LinkTec LABS

NOTE DE RECHERCHE N°03 · IA & DONNÉES APPLIQUÉES

L'IA souveraine, **par conception**

Concevoir pour le RGPD et l'EU AI Act dès l'architecture.

RÉSUMÉ

La souveraineté et la conformité ne sont pas des cases à cocher au moment de l'achat, une fois le système construit ; ce sont des propriétés d'architecture qui doivent être conçues dès la première ligne. À mesure que les obligations de transparence de l'EU AI Act entrent en vigueur et que les droits des personnes au titre du RGPD se heurtent à la façon dont les modèles stockent réellement l'information, la question devient concrète pour toute organisation qui déploie de l'IA sur de vraies données personnelles : où vivent les données, qui peut en exiger la communication, et la fiche d'un client peut-elle réellement être effacée sur demande ? Cette note sépare la *résidence* de la *souveraineté*, cartographie précisément la réalité réglementaire de 2026, et défend un seul argument d'architecture aux conséquences tranchantes, que la *récupération*, et non l'entraînement, est la primitive qui rend les droits des personnes techniquement réels. Nous terminons par l'architecture de référence souveraine et auditable que déploie LinkTec Labs, bouclant l'arc ouvert par les Notes N°01 (contexte) et N°02 (mémoire).

01, DU « OÙ » AU « QUI CONTRÔLE »

La souveraineté est une architecture, pas une case à cocher

Pendant une décennie, « nos données sont-elles en Europe ? » a été considérée comme une question réglée dès qu'une région cloud affichait *eu-west*. Cette époque est révolue. La question qui engage en 2026 n'est plus *où* se trouvent les données mais *qui peut en exiger la communication* et *ce qu'on peut réellement en faire*, et aucune des deux ne se règle par un sélecteur de région. Près de la moitié des entreprises ouest-européennes réévaluent aujourd'hui activement leur dépendance aux fournisseurs cloud non européens, et l'écart qu'elles ont découvert est celui qui sépare la résidence de la souveraineté.

La distinction n'a rien d'académique. Une région d'un hyperscaler à Francfort satisfait la *résidence des données*, le stockage et le traitement ont lieu sur le sol européen. Elle n'apporte pas, à elle seule, la *souveraineté* : un fournisseur dont le siège est aux États-Unis reste soumis au CLOUD Act américain, qui peut contraindre à la divulgation des données indépendamment du lieu où elles résident physiquement. La souveraineté pose une question plus dure, celle de savoir si le fournisseur, et l'ordre juridique auquel il répond, peut être atteint par une juridiction étrangère, tout court. Pour un hôpital, une banque ou un fournisseur de défense, cette différence est celle qui sépare un système conforme d'un système illicite.

La thèse de cette note en découle directement, et c'est le fil qui relie toute la série LinkTec Labs : *la conformité et la souveraineté ne se rajoutent pas après coup.* On ne peut pas greffer l'effacement sur un modèle qui a mémorisé des données personnelles, ni la résidence sur un pipeline qui a déjà expédié un prompt à l'étranger. Ce sont des propriétés de l'architecture, ou bien elles sont absentes. La bonne nouvelle, et la substance de cette note, c'est que l'architecture qui les apporte est désormais bien comprise, et qu'elle est constructible.

TERMES CLÉS

Un vocabulaire commun pour la suite. Les spécialistes peuvent passer.

Résidence des données	Garantie que les données sont stockées et traitées dans un territoire donné (l'UE, p. ex.).
Souveraineté des données	La résidence *plus* l'immunité face à toute juridiction étrangère sur les données et leur opérateur.
Cloud souverain	Infrastructure dont la technologie, les opérations et le contrôle relèvent pleinement du droit de l'UE ; hors d'atteinte du CLOUD Act.
Informatique confidentielle	Environnements d'exécution de confiance (TEE) matériels qui gardent les données chiffrées même pendant leur usage.
RAG souverain	

