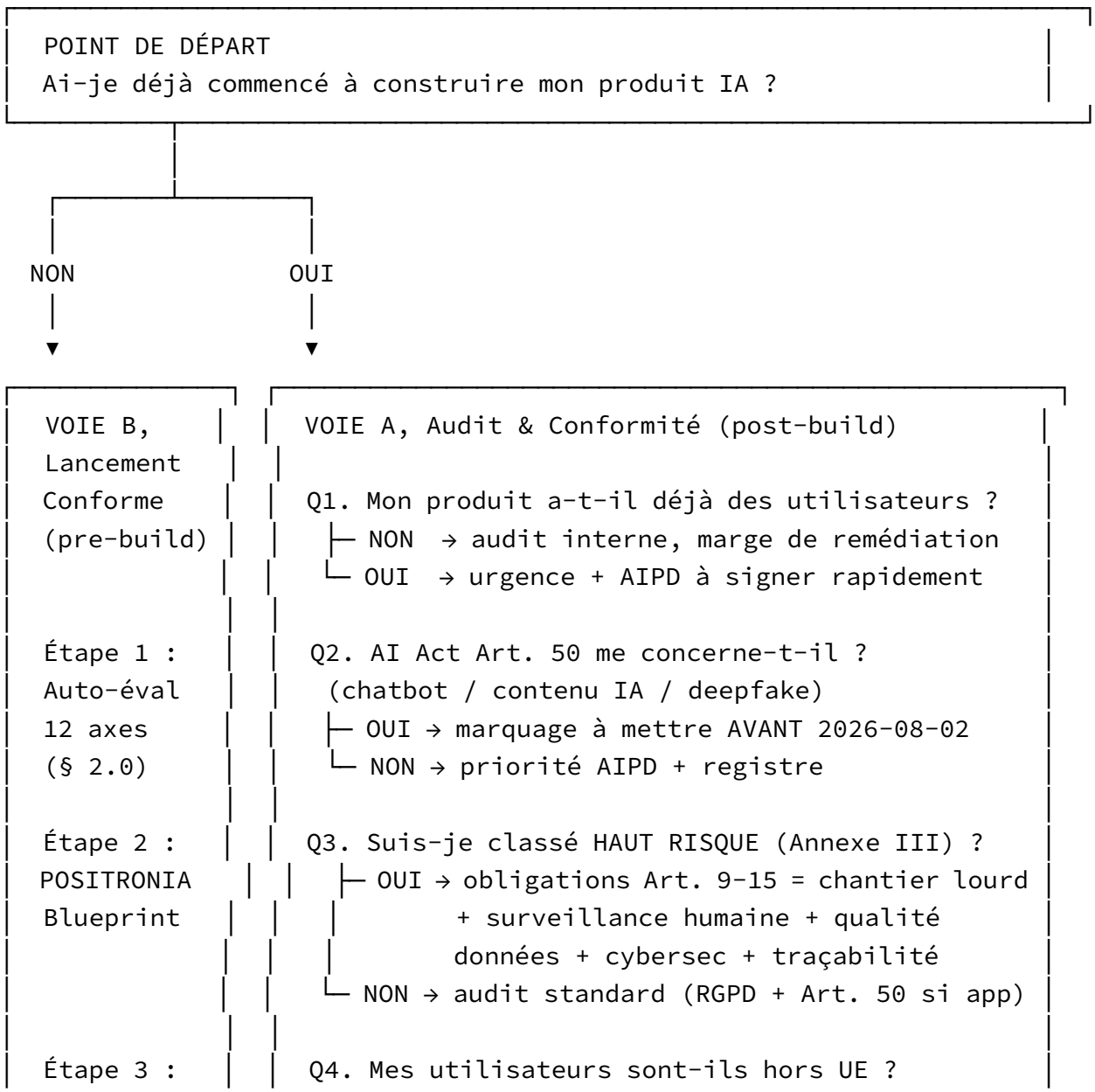
Inclus dès le plan **LANCE-TOI à 49 €** :

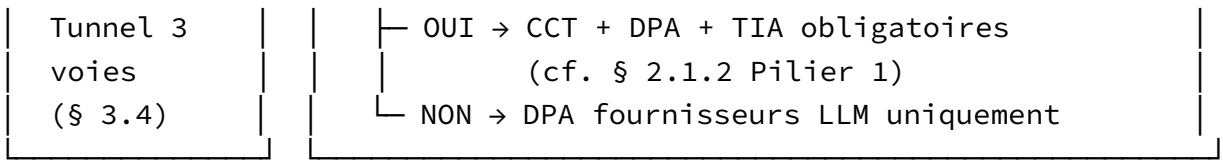
— **Bibliothèque de bandeaux d'avertissement** prêts à intégrer (chatbot, UI génération de contenu, *deepfake*)
— **Templates de notice utilisateur** RGPD Art. 13 + AI Act Art. 50 combinés
— **Procédure de marquage C2PA** pour les images (référence vers `c2pa.org` open-source)
— **Modèle de tests adversariaux** Garak prêts à exécuter en CI
— **Procédure de réponse à un incident** *deepfake* ou empoisonnement (notification + remédiation + post-mortem)

7 Partie 3. Comment l'appliquer concrètement

7.1 3.1 Arbre de décision pre-build. *« Où j'en suis sur chacun des 5 piliers ? »*

L'auto-évaluation 12 axes (§ 2.0) identifie les **risques bruts**. L'arbre suivant les transforme en **action prioritaire** : par où commencer, dans quel ordre, avec quel livrable cible.





7.1.1 Lecture de l'arbre par pilier

Pour **chaque pilier**, posez-vous les **3 questions diagnostiques** suivantes, vos réponses définissent votre charge de travail prioritaire :

Pilier	Question 1	Question 2	Question 3
1, Souveraineté radicale	Mes fournisseurs critiques sont-ils tous établis UE/EEE ?	Ai-je un DPA signé avec chaque sous-traitant ?	Ai-je une alternative EU mappée par couche ?
2, Auto-démontrable	Ai-je un registre Art. 30 à jour ?	Ai-je une AIPD signée pour chaque traitement à risque ?	Ai-je une procédure de violation 72 h écrite ?
3, Humain dans la boucle	Mon système prend-il des décisions à effet juridique ?	Si oui, ai-je un humain qualifié dans la boucle ?	Cet humain peut-il **passer outre** la décision IA ?
4, Transparence données	Ai-je documenté la provenance des données d'entraînement ?	Ai-je une base légale claire pour chaque jeu de données ?	Ai-je testé l'inversion d'anonymat (memorization) ?
5, Anti-deepfake / empoisonnement	Mes outputs IA sont-ils marqués au sens Art. 50 ?	Ai-je un guard d'entrée (anti-prompt-injection) ?	Ai-je documenté un test adversarial trimestriel ?

> *Une réponse négative à plus de 7 questions sur les 15 = **chantier prioritaire majeur**. Souscrivez un abonnement EuTrustedIA pour activer le mode Lancement Conforme ou prenez rendez-vous avec un expert vérifié de l'Annuaire EuTrustedIA via le Plan AVANTAGES.*

7.2 3.2 Checklist 25 points. conformité opérationnelle

Stratifiée **5 points × 5 piliers**. Chaque ligne est un **artefact à produire** ou une **action vérifiable**, pas une déclaration d'intention.

7.2.1 Pilier 1, Souveraineté radicale (5 points)

- ☐ **1.1** Inventaire des sous-traitants traitant mes données (LLM, cloud, base de données, vector store, mailing) avec leur juridiction d'établissement principal
- ☐ **1.2** DPA Art. 28 signé avec chaque sous-traitant identifié au point 1.1 (avec liste des sous-sous-traitants ultérieurs)
- ☐ **1.3** Pour chaque sous-traitant hors UE : CCT (Commission UE 2021/914) + Transfer Impact Assessment documenté
- ☐ **1.4** Pour chaque couche critique (LLM, hébergement, vector store, guards) : **3 alternatives EU** documentées dans un fichier `docs/SOUVERAINETE.md` interne
- ☐ **1.5** Procédure de migration documentée pour chaque dépendance critique (combien de temps + quel coût pour basculer si éviction nécessaire)

7.2.2 Pilier 2, Conformité auto-démontrable (5 points)

- ☐ **2.1** Registre des traitements Art. 30 tenu à jour (8 mentions obligatoires), outil minimum : un fichier `.csv` versionné Git
- ☐ **2.2** AIPD signée par votre DPO pour chaque traitement à risque élevé (Art. 35), référentiel CNIL : guide AIPD
- ☐ **2.3** Journaux opérationnels IA conservés ≥ 6 mois (logs des prompts, sorties, erreurs)
- ☐ **2.4** Procédure écrite de notification de violation sous 72 h (Art. 33-34) avec contact CNIL et personne-référente interne
- ☐ **2.5** Politique d'auto-démontrabilité publique (si vous êtes une entreprise B2B ambitieuse), *« on documente comment on s'applique nos propres règles »*

7.2.3 Pilier 3, Humain dans la boucle final (5 points)

- ☐ **3.1** Cartographie de toutes les **décisions automatisées** prises par votre système avec leur **type d'effet** (juridique, financier, accès service, autre)
- ☐ **3.2** Pour chaque décision à effet juridique : procédure d'intervention humaine documentée (qui, quand, sous quels critères, délai max)
- ☐ **3.3** Notice à la personne concernée (RGPD Art. 13-14) mentionnant explicitement le droit d'opposition (Art. 22) et un canal de contact humain
- ☐ **3.4** Si système haut risque (Annexe III) : surveillance humaine continue documentée (Art. 14 AI Act), formation + autorisation des personnes
- ☐ **3.5** Pour les livrables techniques (AIPD, fiche Art. 50, registre) : **revus et signés par un professionnel qualifié** (DPO / avocat / expert vérifié de l'Annuaire EuTrustedIA)

