

KALICORP

Le Sanctuaire — Infrastructure IA Souveraine

L'IA SOUVERAINE

Pourquoi, Comment, et Ce que Cela Change Concrètement

Panorama global : Souveraineté · Éthique · Éco-responsabilité

Livre Blanc — Édition publique 2026

Reproduction libre avec mention de source

KALICORP — SIREN 907928956 — Sissonne, Aisne, France

Avant-propos

Ce livre blanc n'est pas un argumentaire commercial. C'est un état des lieux — celui d'une transformation profonde dans la façon dont les organisations peuvent et doivent envisager leur relation avec l'intelligence artificielle.

En 2026, l'IA est partout. Dans les outils de productivité, dans les processus métier, dans les services publics. Mais derrière cette omniprésence se cachent des questions que peu d'acteurs posent frontalement : qui contrôle les données traitées ? Où sont-elles hébergées ? Qui décide de ce que le modèle apprend ? Qui peut partir, et à quel prix ?

Kalicorp a été fondé avec une conviction simple : une infrastructure IA digne de confiance n'est pas une promesse contractuelle. C'est une architecture. Ce livre blanc partage ce que nous avons appris — et construit — pour que d'autres puissent s'en saisir.

Thibaut Neihouser, Fondateur — Kalicorp

Sommaire

1. Le contexte : pourquoi la dépendance cloud est devenue un risque stratégique
2. Les trois piliers de l'IA souveraine
 - 2.1 Souveraineté numérique et conformité
 - 2.2 Éthique et gouvernance de l'IA
 - 2.3 Éco-responsabilité et frugalité énergétique
3. Les 4 clauses contractuelles à exiger — et pourquoi elles ne suffisent pas
4. Le Sanctuaire : une infrastructure souveraine en conditions réelles
5. Ce que Kalicorp rend possible : 4 usages concrets
6. Recommandations pratiques
7. Conclusion : la confiance ne se délègue pas

1. Le contexte : pourquoi la dépendance cloud est devenue un risque stratégique

Pendant une décennie, l'adoption du cloud a été présentée comme une évidence économique et technologique. Réduction des coûts d'infrastructure, mise à l'échelle élastique, délégation de la maintenance. L'argument était solide. Il l'est toujours, à une condition près : que le fournisseur partage vos intérêts, votre juridiction, et votre horizon temporel.

Ce n'est plus une hypothèse que l'on peut faire les yeux fermés.

1.1 Le Cloud Act : une loi extraterritoriale méconnue

Le Clarifying Lawful Overseas Use of Data Act, adopté aux États-Unis en 2018, autorise les autorités fédérales américaines à exiger des entreprises américaines l'accès à des données stockées n'importe où dans le monde — y compris sur des serveurs localisés en France ou en Allemagne — sans qu'il soit nécessaire de passer par les voies diplomatiques classiques.

Impact concret

Une organisation française utilisant un service IA d'un fournisseur américain — même hébergé en Europe — peut voir ses données accessibles par des autorités étrangères, sans en être informée, et sans recours immédiat. Cette réalité est juridiquement établie.

Ce n'est pas une théorie. C'est le texte de loi. Le Privacy Shield a été invalidé en 2020 pour cette raison précise. Le Data Privacy Framework qui lui a succédé fait l'objet de contentieux actifs devant la CJUE.

1.2 La concentration du marché IA

En 2026, quelques grands groupes américains représentent l'essentiel de la puissance de calcul IA disponible dans le monde. Cette concentration crée une dépendance structurelle : les organisations qui ont bâti leur stratégie IA sur ces plateformes ne peuvent pas en sortir sans coûts significatifs — techniques, humains, contractuels. C'est ce que les économistes appellent un effet de lock-in.

1.3 L'AI Act européen : une opportunité de clarification

Le règlement européen sur l'intelligence artificielle, entré en vigueur en 2024, impose des obligations de transparence, de traçabilité et de gouvernance pour les systèmes IA déployés en Europe. Il crée un cadre — imparfait, en construction — mais qui offre quelque chose de précieux : une base légale pour exiger des garanties concrètes de ses fournisseurs.

