



SUB-PROCESSOR LIST & SECURITY TRUST POLICY

Transparency & Security Commitments

Version 1.0 | Effective June 10, 2026

A software product of Violet Organization, a 501(c)(3) non-profit organization

EIN: 81-3855319

TABLE OF CONTENTS

- I. Part A — Sub-Processor List
- II. Part B — Security & Trust Policy

www.scantra.ai | Info@scantra.ai

c/o Violet Organization, a 501(c)(3) non-profit organization (EIN: 81-3855319), 210 Lake Dr E, Cherry Hill, NJ 08002

SUB-PROCESSOR LIST

Third Parties Processing Client Data on Scantra's Behalf

Effective Date: June 10, 2026

Scantra.ai DBA Scantra engages the following Sub-Processors who may have access to or process personal data in connection with the Services. All Sub-Processors are reviewed for privacy and security compliance.

Last Updated: June 10, 2026

Section I. INFRASTRUCTURE & HOSTING

Sub-Processor	Location	Purpose	Data Transferred
Amazon Web Services (AWS)	USA / Global	Cloud hosting & infrastructure	All platform data
Cloudflare	USA / Global	CDN, DDoS protection, DNS	IP addresses, traffic data
[Primary Database Provider]	USA	Database hosting	All stored client data

Section II. PAYMENT PROCESSING

Sub-Processor	Location	Purpose	Data Transferred
Stripe, Inc.	USA	Payment processing & billing	Payment card data, billing info

Section III. COMMUNICATIONS & SUPPORT

Sub-Processor	Location	Purpose	Data Transferred
[Email Service Provider]	USA	Transactional & marketing email	Email address, name
[Support Platform]	USA	Customer support ticketing	Account info, support content
[Live Chat Provider]	USA	Live chat support	Chat data, email

Section IV. ANALYTICS & MONITORING

Sub-Processor	Location	Purpose	Data Transferred
Google Analytics	USA	Website analytics	Anonymized usage data
[Uptime Monitoring]	USA	Service availability monitoring	System metrics
[Error Tracking]	USA	Application error tracking	Error logs, IP addresses

Section V. THIRD-PARTY DATA SOURCES

Sub-Processor	Location	Purpose	Data Transferred
Google APIs (Search Console, Analytics)	USA	SEO data retrieval	Client-authorized account data
[Backlink Data Provider]	_____	Backlink index data	Domain/URL data
[Keyword Data Provider]	_____	Keyword & SERP data	Query & ranking data

Section VI. SUB-PROCESSOR CHANGES

We notify Clients at least 30 days before adding or replacing any Sub-Processor. The current list is always available at www.scantra.ai/sub-processors. Questions: Info@scantra.ai

* * *



Copyright 2026 Violet Organization, a 501(c)(3) non-profit organization. All rights reserved.

SECURITY & TRUST POLICY

Our Commitment to Protecting Your Data

Effective Date: June 10, 2026

Scantra.ai DBA Scantra takes the security of Client data seriously. This policy describes our security program, practices, certifications, and how we respond to security issues.

Section I. TECHNICAL SECURITY CONTROLS

Control	Implementation
Encryption in Transit	TLS 1.2+ enforced; HSTS enabled
Encryption at Rest	AES-256 on all stored data and backups
Authentication	MFA required for all staff
Access Control	RBAC; least privilege principle
Vulnerability Management	Annual penetration testing; automated scanning
Logging & Monitoring	Centralized SIEM; 12-month log retention
Backup & Recovery	Daily backups; 30-day retention; quarterly restore tests
DDoS Protection	Cloudflare enterprise-grade mitigation

Section II. ORGANIZATIONAL CONTROLS

- Background checks for all employees and contractors with data access
- Annual security awareness training mandatory for all staff
- Vendor security assessments before engaging new Sub-Processors
- Documented information security policies reviewed annually

Section III. COMPLIANCE

Framework	Status
GDPR / UK GDPR	Compliant — DPA available
CCPA / CPRA	Compliant
LGPD (Brazil)	Compliant — DPA available

Framework	Status
PIPEDA (Canada)	Compliant
Australian Privacy Act	Compliant
SOC 2 Type II	[In progress / Certified]
ISO 27001	[In progress / Certified]

Section IV. INCIDENT RESPONSE

- Containment actions within 1 hour of P1 incident detection
- Affected Clients notified within 48 hours of confirmed impact
- GDPR/LGPD regulatory notifications within 72 hours
- Post-incident report published within 5 business days

Section V. VULNERABILITY DISCLOSURE

Report security issues to Support@scantra.ai — Subject: "Security Vulnerability Report."

- We acknowledge reports within 5 business days
- 90-day coordinated disclosure window before public release
- We do not pursue legal action against good-faith researchers

Section VI. CONTACT

Security questions: Support@scantra.ai | c/o Violet Organization, a 501(c)(3) non-profit organization (EIN: 81-3855319), 210 Lake Dr E, Cherry Hill, NJ 08002

* * *



Copyright 2026 Violet Organization, a 501(c)(3) non-profit organization. All rights reserved.