

Fiche IA & données — Localisation des traitements et résidence UE

LTC Group SRL · Version 1.0 · 12 août 2026 · contact@ltcai.be

Localisation des traitements et résidence UE

Résidence UE par design. Tout traitement et tout stockage de données de dossiers effectués par Nota ont lieu dans l'Union européenne : applicatif, base de données, stockage et IA propriétaires sur l'instance OVHcloud dédiée à Nota, en France ; inférence LLM en régions UE (Francfort, Allemagne) ; sauvegardes en UE (OVHcloud, France). **Il n'existe aucune option de traitement hors UE.** La résidence européenne est un invariant d'architecture du produit, pas un paramètre — elle s'applique d'office à tous les clients professionnels. Aucun transfert de données hors EEE au sens des articles 44 et suivants du RGPD n'a lieu ; le risque d'accès extraterritorial est traité frontalement ci-dessous.

Cartographie complète des traitements et stockages

Composant	Fournisseur	Rôle	Pays / région exacte	Données concernées	Chiffrement
Application web, API, workers	OVHcloud SAS	Hébergement applicatif et traitement (instance dédiée Nota)	France (UE) — ISO 27001	Données de dossiers en cours de traitement	TLS 1.2+/1.3 en transit
Base de données	OVHcloud SAS (PostgreSQL 16 + pgvector, géré par LTC)	Stockage structuré, isolation par étude (Row-Level Security)	France (UE) — ISO 27001, instance dédiée Nota	Dossiers, personnes, biens, métadonnées, index sémantiques	AES-256 au repos + TLS en transit
Stockage objets (GED)	OVHcloud SAS	Stockage S3-compatible des documents (instance dédiée Nota)	France (UE)	Pièces et documents des dossiers	AES-256 au repos + TLS en transit
IA propriétaires	LTC (infra OVHcloud)	NER bilingue fr/nl (C2), LLM critique	France (UE)	Texte des dossiers — ne quitte jamais	TLS en transit ; traitement

Composant	Fournisseur	Rôle	Pays / région exacte	Données concernées	Chiffrement
LTC	dédiée)	C3 (open-weights, famille Llama), embeddings multilingues (multilingual-e5)		l'infrastructure LTC, aucun tiers n'y accède	exclusivement interne LTC
Inférence LLM (Claude via Bedrock)	Amazon Web Services	Génération et raisonnement	Régions UE — Francfort, Allemagne	Texte exclusivement pseudonymisé par Veil™ ; zéro rétention d'inférence, aucun usage pour l'entraînement	TLS en transit ; aucune persistance
Connecteur mail M365 (optionnel)	Microsoft Ireland	Accès aux mails via Graph — uniquement si l'Étude l'active	UE (Microsoft EU Data Boundary)	Mails de l'Étude	TLS en transit
Sauvegardes	OVHcloud SAS	Sauvegardes quotidiennes	France (UE)	Copies chiffrées des bases et du stockage	AES-256 ; stockées en UE (OVHcloud, France) ; rétention 35 jours

Le Compagnon local optionnel (lecteur eID, scan réseau) s'exécute sur le poste de l'Étude et **ne stocke aucune donnée de dossier en local**.

Cycle de vie d'une requête IA, étape par étape

1. **Poste de l'utilisateur** (l'Étude) : la requête est envoyée à Nota en TLS.
2. **Nota** (instance OVHcloud dédiée, France) : assemblage du contexte utile (dossier, GED, mails) — intégralement en UE.
3. **Veil™** (moteur propriétaire de pseudonymisation, infrastructure LTC en UE) : détection déterministe (NRN, IBAN, BCE, etc.), NER bilingue fr/nl, puis LLM critique local. La table de correspondance pseudonymes ↔ données réelles est créée **en mémoire vive uniquement**, dans un vault dédié.
4. **AWS Bedrock, Francfort** : seul le texte pseudonymisé est transmis à Claude — **inférence sans rétention** (aucune conservation des prompts/réponses, pas d'usage pour l'entraînement par AWS/Anthropic).