Le problème est que la plupart des organisations ne savent pas encore comment traduire ces obligations réglementaires en exigences contractuelles et architecturales concrètes. C'est l'un des objets de ce livre blanc.

2. Les trois piliers de l'IA souveraine

L'IA souveraine n'est pas un concept marketing. C'est une architecture de décision qui repose sur trois piliers indissociables : la souveraineté technique et juridique, l'éthique opérationnelle, et la sobriété environnementale. Négliger l'un revient à fragiliser les deux autres.

2.1 Souveraineté numérique et conformité

La souveraineté numérique ne se décrète pas. Elle se construit à travers des choix techniques précis : hébergement des données sur des serveurs physiquement localisés sur le territoire national ou européen, utilisation de modèles dont les poids sont disponibles et auditable, absence de dépendance à des interfaces propriétaires fermées.

Exigence	Ce que cela signifie
Hébergement souverain	Infrastructure sur territoire national ou certifiée par l'ANSSI
Modèles auditables	Comportements documentés, périmètres d'action définis
Zéro transfert non consenti	Aucune donnée vers des serveurs hors UE sans consentement explicite
Conformité RGPD réelle	Conformité article par article — pas uniquement déclarative

Les risques d'une approche purement contractuelle

Beaucoup d'organisations pensent avoir résolu la question de la souveraineté avec une clause contractuelle stipulant que leurs données sont hébergées en Europe. C'est insuffisant pour deux raisons. Premièrement, une clause contractuelle ne protège pas contre une injonction légale étrangère. Deuxièmement, elle ne garantit pas l'auditabilité réelle du traitement — ce qui se passe entre l'envoi de la requête et la réception de la réponse reste une boîte noire.

« La confiance architecturale prime sur la confiance contractuelle. Ce qui est physiquement impossible ne peut pas faire l'objet d'une injonction. »

2.2 Éthique et gouvernance de l'IA

Au-delà de la conformité réglementaire, l'éthique de l'IA concerne la façon dont les systèmes sont conçus, déployés, et la relation qu'ils entretiennent avec leurs utilisateurs. Trois dimensions méritent une attention particulière en 2026.

La transparence des modèles

Un système IA éthique doit être en mesure d'expliquer — au moins partiellement — pourquoi il a produit une réponse donnée. Cette exigence de traçabilité est à la fois réglementaire (AI Act, article 13) et organisationnelle : une décision prise sur la base d'un système opaque ne peut pas être défendue en cas de litige.

La protection des utilisateurs finaux

Les utilisateurs d'un système IA ont des droits. Droit à l'information sur le traitement de leurs données. Droit d'accès, de rectification, d'effacement. Droit de ne pas faire l'objet de décisions entièrement automatisées. Ces droits existent dans les textes ; les faire vivre dans les systèmes est une responsabilité de l'opérateur.

La gouvernance des agents IA

L'émergence des agents IA autonomes — capables d'agir, pas seulement de répondre — crée de nouvelles questions de gouvernance. Qui est responsable d'une action automatisée qui cause un préjudice ? Comment documenter les décisions d'un agent ? Comment le contraindre à des périmètres d'action définis ? Ces questions n'ont pas encore de réponses réglementaires définitives. Mais les organisations qui attendent la réglementation pour y réfléchir prendront du retard.

2.3 Éco-responsabilité et frugalité énergétique

Un entraînement de grand modèle de langage consomme des ressources énergétiques considérables. L'inférence — l'utilisation quotidienne — s'additionne à l'échelle de millions d'utilisateurs. Les grands acteurs cloud ne publient pas de données granulaires sur ces chiffres.

La frugalité énergétique en IA n'est pas un luxe éco-responsable. C'est une nécessité économique et une exigence de cohérence pour toute organisation qui affiche des objectifs RSE sérieux. Il est possible de déployer une infrastructure IA performante avec une empreinte carbone maîtrisée : matériel reconditionné, énergie renouvelable, modèles de taille intermédiaire répondant à la quasi-totalité des cas d'usage métier.

