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.

Where are customer prompts and metadata stored?
All data is hosted exclusively within the European Union (EU-West regions) by default.

Can we pin our data to a specific region or country?
Yes. Enterprise customers may request per-region pinning (e.g., France, Germany) via a DPA addendum.

How is data encrypted in transit?
All communications use TLS 1.3. TLS 1.2 is accepted but flagged; older versions are rejected.

How is data encrypted at rest?
Persisted data is encrypted using AES-256-GCM with envelope encryption via cloud KMS.

Can we bring our own encryption key (BYOK/CMK)?
Yes. Enterprise tier customers may supply a Customer-Managed Key (CMK).

Is Noxys immune to extra-territorial surveillance (e.g., US CLOUD Act)?
Yes. Noxys is 100% EU-owned and uses sovereign hosting providers like OVHcloud.

Do you use any US-based subprocessors for core data processing?
No. Core processing is performed on EU-sovereign infrastructure.

Which hosting providers do you use for sovereign deployments?
By default, OVHcloud (France) and Hetzner (Germany).

Do you offer an 'Air-gapped' version?
Yes. Noxys offers an Air-Gapped Deployment package for high-sensitivity clients.

What certifications does Noxys hold?
SOC 2 Type I is in progress (Q3 2026). We are fully GDPR and EU AI Act ready.

Is Noxys GDPR-compliant?
Yes. Noxys acts as a Data Processor under GDPR Article 28.

What authentication methods are supported?
SSO via OIDC/SAML 2.0, SCIM 2.0 (Q3 2026), and local accounts with MFA.

What access-control model is used?
Role-Based Access Control (RBAC) with Owner, Admin, Analyst, and Read-Only roles.

How long is data retained?
90 days by default for logs (configurable down to 7 days). 1 year for audit logs.

Can we request early deletion of our data?
Yes. Hard-delete requests are executed within 72 hours.

Is a DPA available?
Yes. A standard Noxys DPA is available pre-contract.

What is the notification SLA for security incidents?
24 hours for preliminary assessment; 72 hours for GDPR reporting.

Does Noxys conduct penetration testing?
Yes, annually by an independent third-party.

Can we conduct our own penetration test?
Yes, with 5 business days' notice for black-box testing.

Do you provide a Software Bill of Materials (SBOM)?
Yes, generated for every release in CycloneDX format.

What is your SLA for patching critical vulnerabilities?
Critical vulnerabilities are patched within 24 hours.

Does Noxys carry cyber-liability insurance?
Yes, coverage up to €5,000,000 per claim.

Do you conduct background checks on employees?
Yes, mandatory for all employees with production access.

How is access to production restricted?
Hardware MFA, Bastion hosts, JIT access, and full session recording.

How do you ensure service availability?
Multi-region active-active architecture with 99.9% - 99.99% uptime guarantee.

How do you handle browser extension security?
Manifest V3 compliance, minimum permissions, and third-party script isolation.

What happens after an incident?
Full post-mortem delivered within 7 business days.

What are your sub-processors?
Stripe (Billing), OVHcloud (Database), Hetzner (Compute).

Can we audit Noxys controls?
Yes. Enterprise customers have audit rights and questionnaire support.

How is the data minimization principle applied?
Only hashes of prompts are stored, never the raw text.

—

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