TAKTLY

SECURITY QUESTIONNAIRE - PRE-FILL

Procurement-ready answers for SIG Lite, HECVAT, CAIQ Full.

HOW TO USE THIS

Procurement teams: copy the answers below into your standard SIG Lite / HECVAT / CAIQ Full template. The structure mirrors the SIG question domains. Anything marked [In progress] reflects current status as of issue date; check gettaktly.com/trust for live updates.

ISSUE DATE

April 28, 2026

VENDOR CONTACT

Vernon Lee, Founder, Taktly hello@gettaktly.com

SOURCE DOCUMENTS

DPA: gettaktly.com/taktly-dpa.pdf | CAIQ-Lite: gettaktly.com/taktly-security-questionnaire.pdf | Trust + Operations: gettaktly.com/trust + gettaktly.com/trust/operations

1. Vendor Profile

1.1 Legal name and entity type
Taktly, sole-proprietor SaaS operated by Vernon Lee. Incorporation status available on request under MSA.

1.2 Headquarters location
United States.

1.3 Year founded
2025.

1.4 Number of employees
1 (founder-operator) backed by managed cloud infrastructure providers.

1.5 Customer count + segment
Early-stage. Founding ambassador program with mid-market practitioners. Reference customers available under NDA upon request once first design partner deals close.

1.6 Revenue range
Early-stage. Disclosable under NDA in MSA discussions.

1.7 Cyber liability insurance
[In progress] $1M coverage in process. Certificate published on gettaktly.com/trust upon issue.

1.8 Vendor risk score / financial rating
Available on request once first reference customer engages procurement.

2. Infrastructure & Hosting

2.1 Hosting model
Multi-tenant SaaS on managed cloud. Single-tenant-per-organization with logical isolation enforced by Postgres Row-Level Security policies.

2.2 Application hosting
Vercel (us-east-1 primary, global edge cache). Vercel attestations: SOC 2 Type II, ISO 27001, PCI-DSS Level 1.

2.3 Database hosting
Supabase managed Postgres (us-east-1). Supabase attestations: SOC 2 Type II, HIPAA-eligible.

2.4 File storage
Supabase Storage (S3-compatible, AES-256 at rest).

2.5 Geographic data residency
United States by default (us-east-1). EU residency available on request for Enterprise customers (contact required for confirmation).

2.6 On-premises / VPC deployment
Not currently offered. Roadmap consideration for Enterprise customers with defined classification requirements.

2.7 Subprocessor list
Supabase, Vercel, Stripe, Resend, OpenAI. Full list with purposes + regions: gettaktly.com/trust.

3. Encryption & Key Management

3.1 Encryption at rest
AES-256, managed by Supabase. Customer data is never stored outside encrypted storage.

3.2 Encryption in transit
TLS 1.2+ exclusively. HSTS enabled on the application. Modern cipher suites only; legacy SSL/TLS disabled.

3.3 Key management
Provider-managed keys (Supabase + Vercel). Customer-managed keys (BYOK / HSM integration) not currently supported.

3.4 Key rotation
Per provider policy: Supabase rotates infrastructure keys per their SOC 2 control matrix; Vercel rotates TLS certs automatically through Let's Encrypt + their managed certificate infrastructure.

3.5 Application secrets
Stored in Vercel environment variables (encrypted). Never committed to source control. Service-role keys never exposed to browser.

3.6 Customer credential storage
Passwords bcrypt-hashed via Supabase Auth. Taktly never sees plaintext passwords.

4. Access Control & Authentication

4.1 Authentication method (current)
Email + password via Supabase Auth. MFA available per-user on request.

4.2 SAML 2.0 SSO
[In progress] Available for Enterprise tier. Supports Okta, Azure AD, Ping Identity, OneLogin. Configure via per-org admin console.

4.3 SCIM 2.0 auto-provisioning
[In progress] Available for Enterprise tier alongside SAML SSO.

4.4 RBAC
Six roles: OrgAdmin, SiteAdmin, Reviewer, Editor, Operator, Auditor. Per-role permission matrix enforced at API + Postgres RLS layer.

