Security Overview

Prepared by Navwis Management ApS · April 2026

EXECUTIVE SUMMARY

EUSecureAI is a secure, GDPR-compliant AI platform built for European businesses. The platform enables organizations to build AI-powered knowledge bases and customer support widgets while keeping all data within the European Union. No passwords are stored; authentication uses magic-link emails with optional organisation-enforced two-factor authentication (TOTP). All data is isolated per organization.

INFRASTRUCTURE

All systems operate entirely within the European Union:

- Application server: OVH VPS — Frankfurt, Germany (EU)
- Database: OVH Managed PostgreSQL — EU region, SSL required
- Email delivery: SendGrid HTTP API (HTTPS, port 443)
- AI inference: Nebius AI Studio (EU-accessible endpoint)

ACCESS CONTROL & AUTHENTICATION

Authentication is handled via magic-link emails — no passwords are ever created or stored. Sessions are managed server-side via NextAuth.js with cryptographic session tokens.

Organisation owners may enforce TOTP two-factor authentication (RFC 6238) for all members. Compatible with standard authenticator apps (Google Authenticator, Microsoft Authenticator, Authy). A 7-day grace period applies when enforcement is first enabled. Microsoft OAuth (Azure AD) users are exempt, as MFA is enforced at the identity provider level. TOTP secrets are encrypted at rest using AES-256-GCM and are only persisted after the user successfully verifies a valid code. Backup codes are single-use and stored as bcrypt hashes.

Role-based access control (RBAC) is enforced on every API route:

- Member — can use the AI chat and view permitted documents
- Admin — can manage knowledge base documents and team members
- Owner — full control including billing, widget configuration, and audit log access

DATA PROTECTION

Data is isolated per organization at the database level. AI queries are scoped strictly to the requesting organization's document set — cross-organization data access is architecturally prevented.

Data in transit is encrypted via TLS. Database connections require SSL with certificate verification (OVH CA). Customer data is never used to train AI models.

AUDIT & MONITORING

An append-only audit log records all significant user actions: document uploads and deletions, team member changes, role assignments, invitation events, and widget configuration changes. Each entry captures the actor, action type, timestamp, and organization.

Application errors are tracked in real time via Sentry (EU data region).

AI DATA HANDLING

AI responses are generated via the Nebius AI Studio API using Meta Llama 3.3 70B Instruct. All queries are scoped to the requesting organization's uploaded documents. No query content or customer data is shared with third parties beyond the inference provider under data processing terms.

RESPONSIBLE DISCLOSURE

Security vulnerabilities may be reported to security@eusecureai.com. We aim to acknowledge all reports within 48 hours and provide a remediation timeline within 5 business days.

GDPR ALIGNMENT

All personal data is processed and stored within the European Union. A Data Processing Agreement (DPA) is available upon request. Data subjects may request access to, rectification of, or deletion of their personal data by contacting privacy@eusecureai.com.