DataObserv

Data Processing Agreement

Version 1.0 | Last Updated: June 26, 2026

This Data Processing Agreement ("DPA") forms part of the DataObserv Terms of Service or other written agreement (the "Agreement") between Zink Labs LLC, a Florida limited liability company, doing business as ("d/b/a") DataObserv ("Processor," "we," "us") and the customer organization that accepts it ("Controller," "Customer," "you"). It governs our processing of Customer Personal Data when you use the Service to monitor a data warehouse. By accepting the Agreement in-app or by using the Service, you agree to this DPA. Where this DPA conflicts with the Agreement on data protection, this DPA prevails.

1. Definitions

"Applicable Data Protection Law" means all privacy and data-protection laws applicable to the processing, including the EU GDPR, the UK GDPR, the California Consumer Privacy Act as amended (CCPA/CPRA), and the Florida Information Protection Act (FIPA, Fla. Stat. 501.171). "Controller," "Processor," "Data Subject," "Personal Data," "Processing," and "Personal Data Breach" have the meanings given in Applicable Data Protection Law. "Customer Personal Data" means Personal Data we process on your behalf under the Agreement, as described in Annex 1. "Sub-Processor" means a third party we engage to process Customer Personal Data.

2. Roles and Scope

As between the parties, you are the Controller and we are the Processor of Customer Personal Data. You are responsible for the accuracy and lawfulness of the data you make available to the Service and for having a valid legal basis to do so. We process Customer Personal Data only to provide and support the Service and only on your documented instructions, which consist of the Agreement, this DPA, your configuration of the Service, and your use of its features. We will inform you if, in our opinion, an instruction infringes Applicable Data Protection Law.

3. Processor Obligations

- Process Customer Personal Data only on documented instructions, including for international transfers, unless required by law (in which case we will inform you unless legally prohibited).
- Ensure personnel authorized to process Customer Personal Data are bound by confidentiality.
- Implement and maintain the technical and organizational measures in Annex 2.
- Not engage a Sub-Processor except as permitted by Section 6.
- Assist you, taking into account the nature of processing, in responding to Data Subject requests (Section 5) and in meeting your obligations regarding security, breach notification, data protection impact assessments, and consultation with supervisory authorities.
- At your choice, delete or return Customer Personal Data on termination as described in Section 8.

- Make available information necessary to demonstrate compliance and allow for audits as described in Section 9.

4. Confidentiality

We treat Customer Personal Data and your warehouse schema, table and column names, and query patterns as your Confidential Information and will not access or use them except to provide the Service, comply with law, or as you instruct.

5. Data Subject Requests

Taking into account the nature of the processing, we will assist you by appropriate technical and organizational measures, insofar as possible, to respond to requests from Data Subjects to exercise their rights. If we receive such a request directly, we will, where lawful, refer the Data Subject to you rather than respond ourselves.

6. Sub-Processors

You provide general authorization for us to engage the Sub-Processors listed in Annex 3 to process Customer Personal Data. We impose data-protection obligations on each Sub-Processor that are no less protective than those in this DPA and remain responsible for their performance. We will give you at least thirty (30) days' advance notice (by email or in-app) before adding or replacing a Sub-Processor, during which you may object on reasonable data-protection grounds; if we cannot reasonably accommodate your objection, you may terminate the affected Service.

7. Personal Data Breach

We will notify you without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a Personal Data Breach affecting Customer Personal Data, and will provide information reasonably available to us to help you meet your notification obligations. Where required, we will support notification under FIPA (Fla. Stat. 501.171), including to the Florida Department of Legal Affairs for breaches affecting 500 or more Florida residents.

8. Return and Deletion

On termination or expiry of the Agreement, or on your earlier written request, we will, at your choice, delete or return Customer Personal Data and delete existing copies, except to the extent we are required by law to retain it. Encrypted warehouse credentials are deleted when a connection is removed or the account is closed. Residual copies in routine backups are deleted on a rolling schedule (generally within 30 days). Computed metrics and metadata are deleted within a commercially reasonable period after termination.

9. Audit Rights and Evidence

We will make available to you information reasonably necessary to demonstrate compliance with this DPA, including, on request and subject to confidentiality, our then-current security documentation and responses to a reasonable security questionnaire, and any available third-party audit reports (e.g., SOC 2) once obtained. Where Applicable Data Protection Law grants you an audit right, you may, no more than once per year and on reasonable

prior notice, conduct an audit limited to information relevant to the processing, conducted so as not to disrupt our operations.

10. Processor Personnel Access to Your Workspace

Our support staff can access your organization's workspace only when you (an authorized administrator) explicitly grant temporary access. Such access is time-boxed, recorded with an expiry, can be revoked by you at any time, and is logged. We do not access your workspace as an administrator absent such a grant, except as necessary to maintain the Service or comply with law.

