

• SECURITY OVERVIEW

Security architecture and *controls*.

How Subtonal protects transcript data: encryption, data minimisation, access restrictions, monitoring, and operational safeguards.

01 — ENCRYPTION

Encrypted everywhere

All data is encrypted in transit (TLS 1.2+) and at rest using AWS KMS customer-managed keys.

02 — HOSTING

Stockholm, EU-only

Hosted in AWS Europe (Stockholm), eu-north-1.
Personal data never leaves the EU.

03 — STORAGE

Zero persistence

Transcripts are processed in memory only. No transcripts, audio, or derived records are ever stored.

Pipeline architecture

- ✓ Subtonal is a transcript extraction pipeline: it pulls call and meeting transcripts from note-taker providers, redacts personal data, and forwards the redacted records to a customer-configured analysis endpoint.
- ✓ The worker runs as a scheduled container task (AWS Fargate) that starts, processes, and exits — no long-running servers, no inbound endpoints exposed.
- ✓ Transcripts exist only in process memory. Nothing is written to disk or database inside Subtonal's perimeter.
- ✓ **Optional:** the worker container can be self-hosted inside the customer's own environment, so transcript content never enters Subtonal infrastructure at all.

- ✓ Provider credentials are stored in AWS Secrets Manager, encrypted with a customer-managed KMS key.
- ✓ IAM roles follow least privilege: the worker can read exactly the secrets and records it needs, and nothing else.
- ✓ Every key use (kms:Decrypt) and secret access is recorded in AWS CloudTrail.
- ✓ Administrative access to AWS accounts is centralised and fully logged; the management account hosts no workloads.

Access & credentials

PII *redaction*

- ✓ Two redaction passes are applied before any data leaves the engine.
- ✓ **Rule-based pass:** deterministic, auditable patterns for Swedish personnummer, organisationsnummer, phone numbers, emails, IBANs, payment cards, and addresses.
- ✓ **Named-entity pass:** Microsoft Presidio runs locally inside the worker — transcript content is never sent to any external PII or AI API.
- ✓ Only the redacted version is forwarded downstream — never raw transcript content.
- ✓ AWS AI-service training opt-out is enforced at the AWS Organization root and cannot be overridden by member accounts.

- ✓ An organisation-wide CloudTrail records every management and data-access event across all AWS accounts.
- ✓ Audit logs are delivered to an immutable (Write-Once-Read-Many) archive in a dedicated audit account and retained for seven years.
- ✓ Amazon GuardDuty, AWS Security Hub, and AWS Config run continuously across all accounts, with findings aggregated organisation-wide.
- ✓ Application logs are PII-stripped at the observability layer before they are written.

Continuous monitoring

• DATA INTEGRATION

API-based data collection

- ✓ Transcripts are pulled from source providers over authenticated APIs using scoped, per-customer credentials with least-privilege access.
- ✓ Poll-only design: Subtonal initiates every connection outbound. There are no inbound webhooks and no publicly exposed endpoints.
- ✓ Each source integration is opt-in per customer, under the customer's own contract with that provider.

- ✓ Subtonal is a courier, not a store: only sync cursors and account metadata are kept, in a KMS-encrypted DynamoDB table with point-in-time recovery.
- ✓ The downstream analysis endpoint receives redacted records only, over TLS with token authentication.

• BACKUP & DISASTER RECOVERY

Infrastructure as code

- ✓ The entire platform is defined and deployed as Infrastructure as Code (AWS CDK) — reviewed, versioned, and reproducible.
- ✓ All configuration and source code is version-controlled and backed up outside AWS.
- ✓ Because no customer data is stored, disaster recovery is a redeploy: the full platform can be rebuilt from source at any time.

• DATA MANAGEMENT

Data handling

Compliance roadmap

- ✓ **GDPR:** in effect. A Data Processing Agreement (DPA) is available to all customers on request.
- ✓ **Pre-certification:** we do not yet hold third-party security certifications. We operate against the SOC 2 and ISO 27001 frameworks and are preparing for audit.
- ✓ **Vulnerability disclosure:** reports to security@subtonal.se are acknowledged within two business days, with a status update within five.

ON YOUR SIDE

Recommendations for customers

- ✓ Scope the provider credentials issued to Subtonal to read-only transcript access where the provider supports it.
- ✓ Protect the receiving analysis endpoint with TLS and an authentication token, and rotate the token periodically.
- ✓ If self-hosting the worker, apply container image updates as they are released.
- ✓ Customers are responsible for securing their own environments and downstream systems.

Have questions about our security practices? **Get in touch** → security@subtonal.se