	RAG exécuté sur infrastructure privée/souveraine, avec contrôle d'accès et audit.
Par conception (Art. 25)	Obligation RGPD d'intégrer la protection des données dès la conception et par défaut.
AIPD (Art. 35)	Analyse d'impact relative à la protection des données, requise pour les traitements à risque élevé.
Droit à l'effacement (Art. 17)	Droit d'une personne à faire supprimer ses données personnelles (« droit à l'oubli »).
Désapprentissage machine	Techniques visant à retirer l'influence de données précises des poids d'un modèle, encore approximatives.
GPAI	Modèle d'IA à usage général, encadré par un chapitre dédié et un Code de bonnes pratiques sous l'AI Act.
Article 50	Les obligations horizontales de *transparence* de l'AI Act (signaler l'interaction IA, le contenu de synthèse).
Trace d'audit	Enregistrement exportable reliant chaque sortie à ses entrées, sources et décisions, pour la responsabilité.

02, LA RÉALITÉ RÉGLEMENTAIRE

Ce qui est réellement dû, et quand

Le souverain-par-conception commence par savoir précisément ce que la loi exige, et le tableau 2026 récompense la précision, car les gros titres ont induit en erreur. Deux régimes s'appliquent à la fois : l'EU AI Act gouverne le *système* ; le RGPD gouverne les *données personnelles* qu'il contient.

L'EU AI Act, après le Digital Omnibus

Le 7 mai 2026, le Conseil et le Parlement sont parvenus à un accord politique provisoire sur le « Digital Omnibus on AI », confirmé en plénière du Parlement le 16 juin 2026, étant entendu, surtout, qu'il *n'a pas encore force de loi*, dans l'attente de l'adoption par le Conseil et de la publication au Journal officiel[2]. L'Omnibus a reporté les obligations les plus lourdes : les systèmes à haut risque de l'Annexe III s'appliquent désormais à compter du **2 décembre 2027**, et l'IA à haut risque intégrée à des produits réglementés à compter du 2 août 2028[2]. Mais l'obligation la plus pertinente pour quiconque expédie une fonctionnalité générative n'a *pas* été reportée : les devoirs de **transparence** de l'Article 50 entrent en vigueur le **2 août 2026**, le marquage (watermarking) et la divulgation des contenus de synthèse étant requis pour le 2 décembre 2026[1][2]. Pour les modèles à usage général, le Code de bonnes pratiques GPAI, publié par l'AI Office le 10 juillet 2025 et signé par une vingtaine de fournisseurs, dont les grands labos et le français Mistral AI, demeure la voie de conformité principale[3].

LA DATE QUI COMPTE

2 août 2026, la transparence de l'Article 50 est en vigueur. Signaler l'interaction avec une IA et marquer les contenus de synthèse est un devoir horizontal qui s'applique quel que soit le niveau de risque et n'a *pas* été reporté par l'Omnibus. Traitez-le comme l'échéance contraignante de court terme ; traitez les dates « haut risque » de 2027 comme l'horizon de planification[1][2].

Le RGPD, et ce que le CEPD attend désormais des modèles

Le RGPD est le régime le plus ancien et, pour les données personnelles, le plus exigeant : base légale et transparence (Art. 5-6), sécurité (Art. 32), protection des données dès la conception et par défaut (Art. 25), et une analyse d'impact (AIPD) pour les traitements à risque élevé (Art. 35)[5]. En décembre 2024, le Comité européen de la protection des données (CEPD) a rendu l'Avis 28/2024, le signal le plus clair à ce jour sur l'IA et les données personnelles[4]. Trois conclusions importent ici : un modèle n'est « anonyme » que s'il est *très improbable* à la fois d'identifier des individus et d'en extraire les données par requête, apprécié au cas par cas, la charge pesant sur le responsable de traitement ; l'intérêt légitime ne peut fonder un traitement d'IA qu'au terme d'un test strict en trois étapes ; et, décisif pour l'architecture, le CEPD reconnaît qu'honorer le droit à l'effacement contre un *modèle entraîné* est « techniquement complexe », et pointe vers des mesures d'atténuation, dont des mécanismes de suppression de données et des techniques de désapprentissage[4]. Retenez ce dernier point ; la Section 05 en fait un principe de conception.

