# NordScope Security FAQ

EU Sole-Trader SaaS Posture

Version: NordScope Security FAQ v1.0

Last reviewed: 2026-05-04

Next review due: 2026-11-04

This FAQ supplements the CAIQ v4.0.3 pre-fill at `/trust/caiq-v4.pdf` with EU-specific and sole-trader-specific context that the CCM v4 framework does not directly address. Procurement reviewers evaluating PortalPilot for EU mid-market deployments should read this alongside the published Privacy Policy (`/privacy`), Data Processing Agreement (`/dpa`), and Sub-processor list (`/sub-processors`).

## (a) Legal entity

Operates as a Finnish sole trader (toiminimi). Entity name: **NordScope**. Y-tunnus: **3148476-5**. Jurisdiction: **Finland**.

For liability terms applicable to specific commercial relationships, see the executed DPA and MSA on a per-deal basis.

## (b) Infrastructure

Production runs on Hetzner Cloud in the Helsinki, Finland region. All customer data — credentials, analysis runs, recommendations, and audit logs — is stored within the EU at the Hetzner Helsinki facility. The cloud sub-processor maintains ISO 27001 / 27017 / 27018 certification covering the physical, hypervisor, and network-edge layers.

NordScope operates no datacentre infrastructure of its own. The application stack is an open-source-software set (PostgreSQL database, Node.js / Deno runtime, React frontend, Nginx ingress) running on standard Linux virtual machines, intentionally portable should the relationship with the current cloud sub-processor end.

## (c) Sub-processors

The complete, current sub-processor list is published at `/sub-processors` with each party's name, jurisdiction, processing purpose, data categories accessed, and certification posture. Material additions to the inventory trigger advance customer notification per DPA § 4.2 (Sub-processor changes) with a defined objection window.

The current set is small and EU-favoured: Hetzner (Finland) for infrastructure, Mollie (Netherlands) for payments, Mistral AI (France) for analysis-augmentation, and a transactional-email sub-processor. Each operates under a contract that flows down customer-protective terms (GDPR Art. 28, security baseline, audit cooperation) per DPA § 4.

## (d) HubSpot data handling

PortalPilot integrates with the customer's HubSpot portal via OAuth on the v3 endpoints. The OAuth scope set is restricted to read-only scopes for the data classes required by the analysis features the customer has enabled; write access is requested only for explicit features the customer activates. Tokens are encrypted at rest in the database with AES-256-GCM, with token refresh handled by the application's idempotent refresh procedure to prevent concurrent-refresh races.

PortalPilot does not retain copies of HubSpot record data beyond the scope of the analysis run requested by the customer. Analysis outputs (audit results, recommendations, scores) are PortalPilot-derived artefacts and are retained per the DPA § 9 retention table; underlying HubSpot record data lives on the customer's own HubSpot portal and is programmatically retrievable from HubSpot directly via HubSpot's CRM API.

## (e) DPA and Privacy posture

The public Data Processing Agreement at `/dpa` is the canonical contractual document covering: roles and responsibilities (controller / processor allocation per GDPR Art. 28), scope of processing, sub-processors, security measures, data subject rights, breach notification (72 hours per GDPR Art. 33), audit rights, retention, deletion, and international transfers. The public Privacy Policy at `/privacy` complements the DPA with the lawful-basis statement, processing purposes, and data-subject-rights mechanism for end-user-facing processing.

Both documents are reviewed annually and on material-change triggers (regulatory update, new sub-processor type, customer-requested amendment per DPA § 14).

## (f) GDPR contact

Under GDPR Art. 27, a sole trader in Finland operating wholly within the EU does not require an Article-27 representative for processing within the Union. Article-37 Data Protection Officer (DPO) appointment is not mandatory at this scale (no large-scale systematic monitoring, no large-scale special-categories processing). Privacy and data-protection enquiries are handled directly by the founder via the contact channel documented in the Privacy Policy.

The Finnish supervisory authority for data protection is **Tietosuojavaltuutettu** (Office of the Data Protection Ombudsman). Customers exercising statutory rights against NordScope as processor receive cooperation per DPA § 7 and DPA § 8.

## (g) Incident response and notification

Personal-data breach notification follows DPA § 7: customers (controllers) are notified without undue delay and in any case within 72 hours of becoming aware of the breach, per GDPR Art. 33. The notification includes the nature of the breach, affected data categories, likely consequences, and remedial measures, and the operator cooperates with any subsequent supervisory-authority investigation.

Service-availability incidents and security-relevant events that do not constitute a personal-data breach are notified per the Security page § Incident response (in-app banner + direct email channel).

The current contact channel for vulnerability reports is documented at `/security`. A formal Vulnerability Disclosure Program with safe-harbour language and SLA is planned (tracked separately under WS-04 of the enterprise-readiness program).

## (h) Data residency

All customer data processed by PortalPilot — credentials, analysis runs, recommendations, audit logs, and operational logs — is stored at the Hetzner Helsinki facility within the EU. The AI sub-processor for analysis-augmentation (Mistral AI) is also EU-based (Paris, France). The transactional-email sub-processor delivery infrastructure operates within EU jurisdictions per its published privacy materials. Payments routing via Mollie (Netherlands) is EU-based.

No transfers of customer personal data to non-EU/EEA jurisdictions occur in the standard processing path. Where a customer-initiated action (e.g., support-channel correspondence) results in a transfer outside the EU, the standard GDPR Chapter V mechanism (e.g., Standard Contractual Clauses) applies.

## (i) Mistral AI use posture

PortalPilot uses Mistral AI (EU-based, Paris, France) for analysis-augmentation features such as recommendation generation. Customer data sent to Mistral is the minimum necessary for the requested analysis (typically a sanitised excerpt of the customer's analysis run, never raw HubSpot record data with personally identifying fields). Mistral operates under a contract that prohibits use of customer-submitted content for model training; this is the standard Mistral commercial-API posture documented in their public DPA.

Per ADR-005 (LLM Pinning Strategy), the premium-path Mistral model is pinned to a specific dated model identifier; free-tier paths use the `-latest` alias and auto-rotate per Mistral's deprecation lifecycle. A daily deprecation watch monitors the Mistral API for upcoming retirements.

## (j) References

The following external resources informed this FAQ and the underlying compliance posture:

- **ENISA cloud security guidance for SMEs** — European Union Agency for Cybersecurity guidance on cloud security for small and medium enterprises, applied as a baseline reference for the sole-trader posture. - **VSA-Core GDPR questions** — Vendor Security Alliance core questionnaire GDPR sub-section, used to cross-verify the DPA and Privacy posture against an industry-standard control set. - **CSA CCM v4.0.3** — Cloud Security Alliance Cloud Controls Matrix, the framework underlying the CAIQ v4.0.3 pre-fill at `/trust/caiq-v4.pdf`. - **EU Cloud Code of Conduct (EU Cloud CoC)** — Self-attested adherence published at `/compliance/eu-cloud-coc-self-attestation.html`. - **ISO 27001 Annex A register** — Per-control coverage attested by the founder at `/compliance/iso27001-annex-a-register.html`. - **ISMS scope statement** — In-scope assets and control posture at `/compliance/isms-scope-statement.html`.

For procurement-reviewer enquiries beyond the scope of this FAQ + the published Trust Center, the contact channel documented at `/security` is the appropriate first point of contact.