7.2.4 Pilier 4, Transparence des données d'entraînement (5 points)

- ☐ **4.1** Inventaire des datasets utilisés en entraînement / fine-tuning / inference avec leur provenance déclarée et leur licence
- ☐ **4.2** Pour chaque dataset : analyse base légale (Art. 6 si données personnelles, Art. 9 si catégories particulières)
- ☐ **4.3** Pour les fine-tunes sur données client : consentement explicite Art. 6.1.a documenté + droit de retrait
- ☐ **4.4** Tests d'**inversion d'anonymat** (memorization attack) sur le modèle final, conformément aux recommandations EDPB Opinion 28/2024
- ☐ **4.5** Notice de transparence vis-à-vis des utilisateurs finaux : *« nous utilisons les modèles X / Y entraînés par les fournisseurs Z / W sur les corpus suivants »*

7.2.5 Pilier 5, Anti-deepfake et anti-empoisonnement (5 points)

- ☐ **5.1** Système conversationnel ? **Annonce explicite** *« Vous interagissez avec une IA »* à chaque ouverture de session (Art. 50.1)
- ☐ **5.2** Génération de contenu IA ? **Marquage technique** (C2PA pour images, watermark textuel pour textes longs) à partir du **2 août 2026** (Art. 50.2)
- ☐ **5.3** *Deepfake* ou contenu manipulé ? **Divulgation explicite** au consommateur final (Art. 50.4)
- ☐ **5.4** Guard d'entrée filtrant les prompts malveillants (NeMo Guardrails / Mistral Moderation / équivalent) en série avant le LLM principal
- ☐ **5.5** Tests adversariaux trimestriels documentés (Garak ou équivalent) avec rapport archivé

7.2.6 Comment utiliser cette checklist

— **Score inférieur à 10/25** : démarrage urgent. Souscrivez un abonnement EuTrustedIA pour activer le mode adapté à votre stade (*Audit & Conformité* si déjà construit, *Lancement Conforme* sinon).
— **Score 10 à 18/25** : conformité partielle. Hiérarchisez les manquements via POSITRONIA Blueprint.
— **Score 19 à 23/25** : très bonne hygiène. Focus sur les 5 ou 6 points restants, visez le score plein avant tout audit externe.
— **Score 24 à 25/25** : vous êtes prêt pour un audit externe ciblé. Vous restez responsable de votre conformité, la checklist est un guide, pas une garantie juridique (cf. Avis juridique p. 1).

7.2.7 Et nous, on coche bien toutes les cases ?

Question légitime, et qu'il faut traiter de front. EuTrustedIA s'auto-évalue publiquement sur cette checklist 25 points, dans l'esprit du pilier 2 *« Conformité auto-démontrable »*. Le score actuel et son détail ligne par ligne sont publiés sur `eutrustedia.eu/audit/checklist-25` à la sortie publique du Framework, et mis à jour à chaque évolution structurelle de la stack ou du périmètre. Si nous découvrons une non-conformité, elle est inscrite avec sa date de détection, son plan de remédiation,

et sa date de résolution effective. C’est le seul moyen sérieux de proposer cette doctrine à d’autres : commencer par s’y soumettre soi-même.

7.3 3.3 Stack Recommender. Recommandeur Souverain EU

7.3.1 3.3.1 Philosophie en 6 principes

Le **Stack Recommender** (Recommandeur Souverain EU) produit, pour chaque projet IA, une **recommandation infrastructure + IA 100 % EU souveraine**. Il s'appuie sur 6 principes non-négociables :

1. **EU-first absolu.** Prioriser fournisseurs établis FR / DE / CH / NL / BE / LU / SE / FI / EE / IT / ES / IE.
2. **OSS prioritaire** quand alternative équivalente existe (Apache 2.0 / MIT / BSD / EUPL).
3. **3 alternatives minimum par couche.** Jamais de mono-vendor.
4. **Tagging géopolitique explicite** : (FR) (DE) (CH) (EU) (priorité) / (US) (drapeau d'avertissement souveraineté) / (CN) (à éviter par défaut).
5. **Auto-démontrable.** *« Nous recommandons exactement ce que nous utilisons pour PiaXel Nexus. »* Aucun acteur français / européen / américain ne pratique cela aujourd'hui.
6. **Refresh trimestriel** via routine automatique : 1er janvier / 1er avril / 1er juillet / 1er octobre. Vérification des licences, des versions, de la souveraineté (rachat US toujours possible), des CVE majeures.
7. **Single-binary, self-host, zéro cloud forcé.** Tout outil que nous recommandons doit pouvoir s'installer en un seul binaire, sur le serveur de son utilisateur, sans qu'aucun compte cloud externe ne soit obligatoire. Pas d'inscription préalable, pas de clé API distante imposée, pas d'envoi de données vers un service tiers que l'utilisateur ne contrôle pas. C'est la garantie de souveraineté radicale au niveau technique. Nous vérifions ce principe en pratique chez Coqui TTS, NeMo Guardrails, Promptfoo ou les UI Kubernetes self-hostables natives MCP. À l'inverse, un outil qui exige un compte SaaS US pour démarrer ne passe pas le critère, même s'il se présente comme open source.

7.3.2 3.3.2 Extrait catalogue v0, un échantillon par couche

Couche	EU recommandés (extrait)	Drapeau US courant	À éviter
Cloud / compute	Scaleway (FR), OVHCloud (FR), Outscale (FR), Infomaniak (CH), Hetzner (DE), Clever Cloud (FR), Exoscale (CH)	AWS / GCP / Azure (CCT + TIA obligatoires)	,

Couche	EU recommandés (extrait)	Drapeau US courant	À éviter
LLM frontière	Mistral (FR), Aleph Alpha Pharia (DE), EuroLLM (consortium EU), LightOn Alfred (FR), Pleias (FR), Kyutai (FR)	OpenAI / Anthropic / Google (CCT + TIA + risques transferts)	,
LLM open-weight (self-host)	Llama 3.x (US) (drapeau US, OK pour POC, prudence en production critique), Mistral open-weight (FR)	Llama (origine US, mais utilisable self-hébergé EU avec audit)	Qwen (CN) (sauf cas spécifique audité)
Embeddings	sentence-transformers OSS, Mistral Embed (FR), Pleias embeddings (FR)	OpenAI text-embedding-3	,
Vector store	Qdrant (FR/DE) (origine FR/Berlin), Weaviate (NL), pgvector OSS	Pinecone (US)	,
Inference	vLLM (OSS), TGI HuggingFace (FR), llama.cpp (OSS), Ollama (OSS)	,	,
Guards / safety	NeMo Guardrails (OSS, self-host EU), Mistral Moderation (FR), Garak (OSS)	Lakera (CH) (proche EU mais non-EU stricto sensu, réserve Phase D)	,
Observability LLM	LangFuse (DE), Phoenix Arize (OSS), PandaProbe (OSS, self-host)	,	,
AI dev safety, gouvernance multi-agent	Rosentic (OSS self-host, juridiction EU à confirmer, POC interne EuTrustedIA planifié)	,	,

Couche	EU recommandés (extrait)	Drapeau US courant	À éviter
Eval	Promptfoo (OSS), DeepEval (OSS), Inspect AI (UK) (UK AISI)	,	,
Speech / TTS / STT	Kyutai Moshi/Hibiki (FR), Coqui TTS (DE) recommandé dès la v1 (OSS Mozilla, self-host EU, marquage audio possible), Whisper OSS	xAI Grok Custom Voices et ElevenLabs cloud, à utiliser uniquement avec une sur-couche de marquage Art 50 maison, car ils ne proposent pas par défaut le marquage « *contenu synthétique* » exigé par l'AI Act	,
Watermarking Art. 50	C2PA Coalition (standard ouvert), maison dérivée doctrine PiaXel Nexus CO-031	SynthID Google (US) (en réserve)	,
Privacy / pseudonymisation	Presidio (OSS), spaCy + privacy, Aircloak (DE), Statice (DE)	,	,
Cookie consent	Axeptio (FR), Didomi (FR), Cookiebot (DK), Tarteaucitron (OSS)	,	,
AIPD / Compliance tooling	Witty Works (CH), Trustia (FR), Naaia (FR), Datapard (FR)	OneTrust (US)	,

> *Catalogue complet (~150 entrées) accessible aux abonnés Plan SOLO et au-dessus. Refresh trimestriel automatique. Objet d'un livrable **Stack Recommandée** personnalisée à chaque scan POSITRONIA.*

7.3.3 3.3.3 Différenciation absolue

> *« Voici les ~150 options EU souveraines de qualité élevée pour remplacer chaque brique US ou chinoise, réussir une stack 100 % souveraine est faisable, voici comment, et nous le faisons nous-*

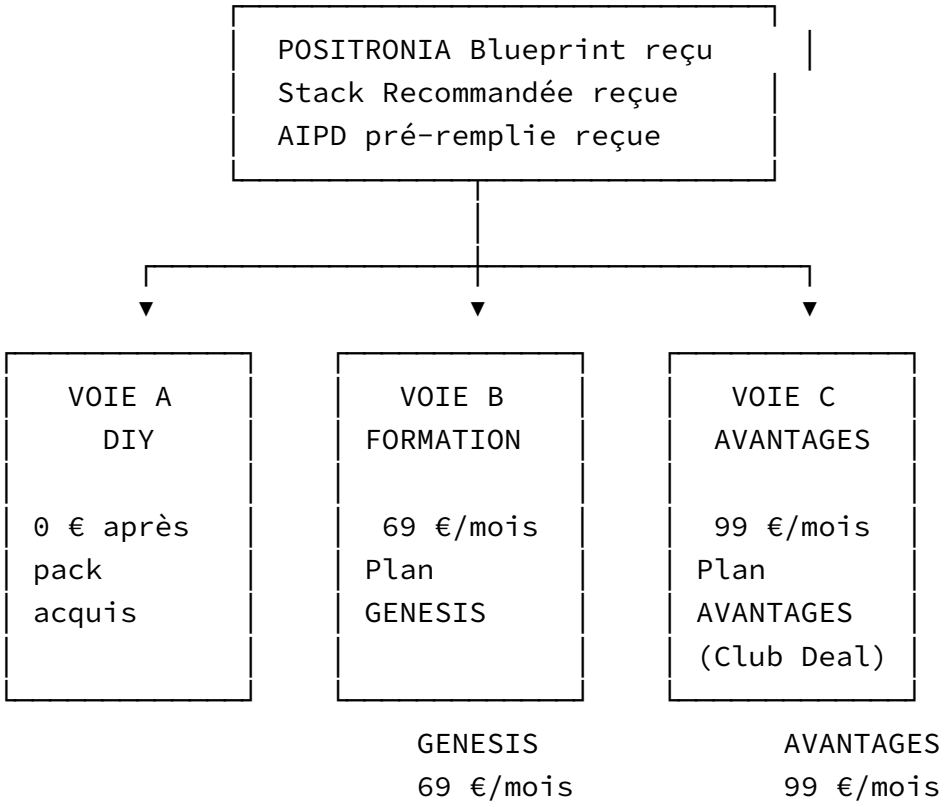
> *mêmes pour PiaXel Nexus. »*

Aucun cabinet de conseil et aucune solution concurrente, Snyk, Vanta, OneTrust, Naaia, Trustia, Witty Works incluses, ne propose un Stack Recommender EU souverain, à jour, gratuit pour la baseline, et appliqué de manière auto-démontrable.