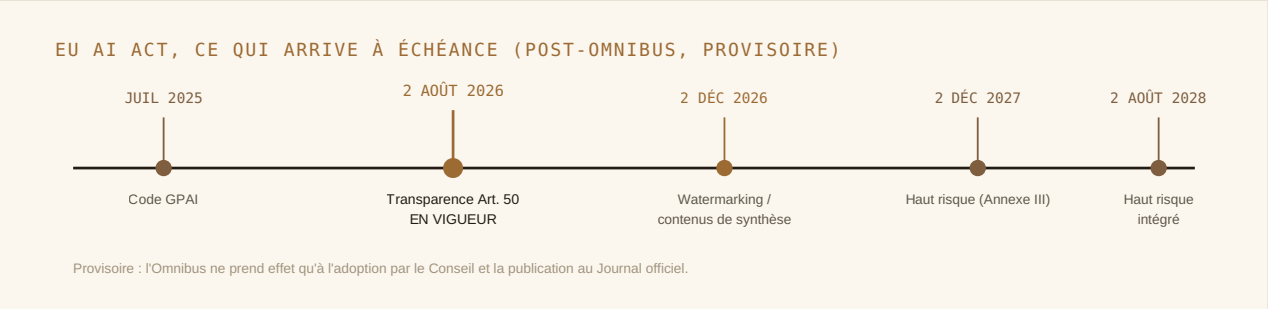

Fig. 1. L'horizon de conformité de l'EU AI Act après le Digital Omnibus. La transparence de l'Article 50 (2 août 2026) est le devoir contraignant de court terme ; les obligations « haut risque » glissent à 2027-2028. Dates provisoires, dans l'attente de publication[1][2].

03, RÉSIDENCE N'EST PAS SOUVERAINETÉ

Trois barreaux, un seul CLOUD Act

Entre « nos données sont en UE » et « nos données sont hors d'atteinte étrangère » se trouvent trois barreaux distincts, et les confondre est l'erreur d'achat la plus courante de 2026. Le cadre de la Commission européenne elle-même rend désormais l'échelle explicite. Dans son marché de cloud souverain de 180 millions d'euros, attribué à quatre consortiums européens, bâtis autour d'OVHcloud, STACKIT, Scaleway et, avec Mistral, le groupe Proximus, trois ont été certifiés **SEAL-3** (une pile entièrement européenne, du matériel au logiciel, du capital aux opérations, sans interférence non-UE) et un **SEAL-2** (technologie non européenne admise, à condition que les opérations, le contrôle et le capital restent entièrement européens)[6]. Le futur schéma de certification EUCS devrait encoder des

paliers de souveraineté équivalents dans une certification de cybersécurité formelle, aux côtés des critères de labellisation Gaia-X[7][8].

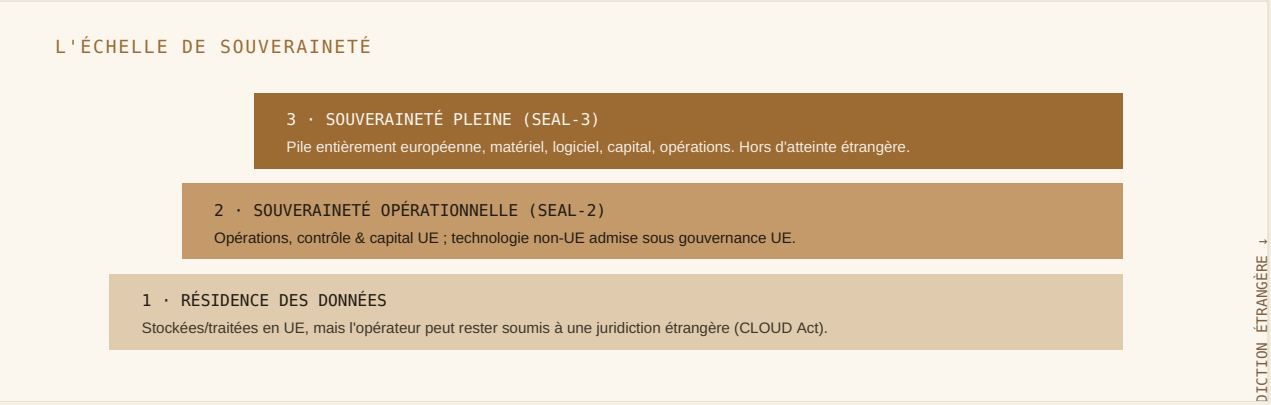

Fig. 2. La résidence est le premier barreau, pas la destination. La souveraineté s'élève de l'opérationnel (SEAL-2) au plein (SEAL-3) ; le marché à 180 M€ de l'UE certifie de vrais fournisseurs à chaque niveau[6].

