SALESZ LLC dba Stratalize

Data Processing Agreement

Version 1.0 — Effective May 2, 2026

This Data Processing Agreement ("DPA") is entered into between SALESZ LLC, a Florida limited liability company doing business as Stratalize ("Processor"), and the Customer identified in the applicable Order Form or subscription agreement ("Controller").
This DPA is incorporated into and forms part of the Stratalize Terms of Service. Capitalized terms not defined herein have the meanings given in the Terms of Service.

ARTICLE 1 — DEFINITIONS

"Applicable Data Protection Law" means all laws and regulations applicable to the processing of Personal Data under this DPA, including without limitation the GDPR, UK GDPR, CCPA/CPRA, and other applicable state and international privacy laws.
"Data Subject" means an identified or identifiable natural person to whom Personal Data relates.
"EEA" means the European Economic Area.
"GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council.
"Personal Data" means any information relating to an identified or identifiable natural person that is processed by Processor on behalf of Controller in connection with the Platform.
"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.
"Processing" has the meaning given under the GDPR and "process" and "processed" shall be construed accordingly.
"Standard Contractual Clauses" or "SCCs" means the standard contractual clauses for the transfer of personal data to third countries pursuant to Commission Decision (EU) 2021/914.
"Sub-processor" means any third party engaged by Processor to process Personal Data on behalf of Controller.

ARTICLE 2 — ROLES AND SCOPE

2.1 Controller and Processor

The parties acknowledge that Controller is the data controller and Processor is the data processor with respect to Personal Data processed under the Platform.

2.2 Processor's Obligations

Processor shall process Personal Data only:
(a) On behalf of and in accordance with Controller's documented instructions, including as set out in this DPA and the Terms of Service;
(b) For the purposes of providing the Platform and related services; and
(c) As otherwise required by Applicable Data Protection Law, in which case Processor shall notify Controller before such processing unless prohibited by law.

2.3 Controller's Instructions

Controller's instructions are documented in the Terms of Service and this DPA. Controller may provide additional instructions in writing, which Processor shall follow if technically and legally feasible.

2.4 Details of Processing

The subject matter, duration, nature, purpose, type of Personal Data, and categories of Data Subjects processed under this DPA are described in Schedule 1 (Description of Processing Activities).

ARTICLE 3 — PROCESSOR'S OBLIGATIONS

3.1 Confidentiality

Processor shall ensure that persons authorized to process Personal Data are under appropriate obligations of confidentiality.

3.2 Security

Processor shall implement and maintain appropriate technical and organizational measures to protect Personal Data against unauthorized or unlawful processing and against accidental loss, destruction, damage, or disclosure, as further described in Schedule 2 (Technical and Organizational Measures).

3.3 Sub-processors

Processor shall:
(a) Not engage Sub-processors without general written authorization from Controller (which Controller provides by entering into this DPA with respect to the Sub-processors listed in Schedule 3);
(b) Impose data protection obligations on Sub-processors substantially equivalent to those in this DPA;
(c) Notify Controller of any intended addition or replacement of Sub-processors with at least 30 days' advance notice, providing Controller the opportunity to object on reasonable grounds related to data protection;
(d) Remain fully liable to Controller for the acts and omissions of Sub-processors to the same extent as if Processor had performed the processing directly.

3.4 Data Subject Rights

Processor shall promptly notify Controller of any Data Subject requests received directly by Processor and shall not respond to such requests without Controller's authorization, except to inform the Data Subject that the request has been received and is being handled by Controller.

3.5 Assistance

Processor shall provide reasonable assistance to Controller in fulfilling its obligations under Applicable Data Protection Law with respect to:
(a) Responding to Data Subject rights requests;
(b) Conducting Data Protection Impact Assessments (DPIAs);
(c) Prior consultation with supervisory authorities;
(d) Data breach notification.

3.6 Breach Notification

Processor shall notify Controller without undue delay, and in any event within 48 hours, after becoming aware of a Personal Data Breach. Such notification shall describe: (a) the nature of the breach; (b) the categories and approximate number of Data Subjects and Personal Data records concerned; (c) the likely consequences; and (d) measures taken or proposed to address the breach.

3.7 Deletion or Return

Upon termination of the Platform subscription or upon Controller's request, Processor shall delete or return all Personal Data within 90 days, unless retention is required by Applicable Data Protection Law. Processor shall provide written certification of deletion upon request.

3.8 Audits

Upon written request (with at least 30 days' notice and no more than once per 12-month period), Processor shall make available to Controller information reasonably necessary to demonstrate compliance with this DPA and allow for and contribute to audits conducted by Controller or an independent auditor appointed by Controller, subject to reasonable confidentiality obligations.

ARTICLE 4 — INTERNATIONAL DATA TRANSFERS

4.1 EEA Transfers

If Controller is subject to GDPR and Personal Data is transferred from the EEA to a third country that has not been deemed to provide adequate protection, such transfers shall be subject to Standard Contractual Clauses (Module Two: Controller to Processor) as set out in Commission Decision (EU) 2021/914, which are hereby

incorporated by reference.

4.2 UK Transfers

For transfers from the United Kingdom, the International Data Transfer Addendum (IDTA) issued by the UK Information Commissioner's Office shall apply.

4.3 Transfer Impact Assessments

Processor shall cooperate with Controller in conducting Transfer Impact Assessments as required by Applicable Data Protection Law.