MCP comme couche de contrôle infra. POSITRONIA et l'Annuaire EuTrustedIA sont conçus pour s'exposer en serveur MCP (Model Context Protocol, standard ouvert publié par Anthropic). Concrètement, un CTO ou un responsable conformité européen branche son IDE (Claude Code, Cursor) sur le serveur MCP qu'il a installé sur son propre serveur, et déclenche un scan ou récupère des recommandations sans qu'aucune donnée client ne quitte son infrastructure. Les acteurs cloud-first américains (Vanta, Drata, OneTrust) ne peuvent pas reproduire ce mode sans casser leur architecture commerciale. C'est un différenciateur technique structurel, pas un argument marketing. Le pattern est mature : il est déjà observé chez plusieurs UI Kubernetes single-binary natives MCP lancées en 2026.

7.4 3.4 Tunnel à 3 voies. *« Vous avez votre recommandation. Comment voulez-vous avancer ? »*

Une fois le **POSITRONIA Blueprint** + le **Stack Recommandée** reçus, l'outil propose **3 chemins** selon profil, budget, compétence technique et appétence pour la délégation.



7.4.1 Voie A, DIY (gratuit après pack acquis)

Pour qui : porteur technique autonome, capable de lire de la doc, à l'aise pour assembler une stack OSS, voulant garder un contrôle complet.

Vous recevez :

- documentation auto-générée du POSITRONIA Blueprint (PDF + markdown versionné)
- liens vers les **tutoriels OSS officiels** des outils recommandés (Mistral, NeMo Guardrails, Qdrant, Promptfoo, Garak, …)
- AIPD pré-remplie sectorielle (à signer par votre DPO une fois le projet stabilisé)
- accès à la communauté EuTrustedIA en lecture seule (forum public)
- vous **revenez nous voir** pour un scan documentaire de conformité post-build (mode *Audit & Conformité*) via un abonnement SOLO, GENESIS ou AVANTAGES

7.4.2 Voie B, FORMATION (Plan GENESIS, 69 €/mois)

Pour qui : porteur technique mais qui veut accélérer et obtenir une validation continue sans avoir à tout déchiffrer seul.

Vous recevez, en plus de la Voie A :

- des modules vidéo de formation appliquée aux 5 piliers EUDAI, mis en ligne progressivement (premier module : Pilier 1 Souveraineté radicale, prévu pour la sortie publique du Framework, suite déployée trimestre par trimestre selon retours utilisateurs) ;
- une bibliothèque d'AIPD sectorielles pré-remplies (chantier en cours, rythme de publication : 3 secteurs en v1, puis 5 secteurs supplémentaires en v1.1, soit le périmètre Phase B) ;
- une communauté Slack privée avec experts vérifiés et autres porteurs ;
- un scan annuel post-build inclus ;
- une consultation 1-to-1 mensuelle (30 min, par chat ou visio).

7.4.3 Voie C, AVANTAGES (Plan AVANTAGES, 99 €/mois)

Pour qui : porteur qui veut maximiser son réseau de partenaires souverains EU et accélérer la prise de décision en s'appuyant sur des experts vérifiés, sans s'engager sur un forfait d'heures arbitraire.

Vous recevez, en plus de la Voie B GENESIS :

- **Club Deal partenaires souverains EU** : un catalogue de remises commerciales préférentielles négociées avec un panel de fournisseurs souverains EU (cloud, LLM, vector store, observability, guards, hébergement, etc.). Le panel est en cours de constitution Phase A, les signatures sont publiées au fil de l'eau sur `eutrustedia.eu/club-deal`, dans l'esprit auto-démontrable du Framework. Aucun partenariat n'est annoncé tant qu'il n'est pas signé.
- **Rendez-vous remisés sur l'Annuaire EuTrustedIA** : sur la **première heure de consultation par expert distinct** (DPO délégué, avocat tech, consultant AI Act, data scientist, RSSI, développeur senior, expert infrastructure IA, expert automatisation), une **remise de 10 %** négociée par EuTrustedIA. Vous prenez rendez-vous avec qui vous voulez, autant d'experts différents que vous voulez. Au-delà de la première heure, le tarif standard de l'expert s'applique. Cette mécanique vous permet de cadrer votre projet à la carte, expert par expert, sans package d'heures imposé.
- **Honoraires versés directement à l'expert.** EuTrustedIA n'intermédie pas la facturation de la prestation. Vous signez et payez directement avec l'expert. EuTrustedIA n'est **pas** un cabinet de conseil et ne perçoit **aucune commission** sur la prestation, ni sur la première heure remisée, ni sur les heures suivantes. Notre modèle économique repose intégralement sur l'abonnement, ce qui garantit notre indépendance vis-à-vis des experts référencés.
- **Livrables expert au format conseil d'administration** : si l'expert produit pour vous un livrable structuré (rapport d'audit, AIPD signée, fiche Article 50), il vous est délivré au format conseil d'administration (présentation prête pour board, données chiffrées, justification juridique opposable).

> *3 voies, 3 prix, **même produit-d'entrée**. Funnel pure. Le porteur choisit son niveau d'engagement, pas son niveau de qualité.*

7.5 3.5 Trois cas pratiques. personas concrets

7.5.1 3.5.1 Persona A, *« Léa, dev solo SaaS chatbot »*

Contexte : Léa lance un SaaS B2C de chatbot pour artisans (réservation + FAQ). Stack actuelle : Next.js + Vercel + OpenAI GPT-4 + Stripe. ~1 500 utilisateurs après 6 mois.

Diagnostic POSITRONIA, articles déclenchés :

- **AI Act Art. 50.1** : système conversationnel, annonce explicite obligatoire à partir du 2026-08-02
- **RGPD Art. 28** : DPA OpenAI signé ? Probablement pas
- **RGPD Art. 44-49** : transfert vers les US (OpenAI) → CCT + TIA obligatoires
- **RGPD Art. 13-14** : information utilisateurs (politique de confidentialité spécifique IA)
- **RGPD Art. 32** : sécurité (chiffrement BDD, MFA, sauvegardes)

Plan EUDAI Léa :

1. **Pilier 1**, switcher OpenAI → **Mistral (FR)** avec BYOK (économie ~30 %, conformité native UE). Effort : 1 semaine de migration code.
2. **Pilier 2**, produire AIPD + registre Art. 30 + procédure violation 72 h (modèles fournis dans Plan SOLO).
3. **Pilier 5**, déployer bandeau *« Vous discutez avec un assistant IA, Léa et son équipe restent disponibles »* à chaque ouverture de chat.
4. Voie recommandée : **Voie B FORMATION (Plan GENESIS 69 €/mois)** ou **Voie C AVANTAGES (Plan AVANTAGES 99 €/mois)** si Léa veut activer le Club Deal partenaires (par exemple pour négocier ses crédits Mistral). Profil technique mais débordée, valeur ajoutée des 12 AIPD sectorielles + scan annuel.

7.5.2 3.5.2 Persona B, *« Marc, consultant data RH »*

Contexte : Marc, consultant data, vend à des PME un outil de **tri automatique de CV** alimenté par un LLM fine-tuné sur 50 000 CV historiques (avec consentement RH des entreprises clientes mais pas des candidats individuels).

Diagnostic POSITRONIA, articles déclenchés (rouge fluo) :

- **AI Act Annexe III + Art. 6** : tri de CV est **systématiquement classé haut risque** → obligations Art. 9-15 = chantier majeur
- **RGPD Art. 22** : décision automatisée à effet juridique (accès à l'entretien) → **droit d'opposition + intervention humaine obligatoire**
- **RGPD Art. 9** : si les CV contiennent des données de santé, opinions, appartenance syndicale (déclarations facultatives) → catégorie particulière, consentement explicite par candidat requis
- **RGPD Art. 6.1.f intérêt légitime des entreprises** : ne couvre **pas** les candidats, base légale fragile
- **RGPD Art. 35** : AIPD obligatoire (large échelle + données sensibles + IA)
- **EDPB Opinion 28/2024** : tests memorization attack à conduire, un fine-tune sur CV peut mémoriser des données individuelles

Plan EUDAI Marc :

1. **STOP**, produit en l'état non conforme, risque CNIL immédiat. Pause commerciale.
2. **Pilier 3**, réintroduire un humain dans la boucle obligatoire (le RH client lit la pile filtrée, l'IA classe mais ne **décide pas**). Reformuler le pitch commercial : *« assistance au tri, pas tri automatisé »*.
3. **Pilier 4**, refondre le fine-tune : retirer les CV avec mentions sensibles, anonymiser nominalement, tester l'inversion d'anonymat.
4. **Pilier 2**, produire AIPD signée + registre + procédure de réponse aux demandes Art. 15-22 candidats.
5. Voie recommandée : **Voie C AVANTAGES (Plan AVANTAGES 99 €/mois)**, Marc a un risque juridique élevé. Le Club Deal et la remise de 10 % sur la première heure de consultation auprès des experts vérifiés de l'Annuaire EuTrustedIA (DPO RH spécialisé, avocat tech, consultant AI Act) lui permettent de cadrer la mise en conformité expert par expert, sans forfait d'heures imposé. ROI : éviter une amende CNIL à 50 k€.