La conséquence pratique est que les modèles à poids ouverts, conçus en Europe, rendent désormais la souveraineté pleine *atteignable* plutôt qu'aspirationnelle. Les modèles de Mistral, hébergeables chez OVHcloud, Scaleway et d'autres clouds souverains, offrent aux institutions européennes régulées, banques, assureurs, hôpitaux, organismes publics, une voie crédible vers une IA performante qui ne quitte jamais la juridiction de l'UE. La souveraineté n'est plus un arbitrage contre la capacité ; c'est un choix de déploiement.

04, LE SUBSTRAT TECHNIQUE

Où vivent les données, qui peut les atteindre, comment elles sont protégées en usage

La souveraineté se résout en trois garanties techniques, et une architecture sérieuse les fournit toutes. **Localisation :** données et inférence tournent dans une région UE ou on-premise. **Juridiction :** l'opérateur est hors de contrainte étrangère, la propriété SEAL-3, pas un simple label de région. **Protection en usage :** c'est celle qu'on oublie le plus. Les données au repos et en transit sont couramment chiffrées ; les données *en usage*, pendant l'inférence, ont historiquement été exposées en mémoire. L'*informatique confidentielle* comble cette faille : des environnements d'exécution de confiance matériels, désormais disponibles sur GPU de datacenter, gardent données et poids du modèle chiffrés même pendant leur traitement, de sorte que ni l'opérateur cloud ni un hôte compromis ne peuvent les lire[9].

Ces garanties n'exigent pas d'envoyer chaque charge de travail dans une enclave souveraine. Le motif mûr est une architecture *routée* : un classifieur répartit le trafic de sorte que tout ce qui touche à des données personnelles ou régulées soit traité par un modèle privé sur infrastructure souveraine et confidentielle, tandis que les charges non sensibles peuvent recourir à un modèle frontière global pour la capacité brute. La souveraineté devient une propriété appliquée là où la loi l'exige, et non une taxe générale sur la performance.

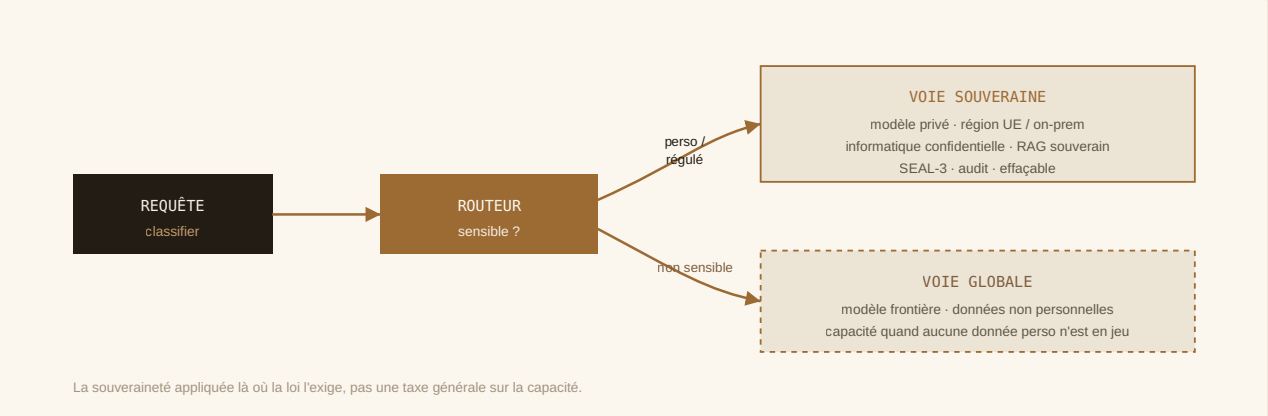

Fig. 3. Souveraineté routée. Un classifieur envoie données personnelles et régulées sur une voie souveraine (modèle privé, informatique confidentielle, RAG souverain) et réserve les modèles frontière globaux au travail non sensible[9].

