NOXYS

Compliance Evidence Report

Security & Procurement FAQ

Tenant	**Noxys Enterprise**
Version	**1.2**
Generated	**May 2026**
Classification	**Public**

Frequently Asked Questions for IT Procurement

This document provides answers to the security and compliance questions frequently asked by enterprise procurement teams.

Où sont stockés les prompts et les métadonnées des clients ?
Toutes les données sont hébergées exclusivement au sein de l'Union européenne (régions EU-West) par défaut.

Pouvons-nous isoler nos données dans une région ou un pays spécifique ?
Oui. Les clients Enterprise peuvent demander un pinging par région (ex: France, Allemagne) via un avenant au DPA.

Comment les données sont-elles chiffrées en transit ?
Toutes les communications utilisent TLS 1.3. TLS 1.2 est accepté mais signalé ; les versions antérieures sont rejetées.

Comment les données sont-elles chiffrées au repos ?
Les données persistantes sont chiffrées à l'aide de AES-256-GCM avec un chiffrement par enveloppe via un KMS cloud.

Pouvons-nous apporter notre propre clé de chiffrement (BYOK/CMK) ?
Oui. Les clients de niveau Enterprise peuvent fournir une clé gérée par le client (CMK).

Noxys est-il immunisé contre la surveillance extra-territoriale (ex: US CLOUD Act) ?
Oui. Noxys est détenu à 100% dans l'UE et utilise des hébergeurs souverains comme OVHcloud.

Utilisez-vous des sous-traitants américains pour le traitement des données critiques ?
Non. Tout le traitement critique est effectué sur une infrastructure souveraine de l'UE.

Quels hébergeurs utilisez-vous pour les déploiements souverains ?
Par défaut, OVHcloud (France) et Hetzner (Allemagne).

Proposez-vous une version 'Air-gapped' ?
Oui. Noxys propose un pack de déploiement Air-Gapped pour les clients à haute sensibilité.

Quelles sont les certifications détenues par Noxys ?
SOC 2 Type I est en cours (T3 2026). Nous sommes entièrement prêts pour le RGPD et l'EU AI Act.

Noxys est-il conforme au RGPD ?
Oui. Noxys agit en tant que sous-traitant au sens de l'article 28 du RGPD.

Quelles sont les méthodes d'authentification supportées ?
SSO via OIDC/SAML 2.0, SCIM 2.0 (T3 2026) et comptes locaux avec MFA.

Quel modèle de contrôle d'accès est utilisé ?
Contrôle d'accès basé sur les rôles (RBAC) avec les rôles Owner, Admin, Analyst et Read-Only.

Combien de temps les données sont-elles conservées ?
90 jours par défaut pour les logs (configurable jusqu'à 7 jours). 1 an pour les logs d'audit.

Pouvons-nous demander la suppression anticipée de nos données ?
Oui. Les demandes de suppression définitive sont exécutées sous 72 heures.

Un DPA est-il disponible ?
Oui. Un DPA Noxys standard est disponible avant la signature du contrat.

Quel est le SLA de notification pour les incidents de sécurité ?
24 heures pour l'évaluation préliminaire ; 72 heures pour le rapport RGPD.

Noxys effectue-t-il des tests d'intrusion ?
Oui, annuellement par un tiers indépendant.

Pouvons-nous effectuer notre propre test d'intrusion ?
Oui, avec un préavis de 5 jours ouvrés pour des tests en boîte noire.

Fournissez-vous un SBOM (Software Bill of Materials) ?
Oui, généré pour chaque version au format CycloneDX.

Quel est votre SLA pour le correctif des vulnérabilités critiques ?
Les vulnérabilités critiques sont corrigées sous 24 heures.

Noxys dispose-t-il d'une assurance cyber-responsabilité ?
Oui, couverture jusqu'à 5 000 000 € par sinistre.

Effectuez-vous des vérifications d'antécédents sur vos employés ?
Oui, obligatoire pour tous les employés ayant un accès à la production.

Comment l'accès à la production est-il restreint ?
MFA matériel, bastions, accès JIT et enregistrement complet des sessions.

Comment garantissez-vous la disponibilité du service ?
Architecture multi-région active-active avec une garantie de disponibilité de 99,9% à 99,99%.

Comment gérez-vous la sécurité de l'extension navigateur ?
Conformité Manifest V3, permissions minimales et isolation des scripts tiers.

Que se passe-t-il après un incident ?
Un post-mortem complet est livré sous 7 jours ouvrés.

Quels sont vos sous-traitants ?
Stripe (Facturation), OVHcloud (Base de données), Hetzner (Calcul).

Pouvons-nous auditer les contrôles de Noxys ?
Oui. Les clients Enterprise ont des droits d'audit et un support pour les questionnaires.

Comment le principe de minimisation des données est-il appliqué ?
Seules les empreintes (hashes) des prompts sont stockées, jamais le texte brut.

—

Contact Information

For detailed security assessments or specific questionnaire completion, contact our security team:

- **Security & Pentest**: security@noxys.eu
- **Privacy & GDPR**: privacy@noxys.eu
- **Legal**: legal@noxys.eu