ARTICLE 5 — GOVERNING LAW

This DPA shall be governed by the laws of the State of Florida, unless otherwise required by Applicable Data Protection Law with respect to GDPR-related obligations, in which case EU law shall apply to those obligations.

SCHEDULE 1 — DESCRIPTION OF PROCESSING ACTIVITIES

Subject matter: Provision of AI governance and intelligence services via the Stratalize platform.
Duration: For the term of the Subscription and for such period thereafter as required by Applicable Data Protection Law or as needed to fulfill post-termination obligations.

Nature of Processing:

- Collection, storage, and organization of account data
- Encryption and secure storage of integration credentials
- Ephemeral staging and immediate deletion of raw integration payloads following AI synthesis
- AI inference using third-party LLM APIs (Anthropic)
- Generation and cryptographic signing of intelligence outputs
- Maintenance of governance audit logs and data lineage records
- Usage analytics and error monitoring

Purpose: To provide the Customer with AI-powered intelligence, governance, and compliance capabilities for business decision-making in regulated industries.

Types of Personal Data:

- Organizational administrators and users: name, email address, job title, department, IP address, session data
- Data Subjects referenced in integration-derived context (e.g., employee data from HR integrations, patient identifiers from healthcare integrations): as submitted by Customer

Special Categories: Processor does not intentionally process special categories of personal data. Customer is responsible for not submitting special category data unless expressly permitted and documented.

Categories of Data Subjects:

- Customer's employees, administrators, and Authorized Users
- Third parties whose data appears in Customer's connected systems and is submitted to the Platform by Customer

SCHEDULE 2 — TECHNICAL AND ORGANIZATIONAL MEASURES

Processor implements the following technical and organizational security measures:

Encryption

- TLS 1.3 for all data in transit
- AES-256-GCM encryption for data at rest (Supabase)
- AES-256 application-layer encryption for integration credentials (OAuth tokens, webhook secrets)

- Ed25519 cryptographic signatures on all AI synthesis outputs

Access Controls

- Attribute-based and role-based access controls (ABAC/RBAC)
- Per-user OAuth credential isolation
- Multi-factor authentication support via SSO providers
- SCIM provisioning for enterprise identity management
- Four-eyes approval for AI-proposed write operations
- AI information barriers via per-user persona configuration

Audit and Logging

- Immutable, hash-chained audit logs for all governance events
- Data lineage records for each synthesis operation
- MCP request logging with organization and user context
- GDPR export logs and deletion request tracking

Operational Security

- Rate limiting and abuse detection
- Content Security Policy (CSP) and HSTS headers
- Sentry error monitoring with credential scrubbing
- Intrusion detection via Vercel platform controls
- Background job isolation via Inngest

Organizational Measures

- Confidentiality agreements with all personnel and contractors
- Security review for all third-party Sub-processors
- SOC 2 certification planned
- Incident response plan maintained internally
- Regular security reviews of integration and authentication paths

Data Minimization

- Raw integration payloads deleted after synthesis
- Structured logger allowlist prevents sensitive data in logs
- No raw integration data transmitted to analytics providers

SCHEDULE 3 — APPROVED SUB-PROCESSORS

Controller provides general authorization to Processor's engagement of the following Sub-processors:

Sub-processor: Supabase, Inc.
Purpose: Database and authentication infrastructure
Data Processed: All platform data including Personal Data
Location: US (EU region available on request)

Sub-processor: Anthropic PBC
Purpose: AI model inference via API
Data Processed: Prompts containing org-context and user queries
Location: United States

Sub-processor: OpenAI, LLC
Purpose: Embedding generation (RAG pipeline)
Data Processed: Text content from uploaded documents and data
Location: United States

Sub-processor: OpenRouter
Purpose: AI model gateway
Data Processed: Prompts routed to third-party models
Location: United States

Sub-processor: Vercel, Inc.
Purpose: Application hosting and serverless compute
Data Processed: HTTP traffic, logs, execution environment
Location: United States

Sub-processor: Stripe, Inc.
Purpose: Payment processing
Data Processed: Billing identifiers and payment metadata
Location: United States

Sub-processor: Resend, Inc.
Purpose: Transactional email
Data Processed: Email addresses, message content
Location: United States

Sub-processor: PostHog, Inc.
Purpose: Product analytics
Data Processed: User ID, org ID, subscription tier, usage events
Location: United States

Sub-processor: Sentry (Functional Software, Inc.)
Purpose: Error monitoring
Data Processed: Error contexts, request metadata (credentials scrubbed)
Location: United States

Sub-processor: Inngest, Inc.
Purpose: Background job orchestration
Data Processed: Job metadata including org_id and integration_id
Location: United States

Sub-processor: Upstash, Inc.
Purpose: Redis caching
Data Processed: Cached synthesis bundles and rate-limit data
Location: United States

Sub-processor: Plaid, Inc.
Purpose: Financial account linking
Data Processed: Financial account metadata (where Customer uses Plaid integration)
Location: United States

Sub-processor: Tavily AI
Purpose: Web search enrichment
Data Processed: Search queries for market data enrichment
Location: United States

Sub-processor: xpay.sh
Purpose: x402 payment settlement
Data Processed: Transaction hashes and settlement metadata
Location: United States

Processor shall provide 30 days' advance notice of any additions or replacements to this list.

CONTACT

To execute this DPA or request a countersigned copy, contact: privacy@stratalize.com

SALESZ LLC dba Stratalize

205 N Michigan Ave Suite 810, Chicago, IL 60601