05, POURQUOI LA RÉCUPÉRATION EST LA PRIMITIVE DE SOUVERAINETÉ

L'argument qui change la construction

Voici l'intuition d'architecture qui transforme la conformité d'un fardeau en choix de conception, et c'est le fil conducteur de toute cette série. Le RGPD accorde à une personne le droit de faire effacer ses données personnelles. Contre un modèle qui a *appris* ces données dans ses poids, ce droit est, selon les mots mêmes du CEPD, « techniquement complexe » : l'information est diffusée à travers des milliards de paramètres, et le désapprentissage machine reste approximatif, invérifiable, et un problème de recherche ouvert[4]. On ne peut pas prouver qu'on a oublié quelqu'un sur qui on s'est entraîné.

Mais les données personnelles tenues dans un *store de récupération*, et dans la mémoire typée des agents de la Note N°02, sont d'une autre nature. Elles sont adressables. Elles peuvent être localisées par personne, corrigées quand elles sont fausses, et supprimées sur demande, avec la preuve que ce fut fait. Il en va de même du contexte de synthèse qui entre dans un prompt à l'inférence et est jeté ensuite. *Le droit à l'effacement est intraitable dans les poids et trivial dans un store.* La conclusion est une instruction d'ingénierie à force juridique :

> Ne pas entraîner sur des données personnelles qu'on pourrait devoir oublier. Les récupérer. Le RAG souverain transforme un problème de machine learning non résolu, le désapprentissage, en un problème d'ingénierie des données résolu : supprimer l'enregistrement.

Cela recadre toute la série. La Note N°01 soutenait que la récupération maintient le *ratio signal/token* élevé ; la Note N°02 soutenait qu'une mémoire typée et gouvernée rend la continuité *abordable* ; cette note ajoute la troisième raison, décisive, que garder les données personnelles *hors des poids et dans un store gouverné* est ce qui rend les droits de la personne, et donc le déploiement licite, techniquement réalisables tout court. Architecture de contexte, mémoire des agents et souveraineté ne sont pas trois

sujets. Ce sont une seule architecture, vue de trois côtés. La récupération est ce qui la rend conforme par construction.

06, LE RAG SOUVERAIN, CONCRÈTEMENT

Du principe au contrôle

Le « RAG souverain » n'est pas un produit ; c'est un ensemble de contrôles, chacun reliant un devoir juridique à un mécanisme concret. La récupération doit être **contrôlée en accès** : le store applique les permissions par document de sorte que le modèle ne fasse remonter que ce que l'utilisateur demandeur est autorisé à voir, la récupération hérite du modèle d'autorisation de l'organisation au lieu de le contourner. Les données personnelles doivent être **minimisées et protégées** : détection et caviardage des PII à l'ingestion et en sortie, et un contexte top-k qui ne porte que ce dont la tâche a besoin. Et chaque interaction doit être **auditable** : une trace exportable du prompt, à travers les sources exactes récupérées, jusqu'à la sortie, la preuve qu'on peut montrer à un auditeur ou à une personne concernée.

DEVOIR JURIDIQUE	CONTRÔLE D'ARCHITECTURE
Protection dès la conception (Art. 25)	Récupération contrôlée en accès, caviardage PII, hébergement souverain par défaut [5]
Minimisation des données (Art. 5)	Récupération top-k et budget de contexte, pas d'historique en masse dans le prompt
Droit à l'effacement (Art. 17)	Supprimer du store / de la mémoire ; garder les données perso hors des poids [4]
Sécurité du traitement (Art. 32)	Informatique confidentielle, chiffrement en usage ; chiffrement au repos & en transit [9]
Transparence (AI Act Art. 50)	Signalement de l'interaction IA ; marquage des contenus de synthèse dès le 2 août 2026 [1]
Responsabilité (Art. 5(2))	Trace d'audit exportable, attribuée à la source, de la requête à la réponse
Analyse d'impact (Art. 35)	AIPD câblée dans le processus de déploiement, pas ajoutée après

07, UNE ARCHITECTURE DE RÉFÉRENCE

Souveraine par conception, telle que LinkTec Labs la construit

Les contrôles se composent en une seule pile, avec un plan de gouvernance explicite qui court en dessous. C'est l'architecture qui unifie la série : la couche de contexte de la Note N°01 et la couche de

mémoire de la Note N°02, hébergées et gouvernées de sorte que souveraineté et conformité soient structurelles, et non aspirationnelles.

