title: Security — FastYoke summary: Executive summary of how FastYoke protects PII — tenant isolation, encryption, access control, auditability, and operational security. order: 4

SECURITY

How FastYoke protects PII

> *Per-tenant database isolation. Opt-in field-level encryption. Append-only audit trail. Designed for the regulated workloads your customers trust you with. Evaluating FastYoke for enterprise procurement? Start at the **Enterprise overview**.*

The one-sentence posture

FastYoke treats PII as **opt-in opaque-by-default** — every tenant's data lives in its own database file, isolation is enforced at the operating-system layer, and the PII / SPI encryption add-on closes the loop with per-tenant AES-256-GCM keys that the platform itself cannot read without an authorized request.

Download

A printable version of this summary is available for security committees and procurement reviews:

- **Download the FastYoke PII security summary (PDF)** — same content as this page, formatted for review packets.
- **Download the FastYoke VPAT 2.5 (PDF)** — accessibility conformance report (WCAG 2.1, Section 508, EN 301 549), auto-regenerated from the live axe coverage and engineer attestation.

What FastYoke counts as PII

The platform treats the following classes of data as in scope for the PII protections described below:

- **Tenant-tagged fields.** Any entity-payload or form-field schema marked `is_pii` (or `is_spi` for sensitive personal information). Tenants decide what's tagged — defaults to *nothing tagged* so opt-in is deliberate.
- **CRM contact records.** Names, emails, phone numbers, addresses, notes — by their nature.
- **Form submission entries** carrying email, phone, SSN, financial account, government ID, or freeform notes likely to contain PII.
- **E-signature signer identity** — the email, IP, signed-at timestamp, and signer chain captured by the e-sign envelope flow.
- **Audit-trail rows** that incidentally carry tenant-identifying information (event log, journal-entry actor, transition events).

Data in scope is governed by the controls in the next section. Data not in scope (e.g., aggregate metrics, public marketplace listings) is held to FastYoke's general security baseline but not the PII-specific controls.

The five-control posture

1. Tenant isolation — at the operating-system layer

Every tenant gets its **own SQLite database file**. There is no `WHERE tenant_id = ?` clause that the database falls back on for isolation — wrong-tenant access is *mechanically impossible* because it would require opening the wrong file.

This is the architectural foundation. Application bugs cannot leak cross-tenant data because the application never has both tenants' files open at the same time.

2. Encryption — three layers, customer-tunable

- **In transit.** All traffic is served over TLS. There is no plaintext path for tenant data over the network.
- **At rest, infrastructure.** Production database volumes are encrypted at rest at the hosting layer (Fly.io managed encryption).
- **At rest, field-level (optional).** The **PII / SPI Field Encryption add-on** ($19/month, available on every tier from Solo and above) encrypts tagged fields under **per-tenant data keys (AES-256-GCM)** wrapped under a platform key. Tagged values are decrypted only when read by an authorized request — they are intentionally opaque to filter / sort / search.

The field-level layer means even a platform administrator with database access cannot read tagged values without going through the authorized read path.

3. Access control — RBAC + scopes + hard refusals

- **Role-based access control.** A 72-permission catalog. Every API endpoint and every UI surface gates on permissions, not on a tenant admin's identity. Authoring once means the permission you grant a PAT means the same thing if you ever ship an extension.

- **Personal Access Tokens (PATs).** Long-lived `fy_pat_` tokens are minted with explicit scopes. The platform issues **hard refusals** — `delegated_credential_refused` — when a token tries to act outside its scopes, even if the underlying user could.
- **WorkOS AuthKit / SSO.** SSO via WorkOS for organizations that require it. The callback resolves tenant by workspace assignment, not by email-domain guessing.
- **Strategic Partner consent.** Partners providing implementation support reach a tenant only while a **per-tenant consent grant** is in place; revocation stops access on the next request.

