Forsyt

ISO 27001 GDPR

Security and trust, documented openly.

Revenue data is the most sensitive asset your company owns. Forsyt is engineered so it never leaves your control, by architecture and by contract. This document summarises our posture, deployment options, and the artifacts your security team will ask for next.

forsyt.com/security · security@forsyt.com

SECURITY ARCHITECTURE

Defense in depth, every control we operate today.

Forsyt runs an Information Security Management System (ISMS) aligned to ISO/IEC 27001 controls. The list below is exhaustive of what is **live in production today** , not aspirational. Items on the roadmap are listed separately on the next page.

1. **Encryption in transit** — LIVE
   TLS 1.3 on all customer-facing endpoints; TLS 1.2+ for service-to-service traffic inside our VPC. HSTS enforced.

2. **Encryption at rest** — LIVE
   AES-256 on all customer pipeline data at the storage layer (platform-managed keys today; customer-managed keys on roadmap).

3. **Tenant isolation** — LIVE
   Logical isolation at the application and database tier; physical isolation available on the dedicated-tenant deployment option (see Page 3).

4. **Role-based access control (RBAC)** — LIVE
   Least-privilege by default. SSO/SAML and SCIM provisioning available on Enterprise. Internal access governed by named-engineer policy with audit logging.

5. **Zero-training LLM posture** — LIVE
   Forsyt uses Anthropic Claude via API with zero-retention, zero-training commercial terms. Customer prompts never enter foundation model weights.

6. **Audit logging** — LIVE
   Application-level audit logs for all customer-data access events; cloud audit trails for infrastructure-level events; retained per contract.

7. **Breach notification SLA** — LIVE
   Confirmed personal-data breaches notified to the controller and supervisory authority within 72 hours, per GDPR Art. 33.

8. **Sub-processor transparency** — LIVE
   Full sub-processor list published at forsyt.com/sub-processors; 30-day notice on additions or material changes.

DEPLOYMENT OPTIONS

Pick the tenancy model your security team needs.

Forsyt is delivered as managed SaaS by default, but procurement, regulated industries, and large enterprises often require stronger isolation. We support three deployment models, all share the same product surface and security controls.

OPTION	MULTI-TENANT (DEFAULT)	DEDICATED TENANT	PRIVATE VPC / ON-PREM
Application instance	Shared, logically isolated	Dedicated app + DB cluster	Deployed inside customer infra
Database	Shared cluster, tenant-keyed	Dedicated MongoDB cluster	Customer-managed DB
Encryption keys	Platform-managed	Platform-managed; CMK roadmap	Customer-managed
Data residency control	Region pinned at onboarding	Region pinned + isolated	Customer's own region
LLM inference	Anthropic API (zero-retention)	Anthropic in dedicated tenancy (optional)	Self-hosted model (subject to scoping)
Typical fit	Mid-market & growth-stage	Regulated / F500	Banking, defense, sovereign data
Mutual NDA before scoping	✓	✓	✓

MUTUAL NDA ON FILE BEFORE ANY SECURITY REVIEW

Sign before we share anything sensitive.

Before a security questionnaire, architecture deep-dive, or any artifact beyond what is already public on forsyt.com/security, Forsyt signs a mutual NDA with your legal team. Request the NDA template from **legal@forsyt.com**, countersigned within one business day.

WHERE YOUR DATA LIVES

Three regions. Pinned at onboarding. Contractually fixed.

Customer pipeline data never leaves the region you choose. Region selection happens during onboarding and is locked into your Order Form, we cannot change it without your written consent.

EUROPEAN UNION

Frankfurt

EU/UK customers default here. Anthropic EU residency available on request.

INDIA & APAC

Mumbai

Indian and APAC customers default here. India data-residency on the SOC 2 roadmap.

NORTH AMERICA

Virginia

Available on request for North American customers.

How we handle your data

- **Zero training.** Your prompts, calls, and CRM data are never used to train any foundation model.
- **Granular retention.** Per-tenant retention windows configurable in the Order Form. AI conversation context is in-memory only; discarded at session end.
- **Deletion on termination.** All customer data deleted within 30 days of contract end. Signed deletion certificate available on request.
- **Auditability.** Every AI answer cites its sources (calls, emails, CRM records) for human verification.
- **Data subject requests.** Forsyt assists you (the controller) within 5 business days for export, rectification, or erasure requests.

COMPLIANCE POSTURE

What we have today. What we're building. No security theater.

We publish what's live, what's in flight, and what's not on the roadmap yet, so your team can size the gap honestly during procurement.

✓

In place today

- ISO 27001 aligned ISMS
- GDPR posture
- TLS 1.3 in transit
- AES-256 at rest
- RBAC + least privilege
- Tenant data isolation
- Zero-training LLM
- DPA available on request
- Mutual NDA template
- Sub-processor disclosure
- 72-hour breach notification
- 30-day deletion on termination

~

On the roadmap

- SOC 2 Type II
- Annual third-party pen test
- Customer-managed encryption keys
- Public status page
- India data-residency formalization
- SOC 2 readiness audit

Status updates published quarterly at **forsyt.com/security** with the latest sub-processor list and roadmap progress.

Documents available on request

N

Mutual NDA

Standard Forsyt template; countersigned within 1 business day. Required before any sensitive disclosure. **legal@forsyt.com**

D

DPA

Data Processing Addendum with SCCs for non-EEA transfers. Aligned to GDPR Art. 28. **privacy@forsyt.com**

Q

Security questionnaire

Pre-filled SIG Lite / CAIQ Lite responses. Custom questionnaires turned around in 5 business days. **security@forsyt.com**

THE AI QUESTIONS EVERY MODERN SECURITY REVIEW NOW ASKS

AI is the new attack surface. Here's how we handle it.

- **Model provider:** Anthropic Claude (Sonnet family) via API. Chosen specifically for zero-training commercial terms, EU residency, public DPA, and EU AI Act alignment.
- **No cross-tenant data exposure:** Prompts include only your tenant's context. Anthropic does not train on customer API prompts.
- **Source citation on every AI output:** Every AI-generated insight cites the underlying call, email, or CRM event with timestamp.
- **Human-in-the-loop for material decisions:** Status changes and close-date pushes are always confirmed by a human before being written back to CRM.
- **Enterprise option, co-locate the model:** Anthropic in a dedicated cloud tenancy, or self-hosted open-source models inside your infrastructure, are scopeable for Enterprise contracts.

Incident response

Forsyt operates a documented incident-response runbook covering detection, containment, eradication, recovery, and lessons-learned. Confirmed personal-data breaches are notified to the controller and the relevant supervisory authority within **72 hours** of confirmed awareness, per GDPR Art. 33. Detection is powered by cloud audit trails, network flow logs, identity anomaly alerts, application audit logs, and dependency-scan alerts. No customer-impacting security incidents to date.

WHO TO CONTACT

One inbox per topic. Always a human reply.

security@forsyt.com: questionnaires, architecture, vuln reports
privacy@forsyt.com: DPA, data subject requests, GDPR
legal@forsyt.com: NDA, MSA, contracting

Trust Center: **forsyt.com/security** · Sub-processors: **forsyt.com/sub-processors**