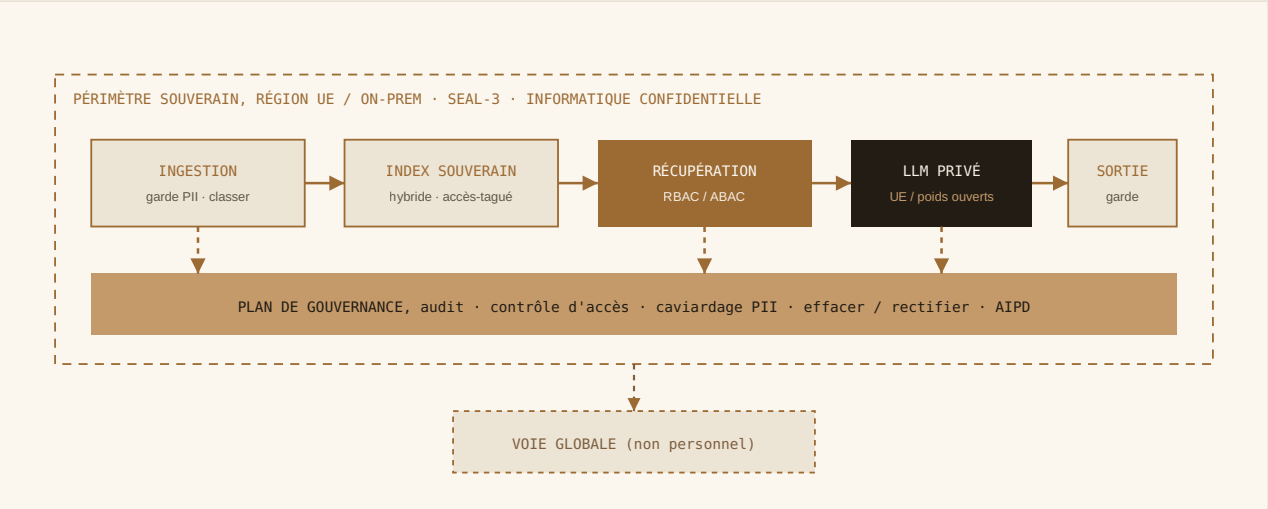

Fig. 4. Architecture de référence souveraine LinkTec Labs. Tout ce qui touche aux données personnelles reste dans un périmètre souverain (UE/on-prem, SEAL-3, informatique confidentielle) ; un plan de gouvernance rend chaque enregistrement auditable, rectifiable et effaçable. Le travail non personnel peut sortir vers une voie globale.

Quatre principes la gouvernent. **Le périmètre est explicite**, données personnelles et régulées ne quittent jamais un périmètre souverain et confidentiel, et ce périmètre est un artefact de conception, pas un espoir. **La récupération hérite de l'autorisation**, le store impose qui peut voir quoi, de sorte que le modèle ne puisse pas blanchir un accès. **Les données personnelles restent hors des poids**, elles vivent dans un store gouverné où l'effacement est réel, jamais entraînées là où il ne l'est pas. Et **la gouvernance est un plan, pas un correctif**, audit, rectification, effacement et AIPD courent sous chaque composant, produisant la preuve qui transforme « nous sommes conformes » en quelque chose de démontrable. Les trois premiers gagnent la confiance ; le quatrième la prouve.