5. **Retour** de la réponse, toujours pseudonymisée, vers l'infrastructure LTC.
6. **Réversion en RAM** : re-substitution des pseudonymes par les valeurs réelles.
7. **Affichage** du résultat à l'utilisateur.

Point clé : la table de correspondance ne quitte jamais l'infrastructure LTC. Elle n'est ni transmise au fournisseur d'inférence, ni persistée. Le LLM cloud ne voit à aucun moment une donnée nominative de dossier. Des tests anti-fuite automatisés (« corpus no-leak ») s'exécutent en continu. Les données pseudonymisées par Veil demeurent des données à caractère personnel au sens du RGPD (considérant 26). AWS (Bedrock) est donc traité comme sous-traitant ultérieur, sous accord article 28, et non comme destinataire de données anonymisées. Un document pseudonymisé conserve par ailleurs un contenu narratif et des combinaisons contextuelles pouvant permettre une individualisation résiduelle (singling-out) sans identifiant direct — risque assumé explicitement et traité au scénario dédié de l'analyse d'impact.

Entités mères non-UE : risque d'accès extraterritorial et mitigations

AWS et Microsoft ont des maisons mères américaines (OVHcloud SAS, hébergeur de l'instance dédiée Nota, est une société française). Même avec des régions de traitement exclusivement européennes, une exposition à des législations à portée extraterritoriale (type CLOUD Act) doit être adressée pour les fournisseurs à maison mère non-UE. Mitigations en place :

- **Pseudonymisation Veil en amont des LLM** : aucun texte nominatif de dossier n'atteint le fournisseur d'inférence ; la table de réversion reste chez LTC.
- **Chiffrement systématique** : TLS 1.2+/1.3 en transit, AES-256 au repos (base de données, stockage objets, sauvegardes).
- **Clés gérées par LTC**, secrets en gestionnaire dédié.
- **Cadre contractuel** : DPA art. 28 avec OVHcloud (fournisseur français) ; DPA + clauses contractuelles types (SCC) avec AWS et Microsoft ; zéro rétention d'inférence côté Bedrock.
- **Choix systématique des régions UE** : France (OVHcloud — instance dédiée Nota : applicatif, base de données, stockage, sauvegardes, IA propriétaires), régions UE Francfort (AWS Bedrock — inférence LLM uniquement), EU Data Boundary (Microsoft).

Conclusion. Aucun transfert de données hors EEE au sens des articles 44 et suivants du RGPD : tous les traitements ont lieu dans l'Union européenne (OVHcloud France ; AWS Bedrock régions UE ; Microsoft EU Data Boundary si activé). **Le risque d'accès par une autorité d'un pays tiers, inhérent au recours à un fournisseur soumis à une législation extraterritoriale (AWS, Microsoft), est traité frontalement : pseudonymisation systématique en amont (Veil™), absence de rétention des données d'inférence, chiffrement avec clés détenues par LTC, et clauses contractuelles types (SCC 2021/914) en garantie résiduelle.** OVHcloud (société française) n'est pas concerné. Les SCC

constituent un filet de sécurité contractuel face au risque résiduel d'accès extraterritorial, non un mécanisme de transfert opérationnel.

Développement vs production

L'API directe Anthropic (hébergée aux États-Unis) **ne fait pas partie de la chaîne de production** : son usage est strictement limité aux environnements de développement, sur **données fictives ou anonymisées** uniquement. Les environnements de développement et de production sont séparés : le développement et le staging s'exécutent sur une infrastructure LTC distincte (OVHcloud), données fictives uniquement ; **les données de production ne sont jamais utilisées en développement ou en test**. Anthropic (API directe) ne figure donc pas dans la liste des sous-traitants de production (cf. [Annexe B du DPA](#)).

Version 1.0 · 12 août 2026 · LTC Group SRL — contact@ltcai.be

LTC Group SRL · BCE 1036.831.317 · Rue du Noir Jambon 13, 7830 Thoricourt, Belgique · contact@ltcai.be
Document publié dans le centre de confiance Nota : <https://www.ltcai.be/nota/confiance>