Navos

Security at Navos

Your data is protected by enterprise-grade infrastructure with strict tenant isolation.

Data Architecture

Your data is hosted on Supabase (AWS EU region) with PostgreSQL. Row-level security enforces per-company isolation at the database level. No shared tables, no data leakage between tenants.

- Every query is scoped to the authenticated user's company via Row Level Security (RLS), enforced by PostgreSQL at the database engine level, not by application logic.
- All data encrypted in transit (TLS 1.2+) and at rest (AES-256).
- Data residency: EU region (AWS eu-central-1). No data leaves the EU unless you explicitly request export.

AI and LLM Data Handling

AI analysis is powered by Anthropic (Claude) and OpenAI APIs. Both providers operate under enterprise API terms: your data is never used to train models.

- Data sent for processing is not stored by providers beyond the request lifecycle.
- Perplexity is used for web intelligence searches only. No company data is sent to Perplexity.

Authentication and Access Control

Role-based access control with four tiers (Owner, Admin, Member, Viewer) per company. Platform admin operations are audited separately.

- Session management via secure tokens with automatic refresh.
- Platform admin tier for Navos operations team. All admin access is logged.

CEO Data Sovereignty

You own your data. Three non-negotiable rights: export everything, delete everything, revoke any access instantly.

- Export: Self-serve data export in JSON and PDF formats from Settings.
- Delete: Account deletion request from Settings, executed within 30 days. Anonymized aggregate data retained only where no longer personally identifiable.
- Revoke: Every access grant is revocable with immediate effect. No grace period.

Operational Security

No client secrets in frontend code. Backend secrets managed via Supabase environment variables, never committed to source control.

- Admin activity audit logging tracks all administrative actions.
- Dependency vulnerability monitoring with documented mitigations.
- Frontend uses only anonymous (public) API keys. No secret keys are exposed.

GDPR Compliance

Legal basis documented per processing function. Data subject rights supported: access, rectification, erasure, portability, and restriction of processing.

- Core advisory services: contract performance (GDPR Art. 6(1)(b)).
- Sub-processors: Anthropic (AI), OpenAI (AI), Supabase/AWS (hosting), Perplexity (intelligence), Resend (email).
- Standard Data Processing Agreement (DPA) available for enterprise clients.
- Data stored in EU region. Deletion available upon request.

Incident Response

Monitoring for unauthorized access patterns. Affected users notified within 72 hours per GDPR requirements.

- Hellenic Data Protection Authority notified within 72 hours if breach poses risk to individuals.
- Root cause analysis and system hardening after any incident.
- Direct, transparent communication. You will never learn about a security incident from the news.

Compliance Roadmap

Current controls include multi-tenant RLS isolation, RBAC, audit logging, and encryption at rest and in transit. We are actively expanding our compliance posture.

- Current: Multi-tenant isolation, role-based access, audit logging, encryption at rest/transit, privacy policy, terms of service.
- Near-term: MFA, SSO/OAuth for enterprise clients, formal data classification, self-serve data export and deletion.
- Planned: SOC 2 Type I certification, penetration testing, formal backup verification, uptime monitoring with SLA.