7.5.3 3.5.3 Persona C, *« Studio Lumina, génération d'images IA »*

Contexte : Studio créatif de 3 personnes, propose un outil web qui génère des **avatars stylisés** à partir de selfies utilisateurs. Modèle : Stable Diffusion fine-tuné sur leur propre dataset + mécanique de partage social.

Diagnostic POSITRONIA, articles déclenchés :

— **AI Act Art. 50.2** : génération de contenu image IA → **marquage obligatoire** à partir 2026-08-02 (C2PA recommandé)
— **AI Act Art. 50.4** : si l'outil permet de créer des *deepfakes* (substitution d'identité) → **divulgation explicite obligatoire**
— **AI Act Art. 5.1.h** : interdiction **catégorisation biométrique** → si Lumina détecte des caractéristiques sensibles (origine ethnique apparente) sur le selfie pour adapter le style, c'est interdit
— **RGPD Art. 9** : si le selfie est analysé (données biométriques au sens large) → catégorie particulière → consentement explicite obligatoire
— **RGPD Art. 6** : avatars partagés sur les réseaux sociaux → traitement de données personnelles à grande échelle → AIPD Art. 35
— **EDPB Opinion 28/2024** : si le dataset d'entraînement contient des images publiquement scrappées → loyauté Art. 5.1.a contestable

Plan EUDAI Studio Lumina :

1. **Pilier 5**, implémenter marquage **C2PA** sur tous les avatars produits (compatible publicateur réseaux sociaux). Bandeau utilisateur : *« Cette image est générée par IA »*.
2. **Pilier 4**, auditer le dataset d'entraînement : si scraping, refondre vers dataset *opt-in* (Adobe Firefly modèle, ou créer son corpus avec consentement).
3. **Pilier 1**, **interdire** la fonctionnalité *deepfake* (substitution d'identité d'autrui) ou la conditionner à un workflow de vérification d'identité du propriétaire de l'image source.

4. **Pilier 3**, modération a posteriori humaine sur les avatars générés (flag automatique des contenus problématiques + revue humaine).
5. Voie recommandée : **Voie C AVANTAGES (Plan AVANTAGES 99 €/mois)**, Studio Lumina est technique, motivé, et a besoin de la communauté + des AIPD sectorielles MarTech + jeux vidéo, et le Club Deal lui ouvre des remises sur les briques C2PA / inférence GPU EU souveraines clés pour son modèle. La remise sur la première heure d'un expert MarTech ou jeux vidéo de l'Annuaire EuTrustedIA finit de sécuriser le périmètre.

7.6 3.6 Quand faire appel à un professionnel humain ?. triage opérationnel

EUDAI est un cadre. POSITRONIA est un outil. Aucun ne **se substitue** à un professionnel qualifié pour les décisions à effet juridique. Voici à quel moment et pour quel rôle :

Besoin	Profil à solliciter	Quand absolument	Référence
AIPD à signer pour un traitement à risque élevé	DPO délégué (interne ou externe)	Avant la mise en production de tout traitement Art. 35	RGPD Art. 35
Validation d'un classement haut risque (Annexe III)	Avocat tech IA	Avant tout pitch commercial d'un système classé haut risque	AI Act Art. 6 + Annexe III
Notification d'une violation à la CNIL sous 72 h	DPO délégué + avocat data	Dès le constat de la violation	RGPD Art. 33
Réponse à une plainte Art. 15-22 d'une personne	DPO délégué (avocat en escalade)	Sous 1 mois	RGPD Art. 15-22
Audit cybersec d'un système haut risque	RSSI freelance ou cabinet pentest	Avant mise en production puis annuellement	AI Act Art. 15 (cybersecurity)
Défense devant la CNIL	Avocat data senior	Dès la notification de procédure	RGPD chapitre VIII
Négociation d'un DPA avec un fournisseur	Avocat data	Avant signature, surtout pour clauses sous-sous-traitants	RGPD Art. 28
Stratégie de marquage Art. 50	Consultant AI Act + DPO	Avant 2026-08-02	AI Act Art. 50
Cas spécifique secteur réglementé (santé, fintech, edtech)	Avocat sectoriel + DPO sectoriel	Dès la phase pre-build	RGPD Art. 9 + sectoriel

7.6.1 Et l'Annuaire EuTrustedIA dans tout cela ?

État actuel à la date de rédaction du Framework. L'Annuaire EuTrustedIA est **en cours de constitution Phase A**. À la publication du présent document, aucun expert n'est encore référencé publiquement. Les premiers experts vérifiés (10 à 15 ambassadeurs cibles) sont publiés au fil de l'eau dès le

go-live de la plateforme `eutrustedia.eu`. La doctrine d'auto-démontrabilité impose de ne rien annoncer qui ne soit pas signé : aucune fiche fictive, aucun profil placeholder, aucun partenaire annoncé qui n'aurait pas signé la charte qualité. Cette transparence est en ligne avec le pilier 2 *Conformité auto-démontrable*.

L'Annuaire référence uniquement des professionnels qui correspondent aux besoins listés ci-dessus, vérifiés un par un par l'équipe PiaXel Nexus en Phase A, puis ouvert à candidatures avec grille de scoring publique en Phase B. La doctrine, énoncée page 1 et résumée par *« si on vend de la conformité, on doit être exemplaire »*, impose un Annuaire curated, pas scrapé. Aucun profil n'y entre par scraping LinkedIn ou base achetée, à aucun stade.

Pour entrer dans l'Annuaire, chaque expert signe une charte qualité dont la rédaction définitive est en cours. Elle posera plusieurs engagements explicites. L'expert ne se substitue pas au DPO interne du client quand celui-ci existe déjà. Chaque livrable produit pour le client est documenté avec ses références d'articles et de jurisprudence. **L'expert s'engage à accorder une remise de 10 % négociée par EuTrustedIA sur la première heure de consultation aux abonnés du Plan AVANTAGES (99 €/mois)**, autant d'experts différents que l'abonné consulte. Au-delà de la première heure, le tarif standard de l'expert s'applique. **EuTrustedIA n'intermédie pas la facturation et ne perçoit aucune commission** sur la prestation, ni sur la première heure remisée, ni sur les heures suivantes : le revenu d'EuTrustedIA repose intégralement sur l'abonnement, ce qui garantit l'indépendance vis-à-vis des experts référencés et préserve la déontologie propre à chaque profession (notamment l'interdiction faite aux avocats de partager leurs honoraires avec un non-avocat). L'expert s'appuie sur les documents et résultats produits par les outils EuTrustedIA (POSITRONIA Blueprint, AIPD pré-remplie, rapport de souveraineté) et il peut faire plus que ce qu'EuTrustedIA recommande, jamais moins. Il ne peut pas réfuter les conclusions techniques d'un scan EuTrustedIA simplement parce qu'elles l'arrangeraient moins.

Une clause d'éviction est intégrée à la charte. Elle prévoit que l'expert peut être retiré de l'Annuaire, sans préavis, en cas de plainte cliente avérée et non résolue, de manquement éthique caractérisé, de fausse déclaration sur ses qualifications, de conflit d'intérêt nouveau non déclaré, ou de non-respect répété de la charte. Cette clause protège le client final en garantissant que l'Annuaire reste un signal de qualité, et elle protège la réputation collective de tous les experts qui y sont référencés.

Pour candidater, chaque expert fournit son numéro d'ordre professionnel quand il est applicable (Barreau, CNIL pour DPO certifié, etc.), une attestation d'assurance responsabilité civile professionnelle en cours de validité, sa grille tarifaire publique, ses conditions générales d'intervention, un lien de prise de rendez-vous, ses coordonnées professionnelles complètes (site, profils LinkedIn et autres réseaux sociaux pertinents). Toutes ces informations sont visibles depuis sa fiche publique sur l'Annuaire EuTrustedIA, en transparence totale pour le futur client.

Enfin, chaque expert référencé bénéficie d'un accès gratuit au Plan SOLO 29 €/mois pour activer le mode *Audit & Conformité*. L'idée est qu'un expert qui recommande EuTrustedIA à ses propres clients, ou qui intervient en mission via l'Annuaire, doit pouvoir manipuler les outils, comprendre les process, lire les rapports type POSITRONIA Blueprint, et se faire son avis personnel sur la doctrine. Les experts qui maîtrisent l'outil deviennent les meilleurs ambassadeurs et les meilleurs interlocuteurs pour les clients.

8 Partie 4. Ressources, plans, et appel à l'action

8.1 4.1 Ressources juridiques européennes. où trouver le texte authentique

EUDAI ne remplace pas la lecture des textes. Pour chaque article cité dans ce document, voici les **sources autoritatives** à consulter directement.

8.1.1 4.1.1 Textes de référence

Texte	Référence officielle	Accès
RGPD	Règlement (UE) 2016/679	EUR-Lex, version consolidée multilingue
AI Act	Règlement (UE) 2024/1689	EUR-Lex, version consolidée multilingue
Directive ePrivacy	Directive 2002/58/CE	EUR-Lex
Directive NIS 2	Directive (UE) 2022/2555 (cybersécurité)	EUR-Lex
DSA *(Digital Services Act)*	Règlement (UE) 2022/2065	EUR-Lex
CCT	Décision (UE) 2021/914, Clauses contractuelles types pour transferts hors UE	EUR-Lex
Schrems II	Arrêt CJUE C-311/18 du 16 juillet 2020	curia.europa.eu

8.1.2 4.1.2 EDPB *(European Data Protection Board)*, Opinions clés

Référence	Sujet	Pertinence EUDAI
Opinion 28/2024 (octobre 2024)	Modèles IA et anonymisation des données d'entraînement	Pilier 4, fondement du *AI Training Hygiene Check*

Référence	Sujet	Pertinence EUDAI
Guidelines 4/2017	Décision automatisée et profilage Art. 22	Pilier 3
Guidelines 4/2022	Calcul des amendes administratives	Référence sanctions
Recommandations 01/2020	Mesures supplémentaires post-*Schrems II*	Pilier 1, TIA

8.1.3 4.1.3 Autorités nationales, France et UE

Autorité	Pays	Site web
CNIL	France	cnil.fr
Bureau de l'IA UE	Bruxelles	digital-strategy.ec.europa.eu/en/policies/ai-office
AEPD	Espagne	aepd.es
Garante	Italie	gpdp.it
Datatilsynet	Danemark	datatilsynet.dk
DPA Bund	Allemagne fédérale	bfdi.bund.de
HBDI / autres bundesländer	Allemagne (16 autorités régionales)	sites individuels
DPC	Irlande (siège européen de la plupart des géants US)	dataprotection.ie
CNPD	Luxembourg	cnpd.public.lu
DPC Malta	Malte	idpc.org.mt

8.1.4 4.1.4 Référentiels CNIL spécifiques (FR)

- **Référentiel AIPD**, guide CNIL d'analyse d'impact relative à la protection des données
- **Référentiel cookies**, recommandation CNIL 2020 sur consentement et bandeaux
- **Pack conformité IA**, décembre 2024
- **Recommandations RGPD-IA**, série 2024-2025 (provenance, base légale, droits personnes)

8.1.5 4.1.5 Sources doctrinales académiques EU

Au-delà des textes officiels et des recommandations des autorités, plusieurs sources académiques font autorité de fait sur les questions d'éthique appliquée à l'IA et de doctrine de souveraineté numérique. EUDAI s'appuie sur les contributions suivantes, sans les substituer aux textes juridiques.