08, PLAYBOOK DU PRATICIEN

Quoi faire dès lundi

- → **Séparer résidence et souveraineté.** Une région UE n'est pas une immunité face au CLOUD Act, vérifiez la juridiction de l'opérateur (SEAL-2 vs SEAL-3)[6].
- → **Inscrire le 2 août 2026 à l'agenda.** La transparence de l'Article 50 est le devoir contraignant de court terme ; les dates « haut risque » sont 2027-2028[1][2].
- → **Garder les données personnelles hors des poids.** Récupérez-les ; n'entraînez pas sur ce qu'il faudra peut-être effacer[4].
- → **Rendre la récupération contrôlée en accès.** Le store doit imposer les permissions par document, pas le prompt[5].

- → **Protéger les PII en entrée et en sortie.** Détecter et caviarder à l'ingestion et en sortie ; minimiser le contexte au top-k.
- → **Protéger les données en usage.** Informatique confidentielle / TEE, pas seulement chiffrement au repos et en transit[9].
- → **Router selon la sensibilité.** Voie souveraine pour les données personnelles ; capacité globale seulement quand aucune PII n'est en jeu.
- → **Construire la trace d'audit d'abord.** Prompt → sources → sortie, exportable, c'est votre preuve d'AIPD et votre preuve d'effacement.

Une conformité qu'on peut démontrer est une architecture. Une souveraineté qu'on peut prouver est un périmètre. Ni l'une ni l'autre ne s'ajoute après coup, et c'est précisément pourquoi elles sont un avantage.

LinkTec Labs conçoit des systèmes d'IA souverains et auditables pour les organisations qui ne peuvent pas expédier leurs données à l'étranger, bâtis sur l'architecture de contexte (N°01), la mémoire gouvernée (N°02) et les principes de souveraineté-par-conception ci-dessus. Cette note clôt l'arc fondateur de notre série de recherche 2026. **linktec.fr / labs**

RÉFÉRENCES

Sources réglementaires, techniques & primaires

[1] Commission européenne. **Cadre réglementaire sur l'intelligence artificielle (EU AI Act).** Shaping Europe's Digital Future, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

[2] Gibson Dunn. **EU AI Act Omnibus Agreement, Postponed High-Risk Deadlines and Other Key Changes.** 2026 (analyse du Digital Omnibus on AI, accord provisoire du 7 mai 2026), https://www.gibsondunn.com/eu-ai-act-omnibus-agreement-postponed-high-risk-deadlines-and-other-key-changes/

[3] AI Office / Commission européenne. **General-Purpose AI Code of Practice** (publié le 10 juillet 2025), https://digital-strategy.ec.europa.eu/en/policies/ai-code-practice

[4] Comité européen de la protection des données (CEPD/EDPB). **Avis 28/2024 sur certains aspects de protection des données liés au traitement de données personnelles dans le contexte des modèles d'IA.** 17 déc. 2024, https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf

[5] Union européenne. **Règlement (UE) 2016/679, Règlement général sur la protection des données (RGPD)** (Art. 5, 17, 25, 32, 35), https://eur-lex.europa.eu/eli/reg/2016/679/oj

[6] Commission européenne. **Commission advances cloud sovereignty through strategic procurement** (marché-cadre cloud souverain de 180 M€ ; SEAL-2 / SEAL-3). 17 avr. 2026, https://commission.europa.eu/news-and-media/news/commission-advances-cloud-sovereignty-through-strategic-procurement-2026-04-17_en

[7] ENISA. **European Cybersecurity Certification Scheme for Cloud Services (EUCS).**, https://www.enisa.europa.eu/topics/cloud-and-big-data/european-cloud-services-scheme

[8] Gaia-X European Association for Data and Cloud. **Cadre, labels & critères.**, https://gaia-x.eu/

[9] NVIDIA. **Confidential Computing** (environnements d'exécution de confiance pour GPU de datacenter ; chiffrement en usage)., https://www.nvidia.com/en-us/data-center/solutions/confidential-computing/

[10] Anthropic. **Effective Context Engineering for AI Agents** (primitives de gouvernance, citations & auditabilité). 2025, https://www.anthropic.com/engineering/effective-context-engineering-for-ai-agents

[11] Lewis et al. **Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks.** NeurIPS 2020. arXiv: 2005.11401, https://arxiv.org/abs/2005.11401