3. Les 4 clauses contractuelles à exiger — et pourquoi elles ne suffisent pas

Quatre clauses sont désormais considérées comme minimales pour tout contrat IA sérieux en 2026.

Clause	Fournisseur cloud standard	Infrastructure souveraine
Non-entraînement	Opt-out souvent requis, parfois impossible	Natif — traitement 100% local, zéro flux externe
Auditabilité	Accès limité, boîte noire propriétaire	Natif — architecture auditable, comportements documentés
Localisation EU	Déclarée, rarement garantie techniquement	Natif — France, territoire national
Sortie sans pénalité	Préavis longs, coûts de migration significatifs	Natif — zéro vendor lock-in

Pourquoi les clauses ne suffisent pas

Une clause contractuelle est une promesse. Elle engage la responsabilité juridique du fournisseur en cas de violation — après la violation. L'architecture souveraine, elle, rend la violation physiquement impossible. C'est une différence de nature, pas de degré.

Cela ne signifie pas que les clauses sont inutiles — elles sont nécessaires. Mais elles doivent être considérées comme un plancher, pas un plafond, et accompagnées d'une vérification architecturale.

4. Le Sanctuaire : une infrastructure souveraine en conditions réelles

Le Sanctuaire est l'infrastructure IA de Kalicorp. Déployée à Sissonne, dans l'Aisne, elle est opérationnelle depuis plusieurs années et sert aujourd'hui une communauté réelle d'utilisateurs et de clients professionnels. Ce chapitre présente les chiffres et les choix tels qu'ils sont — sans idéalisation.

4.1 Chiffres clés

Indicateur	Valeur
Utilisateurs actifs	515+
Clients B2B	8
Souveraineté EU	100%
Dépendance cloud US	0%
Énergie principale	Solaire — ZRR Aisne
Référentiels suivis	ANSSI / RGPD / AI Act
DPO	Désigné — conformité RGPD opérationnelle

4.2 Approche technique

Le Sanctuaire repose sur du matériel d'entreprise reconditionné. Ce choix délibéré répond à deux objectifs : maîtrise des coûts et réduction de l'empreinte carbone de fabrication. La stack logicielle est entièrement constituée de composants sélectionnés pour leur auditabilité et leur indépendance — chaque brique est remplaçable et maintenue indépendamment de tout acteur dominant.

4.3 Gouvernance et conformité

La gouvernance du Sanctuaire repose sur une Analyse d'Impact relative à la Protection des Données (AIPD) formalisée, un DPO désigné, et un registre des activités de traitement maintenu à jour. La conformité AI Act est suivie activement dans les évolutions de déploiement.

Kalicorp est Activateur officiel France Num et poursuit un accompagnement PIIEC/BPI pour la structuration et l'extension de l'infrastructure.

« Le Sanctuaire m'a permis de travailler avec des outils IA sans jamais me poser la question de où vont mes données. C'est la première fois que j'ai cette certitude. »
— Utilisateur, secteur public local

5. Ce que Kalicorp rend possible : 4 usages concrets

La souveraineté ne vaut que si elle s'accompagne d'une expérience utilisateur à la hauteur des standards actuels. Kalicorp a développé quatre environnements complémentaires, chacun répondant à un besoin distinct. Tous partagent le même socle : traitement local, mémoire souveraine, aucune donnée hors du périmètre maîtrisé.

5.1 Collaboration en temps réel avec vos équipes et vos agents IA

La première rupture que Kalicorp introduit est celle de la messagerie souveraine intégrée à l'IA. Les équipes communiquent entre elles sur une plateforme hébergée localement — et interagissent dans le même flux avec leurs agents IA dédiés. L'agent répond dans le canal, en contexte, au même titre qu'un collaborateur, sans quitter l'environnement de travail. L'intelligence est dans le flux de travail, pas à côté. Et elle reste dans vos murs.

5.2 Générer des applications et des interfaces avec votre agent IA

Cette brique s'adresse aux organisations qui souhaitent produire des interfaces numériques — outils internes, applications métier — sans mobiliser une équipe de développement dédiée ni dépendre d'une plateforme SaaS étrangère. L'organisation décrit ce dont elle a besoin, affine en dialogue avec son agent, et obtient une application fonctionnelle hébergée sur son propre périmètre. La productivité du développement sans la dépendance au fournisseur.