Institut EuropIA (Toulouse). Centre de recherche associé à l'INSERM, contributions régulières sur l'IA digne de confiance et l'éthique algorithmique. Référence pour le concept *Ethics by Evolution* mobilisé par EUDAI.

Jérôme Béranger (chercheur associé INSERM Université Toulouse 3, expert IA & Éthique à l'Institut EuropIA). Travaux sur l'éthique des systèmes algorithmiques et la structuration en trois natures d'éthique (descriptive, normative, réflexive).

GoodAlgo. Cabinet de conseil français en éthique du numérique. Contributions opérationnelles sur l'évaluation des biais et l'inclusion éthique proactive.

Polytechnique Insights (média officiel École polytechnique). Source académique vulgarisée. Les tribunes signées par les chercheurs cités ci-dessus apportent un appui doctrinal régulier au cadre EUDAI.

Cette liste s'enrichira au rythme de notre veille trimestrielle et des contributions reçues via la communauté EuTrustedIA.

8.2 4.2 Comment EuTrustedIA vous accompagne. les plans

EuTrustedIA propose **un seul abonnement** qui couvre indifféremment les deux moments de vie d'un projet IA (mode *Audit & Conformité* post-build et mode *Lancement Conforme* pre-build, cf. Préambule). Cinq offres tarifaires, du ticket d'entrée pre-build one-shot au plan ENTREPRISE sur devis, plus une variante **Mode Agence** dédiée aux DPO délégués, avocats tech et cabinets de conseil RGPD/AI Act qui outillent leur pratique sur les dossiers de leurs propres clients.

8.2.1 4.2.1 Le Lead Magnet, seule chose gratuite

EuTrustedIA n'a pas de plan Free récurrent. **La seule chose gratuite est le Livre Blanc** : ce document, le présent **PDF EUDAI Framework v1.0**, publié sous licence Creative Commons Attribution Pas d'Utilisation Commerciale 4.0 International (CC BY-NC 4.0), accessible en téléchargement gratuit avec capture email sur `eutrustedia.eu/eudai`. La newsletter mensuelle gratuite (cf. § 4.4.1 *Comment commencer dès aujourd'hui*) prolonge cette logique en maintenant la relation pédagogique sans contrepartie financière, jusqu'à ce que le porteur soit prêt à passer à un plan payant.

8.2.2 4.2.2 La grille des plans payants

Plan	Tarif	Pour qui	Inclus
LANCE-TOI	**49 € unique**	Solopreneur en phase d'amorçage, étudiant entrepreneur, indépendant en transition, porteur d'idée IA pre-build qui veut un cadrage immédiat	Auto-évaluation EUDAI 12 axes + POSITRONIA Blueprint Lite (diagnostic pré-build sur cahier des charges) + Stack Recommender automatique 100 % EU souverain + 3 modèles d'AIPD génériques + Kit de marquage Art. 50 (démarrage) + accès limité 30 jours à la doc EUDAI complète. Pas de récurrence, ticket d'entrée pre-build one-shot.

Plan	Tarif	Pour qui	Inclus
SOLO *(recommandé Phase A)*	**29 €/mois**	Solopreneurs IA techniciens autonomes, qui veulent rester conformes dans le temps malgré l'évolution de leur code, de leurs datas et du droit	5 scans POSITRONIA BYOK Mistral 3.5/mois (mode *Audit & Conformité* + mode *Lancement Conforme*) + auto-évaluation EUDAI 12 axes illimitée + AIPD pré-remplie versionnée, mise à jour automatiquement quand la jurisprudence évolue + archive scellée SHA-256 + accès complet à la doc EUDAI + veille active intégrée + refresh trimestriel Stack Recommender + support email 48 h

Plan	Tarif	Pour qui	Inclus
GENESIS	**69 €/mois** ou 745 €/an (-10 %)	Solopreneurs voulant maîtriser leur destin numérique, construire et piloter eux-mêmes leur écosystème souverain (infrastructure, stack IA, datas, sécurité, workflows, agents IA)	Tout SOLO + POSITRONIA Blueprint complet (pas Lite) + bibliothèque d'AIPD sectorielles (3 secteurs en v1, 8 en v1.1, 18 en v2) + **6 modules vidéo de parcours d'autonomie souveraine** progressifs (Module 1 au lancement, modules 2-6 trimestre par trimestre) + accès complet à l'**espace Communauté** intégré au site (Discourse OSS self-host EU) + **webinars trimestriels** avec experts en mode interview + scan annuel post-build inclus + support email prioritaire 24 h

Plan	Tarif	Pour qui	Inclus
AVANTAGES *(recommandé pour gagner du temps)*	**99 €/mois** ou 1 069 €/an (-10 %)	TPE / startup post-amorçage / projet financé (BPI / France 2030 / ESS / post-seed) qui veut accélérer le cadrage expert par expert et activer un Club Deal de partenaires souverains EU	Tout GENESIS + **Club Deal partenaires souverains EU** (catalogue de remises commerciales négociées avec fournisseurs cloud, LLM, vector store, observability EU, panel en cours de constitution Phase A, signatures publiées au fil de l'eau sur `eutrustedia.eu/club-deal`) + **rendez-vous remisés sur l'Annuaire EuTrustedIA** (remise de 10 % négociée par EuTrustedIA sur la première heure de consultation par expert distinct, autant d'experts que vous voulez, tarif standard ensuite) + question prioritaire dans la communauté + early access aux nouveaux modules. Honoraires versés directement à l'expert via Mollie Connect. EuTrustedIA n'intermédie pas la facturation et **ne perçoit aucune commission** sur la prestation, ni sur la première heure remisée, ni sur les heures suivantes.

Plan	Tarif	Pour qui	Inclus
ENTREPRISE	Sur devis (10 à 50 k€/an)	Grand compte / scale-up / ETI multi-projets, ou cabinets de conseil RGPD/AI Act qui outillent leurs dossiers clients (variante **Mode Agence**, cf. § 4.2.4)	Multi-scan illimité + SLA 99,9 % + DPO délégué optionnel + roadmap multi-projets dédiée + SSO/SAML + comptes utilisateurs multiples avec rôles + API POSITRONIA + tableau de bord consolidé groupe + onboarding personnalisé + marque blanche optionnelle

> *Le coût marginal client BYOK Mistral Medium 3.5 est estimé à environ 0,002 € par mois pour 5 scans, soit 0,007 % du prix Plan SOLO 29 €/mois (POC mesuré 2026-05-02). La marge brute par plan est élevée, ce qui finance la production de contenu pédagogique, les développements continus de POSITRONIA et la constitution du Club Deal.*

8.2.3 4.2.3 Add-on projet supplémentaire — 19 €/mois

Tous les plans payants (LANCE-TOI étant un one-shot, hors périmètre) incluent **un projet par défaut**. Pour chaque projet supplémentaire à suivre, l'abonné paie **19 €/mois** en supplément. Cet add-on inclut :

- **5 scans mensuels supplémentaires** dédiés au nouveau projet (use-it-or-lose-it, non cumulables)
- **Tous les avantages du plan principal** appliqués à ce nouveau projet (auto-évaluation EUDAI, AIPD versionnée, archive SHA-256, Stack Recommender, livrables)
- **Espace projet dédié** dans le dashboard client (séparation claire entre les projets, pas de mélange de scans, exports par projet)

L'add-on est **toujours facturé en mensuel découplé**, indépendamment du cycle annuel du plan principal. Cette mécanique évite les calculs de prorata et garde une UX simple. Cohérent avec le principe *« on se forme une fois, on utilise N fois »* : le porteur ne paie pas pour s'éduquer plus en ouvrant un 2e projet, il paie pour le **droit d'usage** des outils POSITRONIA sur ce nouveau périmètre.

8.2.4 4.2.4 Variante Mode Agence ENTREPRISE (Phase B)

Activée en Phase B (3 à 6 mois après la sortie publique), la variante **Mode Agence** est conçue pour les **DPO délégués, avocats tech, RSSI freelance, cabinets de conseil RGPD/AI Act** qui travaillent sur les

dossiers de leurs propres clients. Le cabinet utilise EuTrustedIA en interne pour produire ses livrables (AIPD signée, rapport conformité, fiche Article 50). Le client final reçoit ces livrables au nom du cabinet, sous la responsabilité juridique du DPO ou de l'avocat. Le client final n'a aucun compte EuTrustedIA, ne voit jamais l'interface, et n'a pas besoin de connaître nominativement l'outil utilisé en interne par son conseil (sauf au titre de la transparence des sous-traitants ultérieurs RGPD Art. 28.4 dans le contrat de sous-traitance entre le cabinet et son client).