4. Auditability — append-only by design

- **Immutable event log.** Every state change on every entity is recorded as an append-only event-log row. No `UPDATE` or `DELETE` is ever issued. The audit log is the platform's contractual truth.
- **Sealed-PDF evidence.** The General Ledger detail report (and any other auditable artifact) can be exported as a **sealed PDF** signed with ed25519. The seal is verifiable via a public endpoint — no FastYoke involvement required for an external auditor to confirm authenticity.
- **Posted journal entries are immutable.** Reversals are new entries; the original survives. GAAP-aligned by construction.
- **Role-change audit.** Every grant, revoke, and downgrade of an admin role is recorded with actor + timestamp + reason. Exportable for review.

5. Operational security — incident response + dependency hygiene

- **Vulnerability disclosure.** `security@fastyoke.io` with a 24-hour acknowledgement SLA.
- **Dependency scanning.** Dependabot + `gitleaks` (committed-secret detection) + `npm audit` + `cargo deny` run on every PR. Supply-chain advisories block merge until triaged.
- **Incident response plan.** Documented procedures for breach detection, customer notification, and post-incident review.
- **Backups.** Continuous backup via Litestream to S3-compatible cold storage. Backup encryption inherits volume encryption.
- **Region pinning** (Enterprise+). Tenants with data-residency obligations can pin their tenant to a specific Fly.io region or region group.

Customer responsibility — the shared model

Some controls are yours, not ours. The boundary is:

FASTYOKE DOES	CUSTOMER DOES
Provides per-tenant isolation, infra encryption, RBAC catalog, audit log, sealed-PDF export, optional field-level encryption	Decides which fields get the `is_pii` tag
Operates the production stack, monitors for incidents, runs vuln scanning	Configures SSO + 2FA on operator accounts
Offers the HIPAA add-on, region pinning, dedicated SLA	Signs the Business Associate Agreement before processing PHI; opts into region pinning for residency obligations
Holds the platform-level keys for encryption-at-rest	Chooses which third-party integrations process tenant data through the platform
Maintains the public subprocessor list and notifies on changes	Reviews the subprocessor list and approves it for the customer's compliance regime

Subprocessors

FastYoke uses a small list of carefully selected third parties to operate the platform. The complete list — including service, region, DPA status, and certification posture — is published at:

- **FastYoke Subprocessor List**

New subprocessor additions are announced in advance per our contractual commitments. Customers may flag concerns at `security@fastyoke.io` before the addition takes effect.

Formal attestations

ATTESTATION	STATUS
VPAT 2.5 (accessibility)	Current — download the PDF, regenerated on every release from live axe coverage + engineer attestation.
SOC 2 Type II	Roadmap — readiness assessment complete; controls operating; audit engagement scheduled. Bridge letter available on request.
HIPAA posture	Available — BAA executed on Enterprise / ISV+ tier with the HIPAA add-on. PHI processed under documented administrative + technical safeguards.
GDPR readiness	Current — DPA available, data-subject rights honored, EU region pinning available.

ATTESTATION	STATUS
PCI DSS	Not in scope — FastYoke does not store cardholder data. Payment processing routes through Stripe (PCI DSS Level 1).

For pre-audit security reviews or procurement questionnaires, contact `security@fastyoke.io` with your specific framework and timeline.

Related reading: Running your code — safely, at native speed: why FastYoke chose WebAssembly — the sandboxing model behind the guard-evaluation control described above.

Contact + disclosure

- **Vulnerability reports:** `security@fastyoke.io` — 24-hour acknowledgement SLA.
- **Security questionnaires + procurement:** `security@fastyoke.io`.
- **Status + recently-patched issues:** Security fixes log.
- **Full technical Trust Center** (for engineers + builders): /docs/security/trust-center.

We disclose material security issues with the same discipline we ask of our customers — facts, no hand-waving, and a clear remediation path. We're a small team and we own this.

Last reviewed: 2026-06-26. This page is updated on every material change to the platform's PII handling.