4.5 Multi-tenancy isolation
Organization model with org_members table + Row-Level Security policies tied to auth.uid() and org membership. No cross-org data access possible.

4.6 Privileged access (Taktly side)
Single founder-administrator with break-glass access to production. Documented in BCP. Access logs retained 30 days.

4.7 Session controls
Idle timeout, session expiry, and IP allowlist available at Enterprise tier on request.

4.8 Account lifecycle
Self-service signup. SCIM-driven provisioning + deprovisioning at Enterprise. Manual deprovisioning honored within 24 hours of request.

5. Application Security

5.1 Secure SDLC
All changes flow through Git + GitHub PR review + CI checks (TypeScript strict, parity tests). Production deploy is the same code that passed CI.

5.2 Static analysis
TypeScript strict mode enforces type safety. ESLint configured with Next.js rules. No use of unsafe-inline / eval at the application level.

5.3 Dependency management
Dependencies pinned in package.json + lockfile. Renovate / Dependabot-class monitoring planned.

5.4 Penetration testing
[In progress] Annual external penetration test scheduled. Executive summary available under NDA after first test completes.

5.5 Web application firewall
Provided by Vercel edge layer (request rate-limiting, basic OWASP coverage).

5.6 OWASP Top 10 controls
Parameterized queries (Postgres + Supabase client). CSRF tokens on state-changing endpoints. Output encoding (React) by default. CSP headers configured at Vercel layer.

5.7 Vulnerability disclosure
security@gettaktly.com monitored daily. Responsible disclosure honored. No legal action against good-faith researchers. Public bug bounty in roadmap.

6. Data Handling & Privacy

6.1 Categories of personal data processed
Identification (name, email, role); Account credentials (bcrypt-hashed); Project content (free-form text + uploaded files); Audit/log metadata (IP, user-agent, timestamps).

6.2 Lawful basis for processing
Performance of contract (MSA) + legitimate interest (security, fraud prevention). GDPR-aligned DPA available.

6.3 Data subject rights
Access, rectification, deletion, portability, objection. Honored within 30 days. Self-service export per project; org-wide export at Enterprise tier.

6.4 Data retention
Active accounts: indefinite (subject to contract). Closed accounts: 90 days then deleted. Backups: 7 days standard, 30 days Enterprise. Audit logs: 12 months.

6.5 Data deletion / right to erasure
Self-service deletion in admin console; full deletion confirmed within 30 days. Backups age out within 30 days.

6.6 Cross-border data transfer
EU/UK SCCs included in DPA. Standard transfer mechanisms.

6.7 Use of customer data for AI training
Never. Customer text sent to OpenAI for LLM-assist is single-shot inference, retained for up to 30 days for abuse monitoring per OpenAI policy, then deleted. Never used to train any model.

6.8 Data classification
Customer treats project content as their own data classification level. Taktly does not impose a classification scheme.

6.9 Privacy Officer / DPO
[On request] Designated Privacy Contact named in MSA. Formal DPO appointment when EU customer base requires.

7. Availability & Resilience

7.1 Uptime target
Pro: 99.5% per calendar month. Enterprise: 99.9% per calendar month with service credits.

7.2 Service credits
Enterprise: 10% credit if monthly uptime <99.9%, 25% if <99.0%, 50% if <95.0%. Applied to next invoice.

7.3 RTO / RPO
RTO 4 hours, RPO 1 hour. See gettaktly.com/trust/operations#dr.

7.4 Backup frequency
Continuous WAL archive + daily full snapshot via Supabase managed backup. 7-day retention standard, 30-day Enterprise.

7.5 Disaster recovery testing
Quarterly full-stack restore drill into staging environment.

7.6 Business continuity plan
Documented at gettaktly.com/trust/operations#bcp. Continuity contact named in MSA at signing.