Trois sous-modes selon la taille du cabinet :

— **AGENCE STARTER** : DPO solo, avocat indépendant, RSSI freelance. Jusqu'à 5 dossiers clients suivis simultanément + scans dédiés par dossier + livrables au format cabinet sans branding EuTrustedIA visible + DPA signé entre EuTrustedIA et le cabinet
— **AGENCE PRO** : Cabinet 2-10 personnes. Multi-utilisateurs avec rôles + jusqu'à 25 dossiers + dashboard agence consolidé + onboarding personnalisé + responsable EuTrustedIA dédié
— **AGENCE ENTERPRISE** : Cabinet 10+ personnes. Dossiers illimités + SSO/SAML + API POSITRONIA + marque blanche optionnelle + SLA 99,9 % + comité de pilotage trimestriel

Tarification sur devis Phase B, fourchette indicative **149 € à 2 990 €/mois** selon volume de dossiers, nombre d'utilisateurs et niveau de service.

Cette variante est **distincte de la marque blanche** : la marque blanche permet de **revendre** EuTrustedIA sous le branding d'un cabinet revendeur (mode B2B2C). Le Mode Agence est un **outil de production interne** pour le cabinet, pas une revente.

8.2.5 4.2.5 Cycle de facturation et options annuelles

Tous les plans (sauf LANCE-TOI one-shot et ENTREPRISE sur devis) sont **mensuels par défaut**, sans engagement, résiliables à tout moment depuis le dashboard client. Le porteur qui veut s'engager peut basculer son plan en annuel et bénéficie de **10 % de réduction** sur le tarif total :

Plan	Mensuel	Annuel à -10 %
SOLO	29 €/mois × 12 = 348 €	**313,20 €/an**
GENESIS	69 €/mois × 12 = 828 €	**745,20 €/an**
AVANTAGES	99 €/mois × 12 = 1 188 €	**1 069,20 €/an**

L'add-on projet supplémentaire reste mensuel découplé même sur un abonnement annuel.

8.2.6 4.2.6 Le cycle complet, pourquoi vous restez avec nous longtemps

```
mois 0        Lance-Toi     → audit pre-build, premier projet (49 € one-
shot)
mois 1-3      Solo        → vous restez conformes dans le temps (29 €/mois)
mois 3-6      Genesis      → parcours d'autonomie souveraine (69 €/mois)
```

```
mois 6-12      Avantages     → Club Deal partenaires + experts à la carte (99 €/mois)
mois 12+          Avantages /    → vous scalez, multi-projets, équipe
                  Entreprise
```

LTV cumulée typique sur 36 à 48 mois : **2 500 à 5 500 €** par client de cohorte d'entrée moyenne, **15 à 50 k€/an** par client ENTREPRISE. C'est exactement la **valeur vie client multipliée par 5 à 10** comparée à un audit ponctuel one-shot. Et c'est pourquoi notre tarification d'entrée est volontairement basse, nous misons sur la durée de la relation, pas sur le ticket d'achat unique.

8.3 4.3 Disclaimers techniques. comment ce document a été produit

Conformément au principe **auto-démontrable** (Pilier 2) et aux obligations **AI Act Art. 50.2**, voici comment ce document a été conçu.

8.3.1 4.3.1 Production éditoriale

- **Édité par** : **PiaXel Nexus** (SASU française en cours de constitution), incubateur de projets dont **EuTrustedIA.eu** est le premier projet monétisé. Une transformation en **EU Inc.**, premier statut d'entreprise 100 % européenne, est planifiée à 12-24 mois selon l'avancement de la législation européenne sur ce statut.
- **Aide rédactionnelle** : assistant IA Claude (Anthropic, modèle Opus 4.7, janvier 2026), utilisé pour la mise en forme, la structuration des tableaux, la cohérence de tonalité et la vérification croisée des références juridiques. Conformément à la doctrine PiaXel Nexus sur les niveaux d'usage IA (cf. Préambule, § *Trois niveaux d'usage IA*), l'usage de Claude relève ici du **niveau 2** (outillage interne au service de l'éditeur), pas du niveau 3 (système IA exposé aux clients finaux). Aucune donnée personnelle de tiers n'a été soumise au modèle pendant la production de ce document.
- **Validation finale** : 100 % humaine. Chaque article cité a été vérifié sur source authentique (EUR-Lex, EDPB, CNIL).
- **Versionnage** : `eutrustedia/eudai-framework` (Git public CC BY-NC 4.0).

8.3.2 4.3.2 Marquage AI Act Art. 50 sur ce document

Ce document est un **contenu hybride** : structure et exemples conçus humainement, mise en forme et reformulations *aidées par LLM*. Au sens strict de l'AI Act Art. 50.2 (qui s'applique aux systèmes IA en service à partir du 2026-08-02), ce document **précède** la date d'application, mais nous appliquons volontairement la règle **dès maintenant**, par cohérence avec la doctrine *« si on vend de la conformité, on doit être exemplaire »*.

8.3.3 4.3.3 Limites connues

- **Couverture sectorielle non exhaustive** : santé (HDS, dispositifs médicaux), fintech (DORA, MIFID II), edtech, public-sector traités en surface. Versions sectorielles approfondies prévues Phase B+.
- **Pas de jurisprudence consolidée** sur AI Act (texte récent, premiers contentieux à venir 2026-2027).
- **Phase A** : recommandations basées sur 50 exemples synthétiques + 12 ambassadeurs Annuaire EuTrustedIA. Phase B : enrichissement à 125 exemples stratifiés + cas clients réels (cf. § 2.2.3).
- **Pas une consultation juridique** : voir Avis juridique page 1.

8.4 4.4 Comment commencer dès aujourd'hui

> **La conformité n'est pas un coût pour vous, c'est votre meilleur argument commercial.** Un client B2B européen qui vous commande une mission demain vous demandera trois choses, dans cet ordre : où sont les données, comment vous traitez le RGPD, et quelle est votre position sur l'AI Act. EUDAI vous met en position de répondre *« voici mon dossier, signé par mon DPO partenaire, en 24 heures »* pendant que votre concurrent répond *« il faut que je me renseigne, sous trois semaines »*. Sur un projet à 5 000 € de valeur, l'avance commerciale vaut bien plus que le coût d'avoir tout préparé en amont.

8.4.1 4.4.1 Trois actions concrètes en moins d'une heure

1. Faites votre auto-évaluation 12 axes (gratuit, 20 minutes). Allez sur `eutrustedia.eu/auto-evaluation` et répondez aux 12 axes décrits au § 2.0. Vous recevez immédiatement un POSITRONIA Blueprint Lite et un score de risque par pilier.

2. Téléchargez la checklist 25 points (gratuit). Disponible en PDF, DOCX et Markdown sur `eutrustedia.eu/checklist-25`. À cocher en équipe, à conserver dans `docs/COMPLIANCE/` de votre dépôt Git.

3. Inscrivez-vous à la newsletter EuTrustedIA (gratuit). Une newsletter tous les 15 jours sur les évolutions concrètes RGPD et AI Act applicables aux solopreneurs IA EU. Pas de remplissage : chaque numéro contient un article ou une jurisprudence, suivi de ce que cela change pour vous opérationnellement. Inscription sur `eutrustedia.eu/newsletter`. La mise en place de cette newsletter (outil d'envoi, ligne éditoriale, calendrier de publication, moteur de constitution de la liste, conformité opt-in renforcée) fait elle-même l'objet d'un chantier dédié documenté en interne, dans l'esprit auto-démontrable du Framework.

8.4.2 4.4.2 Si vous voulez aller plus loin

- **Plans EuTrustedIA** : `eutrustedia.eu/plans` (LANCE-TOI 49 € unique, SOLO 29 €/mois, GENESIS 69 €/mois, AVANTAGES 99 €/mois recommandé, ENTREPRISE sur devis).
- **Mode Audit & Conformité** (post-build) : `eutrustedia.eu/audit-conformite` (présentation du parcours et accès aux plans).
- **Mode Lancement Conforme** (pre-build) : `eutrustedia.eu/lancement-conforme` (présentation du parcours et accès aux plans).
- **Annuaire des experts** : `eutrustedia.eu/annuaire` (consultation gratuite, prise de rendez-vous via les experts vérifiés, remise 10 % sur la première heure pour les abonnés AVANTAGES).
- **Devenir expert de l'Annuaire** (consultants, DPO, avocats tech, RSSI, data scientists) : `eutrustedia.eu/devenir-expert`.
- **Mode Agence ENTREPRISE** (DPO délégués, cabinets de conseil RGPD/AI Act, ouverture Phase B) : `eutrustedia.eu/agence`.

8.4.3 4.4.3 Nous écrire

Les adresses de contact sont en cours de mise en place pour la sortie publique du Framework.

- Pour une question juridique sur ce document : `legal@eutrustedia.eu` (réponse sous 5 jours ouvrés une fois la boîte ouverte).
- Pour un partenariat ou une collaboration : `partenaires@eutrustedia.eu`.
- Pour la presse : `presse@eutrustedia.eu`.

8.5 4.5 Avis juridique final. à relire avant action

Reprise et confirmation de l'Avis juridique placé en page 1.

EUDAI Framework est un **référentiel doctrinal et opérationnel**. Il n'est **pas** un avis juridique individualisé. EuTrustedIA et PiaXel Nexus ne sont **ni** un cabinet d'avocats, **ni** un cabinet de DPO délégué, **ni** un organisme habilité à délivrer une certification au sens du RGPD (Art. 42-43) ou de l'AI Act (Art. 43).

EuTrustedIA documente la conformité ; elle ne la certifie pas. Tout livrable produit par nos outils (AIPD pré-remplie, fiche Article 50, registre des traitements, rapport de souveraineté) doit être **revu et signé** par un professionnel qualifié, DPO délégué, avocat tech, ou expert vérifié de l'Annuaire EuTrustedIA, **avant production de tout effet juridique opposable**.

Les recommandations de ce document sont **génériques** et ne tiennent pas compte de votre cas particulier, de votre secteur, de votre juridiction d'établissement principal, ni de l'état du droit en vigueur à la date de votre lecture.

8.6 4.6 Lexique. acronymes et termes techniques

Ce lexique regroupe par ordre alphabétique les acronymes et termes techniques utilisés dans le présent document. Il n'a pas vocation à se substituer aux définitions juridiques officielles, qui se trouvent dans les textes eux-mêmes (cf. § 4.1 *Ressources juridiques européennes*).