5.3 Un espace de travail IA complet — mémoire, documents, images

Le cœur de l'offre est un environnement de travail IA augmenté. Chaque agent dispose d'une mémoire persistante et d'une base de connaissances documentaire alimentée par les documents de l'organisation, interrogeable en langage naturel. Rapports, synthèses, analyses réglementaires — l'agent produit des documents structurés directement exploitables. Un seul environnement souverain remplace une dizaine d'abonnements SaaS dispersés.

5.4 Production de contenu structuré avec votre agent en API

Pour les organisations qui produisent régulièrement du contenu structuré : rapports périodiques, notes de synthèse, documentation technique. L'agent prend en charge la mise en forme, la structuration et la première rédaction — pour que les équipes se concentrent sur ce qui requiert leur expertise. Rigueur, précision, sobriété. L'agent est au service de l'organisation, pas l'inverse.

Quatre environnements. Une philosophie commune : l'IA travaille pour vous, dans votre périmètre, sous votre contrôle. Pas l'inverse.

6. Recommandations pratiques

Quelle que soit la taille de votre organisation — TPE, ETI, collectivité, établissement d'enseignement, service public — voici les étapes concrètes pour progresser vers une IA plus souveraine, plus éthique et plus durable.

Étape 1

Évaluer sa dépendance actuelle

Cartographier tous les services IA utilisés. Identifier pour chacun : pays d'hébergement, loi applicable, clauses de non-entraînement. Évaluer l'exposition aux législations extraterritoriales. Mesurer le coût réel de sortie.

Étape 2

Prioriser par criticité des données

Toutes les données ne méritent pas le même niveau de protection. Classer les cas d'usage IA par sensibilité : données RH, médicales, juridiques, financières en priorité maximale ; données métier sensibles en souveraineté recommandée.

Étape 3

Construire progressivement

La souveraineté IA ne s'atteint pas en une migration. Elle se construit par couches. Exiger les 4 clauses minimales dans les nouveaux contrats. Déployer un premier service local sur un cas d'usage défini. Former les équipes. Structurer une gouvernance IA interne.

Étape 4

Ne pas confondre modèle auditable et infrastructure souveraine

Un modèle dont les comportements sont documentés, déployé sur un cloud étranger, n'est pas souverain. La souveraineté dépend de l'infrastructure d'hébergement et de la gouvernance des données — pas uniquement des caractéristiques du modèle.

Règle fondamentale

Modèle auditable + infrastructure souveraine + gouvernance documentée = confiance réelle.

Modèle auditable + hébergement étranger = illusion de maîtrise.

7. Conclusion : la confiance ne se délègue pas

L'intelligence artificielle est en train de devenir une infrastructure critique — au sens où l'électricité, les télécommunications et les réseaux de données le sont devenus avant elle. Et comme pour ces infrastructures, la question n'est pas de savoir si l'on peut se permettre d'investir dans leur souveraineté. C'est de savoir si l'on peut se permettre de ne pas le faire.

La confiance dans un système IA ne peut pas se déléguer entièrement à un contrat ou à la réputation d'un fournisseur. Elle doit être ancrée dans des choix architecturaux vérifiables, une gouvernance documentée, et une capacité réelle à comprendre ce qui se passe dans les systèmes que l'on déploie.

Ce n'est pas une posture idéologique. C'est une exigence de responsabilité — vis-à-vis des utilisateurs, des régulateurs, et des organisations elles-mêmes.

Kalicorp a choisi de bâtir cette démonstration en conditions réelles, avec des contraintes réelles — budget limité, équipe réduite, territoire rural. Le Sanctuaire existe. Il fonctionne. Il prouve que la souveraineté IA n'est pas réservée aux grandes organisations dotées de budgets cloud de substitution.

Elle est accessible à quiconque choisit de la construire.

Kalicorp — SIREN 907928956 — Sissonne, Aisne, France

Contact : kalicorp@proton.me — kalicorp.fr

Reproduction libre avec mention de source — Édition publique 2026