7.7 Incident response
NIST 800-61-aligned. Severity classification + notification timelines published at gettaktly.com/trust/operations#irp. 72-hour breach notification per GDPR.

8. Compliance & Certifications

8.1 SOC 2
[In progress] Type II evidence collection underway with a top SOC 2 platform. Type I letter available on request once issued. Target Type II completion: 12 months.

8.2 ISO 27001
Not currently certified. Roadmap consideration for years 2-3.

8.3 HIPAA
BAA available on request for healthcare-bound deployments. Subprocessor (Supabase) is HIPAA-eligible.

8.4 GDPR
DPA with EU/UK Standard Contractual Clauses available. 72-hour breach notification. Data subject rights honored within 30 days.

8.5 21 CFR Part 11 (FDA)
[In progress] Multi-user approval workflows + immutable audit trail in place. Full Part 11 conformance requires IQ/OQ/PQ validation package, scheduled for GxP-bound deployments.

8.6 PCI-DSS
Not in scope - Stripe handles all payment data; Taktly never touches card data. Stripe is PCI-DSS Level 1.

8.7 FedRAMP
Not in scope. Federal customers contact for tailored deployment options.

8.8 Industry-specific (FSMA, MDR, ICH Q7)
Taktly is industry-aware (22 industry profiles + 8 contamination modules) but is not a validated GxP / FSMA / MDR system. Position as documentation + decision-support tool, not system of record.

9. Integration & Interoperability

9.1 API
[Roadmap Q2] REST API for read access to projects, signatures, audit log. Webhooks for project events.

9.2 Data export
Per-project JSON export available today. Org-wide bulk XLSX/CSV export at Enterprise tier.

9.3 Identity provider integration
[In progress] SAML 2.0 SSO + SCIM 2.0 at Enterprise tier.

9.4 SIEM integration
Audit log export to JSON/CSV today; native syslog / S3 forwarding on roadmap for Enterprise.

9.5 QMS integration (Veeva, MasterControl, TrackWise, EtQ)
Not currently integrated. API-based bridge possible at Enterprise tier on request.

9.6 Single sign-out
Supported via SAML SLO when SSO is configured.

10. Operations & Support

10.1 Support hours
Email support 24x7 best-effort. Enterprise tier: 24x7 critical-incident response within 1 hour.

10.2 Support contact
hello@gettaktly.com (general) | security@gettaktly.com (security) | named CSM at Enterprise tier.

10.3 Onboarding
Self-service for Solo/Pro/Team. Dedicated onboarding for Enterprise (typical: 1-2 weeks of structured rollout).

10.4 Customer success
Founder-direct today. Formalized Customer Success function at first Enterprise deal.

10.5 Service status page
[In progress] gettaktly.com/status (aggregating Vercel + Supabase upstream feeds).

10.6 Change management
Production deploys via Git + Vercel. Customer-impacting changes communicated via email + changelog. Breaking changes require 30-day notice for Enterprise customers.

Closing

HONEST POSITIONING

Taktly is an early-stage product with a category-of-one intelligence layer (TAKTLY-001 - single intelligence source across workspace, bubble, and exports), wrapped in pre-enterprise operational infrastructure that is actively being upgraded. We do not over-claim. We disclose what is in progress versus what is live, and we welcome procurement scrutiny - that is what builds the right kind of customer relationships.

WHAT WE WILL NEGOTIATE IN MSA

Vendor audit rights; named DPO if required; custom data retention; specific subprocessor approvals; SLA credits; Part 11-related contractual commitments; deletion confirmations.

WHAT WE WILL NOT DO

Train any model on customer data. Sell or share customer data. Operate without an MSA + DPA. Ship a feature that we have not actually built. Claim a certification we have not earned.

For live status of any in-progress item above, see gettaktly.com/trust. For procurement-grade operational documents (SLA, BCP, DRP, IRP, architecture diagram, data-flow diagram), see gettaktly.com/trust/operations.

Vernon Lee, Founder, Taktly | hello@gettaktly.com