AaaS *(Agentic as a Service)*. Modèle commercial dans lequel un fournisseur expose un agent IA autonome (capable d'exécuter des tâches en plusieurs étapes via des outils) sous forme de service en ligne. Le déploiement à des clients finaux relève du niveau 3 d'usage IA et engage les obligations AI Act du déployeur, et potentiellement du fournisseur.

ADR *(Architecture Decision Record)*. Document court et daté qui consigne une décision technique structurelle, son contexte, ses options évaluées et la justification du choix retenu. Utilisé chez PiaXel Nexus comme outil opérationnel du Pilier 2 *Conformité auto-démontrable*.

AIPD *(Analyse d'Impact relative à la Protection des Données)*. Document obligatoire au sens du RGPD Art. 35 pour les traitements à risque élevé (large échelle, IA, données sensibles). Identifie les risques pour les personnes concernées, les mesures de mitigation, et est signé par le DPO.

AI Act. Règlement (UE) 2024/1689 sur l'intelligence artificielle. Texte européen majeur applicable de manière échelonnée 2024-2027, dont l'Art. 50 (transparence des contenus IA) entre en vigueur le 2 août 2026. Encadre les fournisseurs et déployeurs de systèmes IA selon leur niveau de risque.

Annexe III (AI Act). Liste limitative des cas d'usage classés *haut risque* par l'AI Act : biométrie, infrastructures critiques, éducation, emploi, services privés et publics essentiels, application de la loi, migration, justice. Une classification haut risque déclenche les obligations Art. 9-15 (qualité des données, traçabilité, surveillance humaine, robustesse, cybersécurité).

Annuaire EuTrustedIA. Annuaire de professionnels vérifiés (DPO délégués, avocats tech, consultants AI Act, RSSI, data scientists conformité) référencés par PiaXel Nexus pour intervenir auprès des abonnés EuTrustedIA dans les modes *Audit & Conformité* et *Lancement Conforme*. Aucune entrée par scraping, vérification individuelle. Remise négociée de 10 % sur la première heure de consultation pour les abonnés du Plan AVANTAGES, par expert distinct, autant d'experts que l'abonné consulte.

Anonymisation vs pseudonymisation. Au sens RGPD, une donnée *anonymisée* ne permet plus, par aucun moyen raisonnable, de réidentifier la personne ; elle sort du champ du RGPD. Une donnée *pseudonymisée* (clé de réidentification stockée séparément) reste une donnée personnelle au sens RGPD. L'EDPB Opinion 28/2024 rappelle que beaucoup d'anonymisations ne tiennent pas le test d'inversion d'anonymat.

Article 50 (AI Act). Article central pour les solopreneurs IA. Quatre obligations distinctes : informer l'utilisateur d'un système conversationnel qu'il interagit avec une IA (50.1), marquer les contenus générés par IA dans un format lisible par machine (50.2), informer les personnes en cas de catégorisation biométrique (50.3), divulguer les *deepfakes* (50.4). Entrée en vigueur 2 août 2026.

Auto-démontrable. Doctrine PiaXel Nexus selon laquelle l'éditeur s'applique à lui-même, en premier et publiquement, chacune des recommandations qu'il émet. Matérialisée par six artefacts permanents (LEDGER, méthodologie publique, banc d'essai, AIPD interne, marquages Art. 50, audits cybersec).

Banc d'essai (sentinel-bench). Jeu de données d'évaluation versionné Git public utilisé pour mesurer les performances de POSITRONIA (accuracy, biais, intervalle de confiance). Stratifié en train / validation / test à partir de la Phase B, conformément à la doctrine PiaXel Nexus sur les datasets.

BYOK *(Bring Your Own Key, Apportez votre propre clé)*. Architecture dans laquelle le client conserve le contrôle de ses propres clés cryptographiques et de ses jetons d'accès aux fournisseurs LLM. Garantit que le fournisseur de la plateforme ne peut pas lire les données client et ne peut pas réutiliser les requêtes pour entraîner ses modèles.

C2PA *(Coalition for Content Provenance and Authenticity)*. Standard ouvert de marquage cryptographique de la provenance des contenus (images, vidéos, audio). Solution recommandée par EUDAI pour satisfaire l'obligation AI Act Art. 50.2 sur le marquage des contenus IA.

CCT *(Clauses Contractuelles Types)*. Clauses standardisées validées par décision (UE) 2021/914 de la Commission européenne pour encadrer les transferts de données personnelles vers un pays sans décision d'adéquation. Obligatoires dès qu'un sous-traitant est établi hors UE/EEE.

Chiffrement par enveloppe *(envelope encryption)*. Technique cryptographique dans laquelle chaque donnée est chiffrée avec une clé propre (DEK), elle-même chiffrée par une clé maître (KEK). Permet de réduire la surface d'exposition de la KEK et de faire tourner les DEK indépendamment. Standard chez les services de stockage souverains EU.

CJUE. Cour de Justice de l'Union Européenne. Sa jurisprudence est obligatoire pour tous les États membres et les autorités de protection des données. Arrêt clé pour les transferts internationaux : *Schrems II* (C-311/18, 2020).

CNIL. Commission Nationale de l'Informatique et des Libertés. Autorité française de protection des données. Source autoritative pour la France via ses référentiels (AIPD, cookies, IA), ses sanctions publiques et ses recommandations sectorielles.

Deepfake. Contenu (image, vidéo, audio) artificiellement généré ou manipulé qui ressemble de manière trompeuse à une personne, un objet, un lieu ou un événement réel. Soumis à obligation de divulgation explicite par AI Act Art. 50.4.

DPA *(Data Processing Agreement, contrat de sous-traitance)*. Contrat entre un responsable de traitement et un sous-traitant exigé par RGPD Art. 28.3. Doit contenir les huit clauses obligatoires (objet, durée, finalités, instructions, confidentialité, sécurité, sous-traitance ultérieure, droits des personnes).

DPO *(Data Protection Officer, délégué à la protection des données)*. Personne physique chargée de veiller à la conformité RGPD d'une organisation. Obligatoire dans certains cas (RGPD Art. 37). Peut être interne ou délégué (mutualisé entre plusieurs organisations).

DSA *(Digital Services Act)*. Règlement (UE) 2022/2065 sur les services numériques. Hors périmètre central EUDAI v1, traité en surface, version sectorielle prévue v2.

EDPB *(European Data Protection Board)*. Comité européen de la protection des données. Assemblée des autorités nationales (CNIL et équivalents). Publie les *Guidelines* et *Opinions* qui font autorité de fait sur l'interprétation du RGPD.

Ethics by Design* / *Ethics by Evolution. Approches éthiques appliquées à l'IA. *Ethics by Design* exige que les exigences éthiques soient intégrées dès la conception. *Ethics by Evolution*, prolongée par les travaux de Béranger et Ait Thami (Polytechnique Insights, avril 2026), exige en outre que ces exigences soient adaptées tout au long du cycle de vie. EUDAI s'inscrit dans la seconde approche.

EU Inc.. Statut d'entreprise européenne unifiée en cours d'élaboration au niveau UE, qui vise à offrir un cadre juridique d'incorporation transfrontalier au sein de l'Union. PiaXel Nexus prévoit une transformation de SASU vers EU Inc. à 12-24 mois selon avancement de la législation.

EUDAI. Cadre Européen de Doctrine IA (*European Union Doctrine on AI*). Cf. § *Que signifie EUDAI ?* en début de Préambule.

EuTrustedIA.eu. Premier projet monétisé de PiaXel Nexus. Comporte deux briques : l'**Annuaire EuTrustedIA** (annuaire d'experts conformité) et **POSITRONIA** (plateforme de scan et d'auto-évaluation).

Fine-tuning. Technique consistant à spécialiser un modèle de fondation pré-entraîné en l'entraînant complémentairement sur un jeu de données ciblé. Peut être léger (LoRA, instruct-tuning) ou complet. Engage des obligations AI Act Art. 10 si conduit sur données personnelles à grande échelle.

GPAI *(General-Purpose AI)*. Modèle d'IA à usage général. Catégorie introduite par l'AI Act (Art. 51-55) qui crée des obligations spécifiques pour les fournisseurs et les déployeurs de modèles de fondation à grande échelle.

HDS *(Hébergement de Données de Santé)*. Certification française obligatoire pour héberger des données de santé. Hors périmètre central EUDAI v1, traité en surface, version sectorielle santé prévue Phase B+.

LEDGER. Registre append-only horodaté et chaîné par signature SHA-256, dans lequel PiaXel Nexus inscrit chaque décision technique structurelle (intégration d'un OSS tiers, choix d'architecture, modification de scope, incident sécurité). Toute modification rétroactive est détectable. Public, accessible à `eutrustedia.eu/audit/ledger`.

LLM *(Large Language Model)*. Modèle de langage à grande échelle. Catégorie technique qui couvre les modèles de fondation utilisés pour le traitement et la génération de texte (Mistral, Llama, GPT, Claude, etc.).

MCP *(Model Context Protocol)*. Protocole ouvert publié par Anthropic en 2024, qui permet à un assistant IA d'interagir avec des serveurs d'outils ou de données via une interface standardisée. EUDAI l'utilise comme couche de contrôle d'infrastructure pour exposer POSITRONIA et l'Annuaire dans l'IDE du client sans casser sa souveraineté.

Memorization attack *(et membership inference attack)*. Tests adversariaux visant à vérifier qu'un modèle ne mémorise pas verbatim des données d'entraînement (memorization) ou qu'on ne peut pas déterminer si une personne précise figurait dans l'ensemble d'entraînement (membership inference). Recommandés par EDPB Opinion 28/2024 pour valider une anonymisation.

NIS 2. Directive (UE) 2022/2555 sur la cybersécurité des réseaux et systèmes d'information. Hors périmètre central EUDAI v1, traité en surface.

OEM *(Original Equipment Manufacturer)*. Modèle commercial dans lequel une brique technique est intégrée par un acteur tiers et redistribuée sous sa propre marque. EUDAI privilégie l'OEM minimal (couches techniques verrouillables et auditables).

OSS *(Open-Source Software)*. Logiciel publié sous licence open source (Apache 2.0, MIT, BSD, EUPL, etc.). Critère prioritaire dans le Stack Recommender quand une alternative équivalente existe.

