TRUST CENTER

Sécurité & Confidentialité

Architecture, documents juridiques, conformité IA et gouvernance — l'ensemble des contrôles que Titane Intelligence applique sur les données de ses clients e-commerce.

Architecture & sécurité

- Hébergement UE exclusif — AWS région eu-west-3 (Paris)
- Architecture à deux couches : data lake analytique pseudonymisé / coffre d'activation isolé
- Pseudonymisation par défaut — jamais « anonymisation »
- Chiffrement AES-256 KMS at-rest, TLS 1.3 in-transit, CMK distinctes par client
- Forteresse réseau : VPC privés + Endpoint Policies + bucket policies aws:sourceVpce
- Politique Zéro Donnée Locale
- RBAC, MFA hardware admins, IAM Identity Center, moindre privilège
- PRA/PCA — RTO 4h / RPO 24h (1h modèles prod), tests trimestriels

Documents juridiques

- Politique de confidentialité 2 sections (RT propre / sous-traitant art. 28)
- Mentions légales LCEN complètes
- Data Processing Agreement (DPA), Accord de confidentialité (NDA)
- 8 clauses art. 28 §3 + 4 annexes (traitement, TOMs, sous-traitants, SCC)
- Clause anti-cross-training en clause 3.4 du DPA
- Liste publique des sous-traitants ultérieurs (AWS, Vercel)
- Engagement notification violation ≤ 12h (vs. 72h CNIL)

Conformité IA

- Exclusion contractuelle de tout usage solvabilité / BNPL / crédit (sortie haut risque Annexe III)
- Model cards, datasheets, lineage de modèle complet (dataset + code + paramètres + opérateur)

Gouvernance & contact

- DPO externe mutualisé — dpo@titane-intelligence.com
- Point de contact sécurité — securite@titane-intelligence.com
- Procédure d'exercice des droits (accès, effacement, portabilité, opposition)
- Effacement en cascade : CMS → Foundry Titane → Deep Learning → CRM → La Forge
- Sous NDA : Security White Paper, rapports pentests, AIPD interne
- Registre art. 30.2 interne (extrait public dans Trust Center)
- Droit de réclamation CNIL rappelé

Pseudonymisation par défaut

> *« Pseudonymisation par défaut. Identifiants d'activation stockés séparément dans un coffre cryptographique. Nos algorithmes ne traitent que des jetons mathématiques décorrélés de toute identité civile. Le rapprochement final s'effectue automatiquement au sein de fonctions*

éphémères sécurisées, sans intervention humaine. »

Roadmap conformité — Certifications et travaux en cours

« Titane applique déjà les contrôles essentiels, documente sa sécurité, et construit progressivement un système de management conforme aux standards reconnus, avec une certification ISO 27001 visée à moyen terme (2027). Notre Security White Paper est disponible sur demande sous NDA. »

- Titane a engagé une démarche ISO 27001:2022 : gap analysis réalisé, SMSI en cours de structuration, contrôles prioritaires déjà appliqués, certification visée en 2027.
- ISO 27701 est prévue comme extension privacy après stabilisation et certification du SMSI ISO 27001.
- SOC 2 Type II est inscrit dans la roadmap conformité, avec une fenêtre de préparation estimée à 6-12 mois selon les exigences clients et les ressources disponibles.
- Red teaming périodique des modèles ML (ML Privacy Meter)
- Évaluation DP-SGD (Opacus) sur scoring client — POC en cours
- Migration définitive VS Code/Cursor/Antigravity Remote SSH — Zéro Donnée Locale appliquée