PiaXel Nexus. Dénomination juridique officielle de l'incubateur de projets éditeur du présent Framework (SASU française en cours de constitution), avec évolution prévue en EU Inc. à 12-24 mois selon l'avancement de la législation européenne sur ce statut. EuTrustedIA.eu est le premier projet monétisé porté par PiaXel Nexus. *PiaXel* (sans le suffixe Nexus) reste utilisé en interne dans les noms de fichiers techniques (par exemple `DOCTRINE_DATASETS_PIAXEL.md`), les codes de chantiers ouverts (par exemple CO-031) et les noms de repositories Git, pour préserver la stabilité des références techniques.

Prompt injection. Attaque consistant à insérer des instructions malveillantes dans un prompt utilisateur ou dans des données traitées par un LLM, dans le but de détourner son comportement ou d'exfiltrer des informations. Première barrière : un guard d'entrée (NeMo Guardrails, Mistral Moderation, Garak en testing).

RGPD. Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Applicable depuis le 25 mai 2018. Texte fondateur du droit européen des données personnelles.

RSSI *(Responsable de la Sécurité des Systèmes d'Information)*. Profil pluridisciplinaire combinant cybersécurité, conformité et gestion des risques. Sollicité dans le cadre EUDAI pour les audits cybersec des systèmes haut risque (AI Act Art. 15).

Rubber stamping. Pratique consistant à valider mécaniquement une décision automatisée par un humain qui n'examine pas réellement le dossier (signature de pure forme). Non conforme aux exigences RGPD Art. 22 et AI Act Art. 14 sur la surveillance humaine effective.

SaaS *(Software as a Service)*. Logiciel délivré sous forme de service en ligne, sans installation locale. Modèle commercial dominant pour les outils B2B contemporains.

SAST / SCA. *Static Application Security Testing* (analyse statique de code source pour détecter les vulnérabilités, ex. Semgrep) et *Software Composition Analysis* (analyse des dépendances tierces et des CVE associées, ex. Trivy, OSV). Briques techniques utilisées par POSITRONIA.

SASU. Société par Actions Simplifiée Unipersonnelle. Forme juridique française à associé unique, choisie par PiaXel Nexus pour son démarrage avant transformation en EU Inc.

Schrems II. Arrêt CJUE C-311/18 du 16 juillet 2020. Invalide le *Privacy Shield* entre l'UE et les États-Unis et impose, pour tout transfert hors UE, une analyse du risque local et la mise en place de mesures supplémentaires (TIA + clauses contractuelles types + chiffrement, pseudonymisation).

Self-host / **self-hostable**. Capacité d'un logiciel à être installé et exécuté sur l'infrastructure du client, sans dépendance forcée à un cloud externe. Critère prioritaire dans le Stack Recommender (principe 7, single-binary).

POSITRONIA. Plateforme technique de PiaXel Nexus exposée aux abonnés payants d'EuTrustedIA.eu. Combine SAST + SCA + scan d'agents IA + livrables Art. 50 + AIPD pré-remplie.

POSITRONIA Blueprint. Diagnostic Pré-build du mode *Lancement Conforme*. Audit du cahier des charges client (PRD, architecture, schémas de flux), pas du code. Produit un score de risque pilier par pilier et trois recommandations de voie d'exécution (DIY = autonomie SOLO 29€, AUTONOMIE SOUVERAINE = GENESIS 69€ avec modules formation inclus, ACCOMPAGNÉ = AVANTAGES 99€ avec Club Deal partenaires + RDV remisés experts Annuaire). Version Lite incluse dans le ticket LANCE-TOI 49 €, version complète à partir du Plan GENESIS.

Stack Recommender. Recommandeur Souverain EU. Outil EUDAI qui produit, pour chaque projet IA, une recommandation infrastructure plus IA 100 % EU souveraine, avec 3 alternatives par couche minimum, refresh trimestriel et tagging géopolitique explicite.

TIA *(Transfer Impact Assessment)*. Analyse documentée du risque local en cas de transfert de données personnelles vers un pays sans décision d'adéquation européenne. Obligatoire post-*Schrems II*. Évalue notamment la législation du pays de destination, les pouvoirs d'accès des autorités locales et l'effectivité des mesures supplémentaires.

Mode Audit & Conformité *(post-build)* / **Mode Lancement Conforme** *(pre-build)*. Les deux moments de vie d'un projet IA adressés par EUDAI, traités par un seul abonnement EuTrustedIA. *Audit & Conformité* pour les produits déjà construits qui doivent documenter leur conformité. *Lancement Conforme* pour les projets en phase de structuration qui veulent partir conformes dès la première ligne de code. Voir aussi les trois voies d'exécution post-POSITRONIA Blueprint (distinctes des modes de positionnement) : **Voie A DIY** (autonomie technique, plan SOLO 29€/mois), **Voie B AUTONOMIE SOUVERAINE** (modules formation conformité IA inclus, plan GENESIS 69€/mois), **Voie C ACCOMPAGNÉ** (Club Deal partenaires souverains EU + RDV remisés experts Annuaire, plan AVANTAGES 99€/mois).

Watermarking. Technique de marquage discret d'un contenu (texte, image, audio) permettant d'identifier son origine et ses propriétés (généré par IA, source, licence). Recommandé par EUDAI pour satisfaire l'obligation AI Act Art. 50.2 ; standard ouvert privilégié : C2PA.

8.7 Mentions

Champ	Valeur
Titre	EUDAI Framework v1.1, Cadre Européen de Doctrine IA
Sous-titre	Le référentiel de conformité opérationnelle pour solopreneurs IA
Éditeur	**PiaXel Nexus** (SASU française en cours de constitution), projet **EuTrustedIA.eu**. Évolution prévue en **EU Inc.** à 12-24 mois.
Édition	v1.1, 2026-05-05 (refonte architecture commerciale unifiée)
Licence	Creative Commons Attribution, Pas d'Utilisation Commerciale 4.0 International (CC BY-NC 4.0)
Langue	Français (version anglophone prévue Phase C, post-validation marché FR)
Identifiant Git	`eutrustedia/eudai-framework` (à publier au go-live Phase B)
Aide rédactionnelle	Assistant IA Claude (Anthropic Opus 4.7), usage marqué au sens AI Act Art. 50.2
Site	`eutrustedia.eu`
Contact	`contact@eutrustedia.eu`

8.7.1 Versions et évolutions

— **v1.0**, 2026-05-05, version initiale (intégration dual-positioning Voies A + B, 5 piliers, checklist 25 points, Stack Recommender, tunnel à 3 voies, définition acronyme EUDAI, distinction des trois niveaux d'usage IA, lexique). Remplacée par v1.1 le jour même suite à refonte commerciale

— **v1.1**, 2026-05-05, **refonte de l'architecture commerciale** : fusion des anciennes Voie A *Audit & Conformité* et Voie B *Lancement Conforme* en un **seul abonnement** couvrant les deux modes selon le stade du projet. Suppression du plan FREE 0 € (remplacé par le Lead Magnet du présent Livre Blanc gratuit). Nouvelle grille tarifaire : LANCE-TOI 49 € unique, SOLO 29 €/mois, GENESIS 69 €/mois, AVANTAGES 99 €/mois (recommandé), ENTREPRISE sur devis. Ajout de la variante Mode Agence ENTREPRISE (Phase B) pour DPO délégués, avocats tech et cabinets de conseil. Ajout de l'add-on projet supplémentaire 19 €/mois mensuel découplé. Annuel optionnel à -10 % (au lieu de -17 %). Ajout du Club Deal partenaires souverains EU avec manifesto préférence française et européenne et boucle vertueuse client devenu partenaire. Ajout du programme d'affiliation infopreneurs custom Next.js + Mollie (activation Phase B) avec dispositif de sécurité

multi-couches. Refonte des sections du Préambule, du § 3.4 Tunnel à 3 voies, du § 4.2 Plans tarifaires, des personas et du lexique

- **v1.1.1**, 2026-05-06, **patch stack tech foundation Phase A** (§ 2.1.3 actualisé) : décisions actées Vercel+DPA EU Frankfurt + Neon EU + Infisical Cloud EU + Mollie ▯▯ + Brevo ▯▯ + kMeet Infomaniak ▯▯ ; assomption publique du compromis transitoire « majoritairement européen » Phase A avec migration Phase C 100 % souveraine vers Infomaniak Public Cloud / Postgres / Infisical self-host. Source : `docs/build-journal/2026-05-06__stack-tech-foundation.md`.
- **v1.3**, 2026-05-26, **ajout § 1.6 LLM Fallacy / Capability Divergence** : fondation cognitive de la posture EUDAI (réf. académique arXiv :2604.14807, Kim/Yu/Yi, ddai Inc., 2026). Explique mécaniquement pourquoi le disclaimer de non-certification est un fait cognitif documenté, pas une précaution légale. Justification cognitive de l'Annuaire EuTrustedIA et du Plan AVANTAGES 99 €/mois. Tableau comparatif concurrents DIY. Marquage BROUILLON systématique sur livrables POSITRONIA-CORE. Bump date 2026-05-13 → 2026-05-26 + ajout métadonnées version/last_updated/changelog frontmatter
- **v1.4** *(prévu Q3 2026)*, retours premiers clients Phase A + 5-10 ambassadeurs Annuaire signés + premiers partenaires Club Deal signés + activation programme d'affiliation et Mode Agence en Phase B
- **v2.0** *(prévu Q1 2027)*, sections sectorielles approfondies (santé, fintech, edtech, public-sector) + premiers retours bench `sentinel-bench-v0.2-stratified-125`

8.7.2 Remerciements

À tous les solopreneurs IA EU qui construisent dans la lumière au lieu d'attendre que les Big 4 daignent les regarder. À la CNIL pour la rigueur de ses publications. À l'EDPB pour ses Opinions précisantes. À la communauté open source européenne (Mistral, Qdrant, Hugging Face FR, Coqui, Kyutai, et tous les autres) qui prouve chaque jour qu'une stack EU souveraine est possible. Et à l'équipe PiaXel Nexus, qui s'engage à appliquer ses propres règles avant de demander aux autres de les appliquer.

« Si on vend de la conformité, on doit être exemplaire. »

Fin du document.