11. International Transfers

We process Customer Personal Data in the United States. For transfers of Personal Data from the EEA, UK, or Switzerland, the parties incorporate the European Commission's Standard Contractual Clauses (Module Two: Controller-to-Processor, and Module Three where we engage Sub-Processors) and the UK International Data Transfer Addendum, which are deemed executed by entry into this DPA. In case of conflict, the SCCs prevail over this DPA on transfer matters. Annex 1 supplies the information required by the SCC appendices; Annex 2 supplies the technical and organizational measures.

12. Liability and Governing Law

Each party's liability under this DPA is subject to the limitations and exclusions of liability in the Agreement. This DPA is governed by the laws of the State of Florida, consistent with the Agreement, except where Applicable Data Protection Law or the SCCs require otherwise.

Annex 1 — Details of Processing

Subject matter:

Provision of the DataObserv data-observability Service to the Controller.

Duration:

For the term of the Agreement, plus the return/deletion period in Section 8.

Nature and purpose:

Ingesting warehouse metadata and query history; computing freshness, volume, anomaly, schema-change, and cost metrics; optional opt-in column profiling; raising alerts; and providing optional AI-assisted insights over organization metadata.

Categories of Data Subjects:

The Controller's authorized users; and any individuals whose Personal Data the Controller's warehouse usernames or query text may identify or contain.

Categories of Personal Data:

Category	Examples	Source
Account & identity data	Name, email address, organization name, role, authentication identifiers.	Provided by you at sign-up.
Billing data	Billing contact, subscription tier, and the count of monitored tables used to meter usage. No card numbers (handled by Stripe).	Provided by you / generated by use.
Warehouse connection credentials	Account/host, username, and a secret (password or key-pair private key, access token, or service-account JSON). Encrypted at rest with AES-256-GCM; decrypted only inside the processing worker.	Provided by you when you connect a warehouse.
Warehouse metadata	Table and column names, row counts, byte sizes, retention settings, freshness timestamps, schema definitions, and computed freshness/volume/anomaly/cost metrics.	Read from your warehouse's metadata views.
Query history	Recent query text (truncated), executing warehouse usernames/roles, and per-query row/byte counts. Query text may contain values you placed in SQL; warehouse usernames identify your warehouse's users.	Read from your warehouse's query-history views.
Transiently-sampled column values	For columns you opt in to profile, a bounded sample of rows is read into worker memory to compute aggregate statistics. Only aggregates are stored (null/missing rates, string lengths, and numeric minimum/maximum/average/median — note numeric minimum and maximum are actual values from your data). Raw rows are not stored.	Sampled from your warehouse on profiling.

Sensitive data: The Service is not designed to process special-category data. The Controller is responsible for not directing monitoring or profiling at sensitive data without a lawful basis and for granting a least-privilege, read-scoped warehouse role.

Annex 2 — Technical and Organizational Measures

- **Encryption:** Warehouse credentials are encrypted at rest using AES-256-GCM; the decryption key is held only in the processing environment and credentials are redacted from logs.
- **Encryption in transit:** All data in transit is encrypted using TLS.
- **Least privilege:** The Service connects to your warehouse with a least-privilege, read-scoped role; it does not write to your warehouse.
- **Tenant isolation:** Row-Level Security enforces organization isolation across all multi-tenant data; access is role-based (owner / admin / member, plus restricted internal support access).
- **Access logging:** Administrative and security-relevant actions, including support-access grants, are logged.
- **Secret management:** Secrets are stored in managed secret stores; payment webhooks are signature-verified with replay protection.
- **Operational controls:** We maintain documented data-retention, incident-response, disaster-recovery, and key-rotation procedures.
- **Monitoring:** A security posture program tracks controls and findings against SOC 2 criteria.

Annex 3 — Authorized Sub-Processors

The following Sub-Processors are authorized to process Customer Personal Data to provide the Service. The Controller's own data warehouse is the Controller's system, read by the Processor, and is not a Sub-Processor.

Sub-Processor	Location	Purpose
Supabase, Inc.	United States	Application database (Postgres), authentication, storage, and edge functions; stores account data, tenant metadata, encrypted warehouse credentials, and computed observability metrics.
Amazon Web Services, Inc.	United States (us-east-1)	Cloud compute and storage for the data-pipeline orchestration; transiently processes sampled warehouse rows in worker memory; stores pipeline run state.
Vercel Inc.	United States	Frontend application hosting and content delivery; processes request metadata only.
Stripe, Inc.	United States	Subscription billing and payment processing; processes billing contact and subscription/usage data. No card data is stored by DataObserv (Stripe-hosted Checkout).
OpenRouter, Inc.	United States	Primary AI inference router for the in-app assistant and table-profiling; receives user prompts and organization metadata (table/column names, freshness, anomalies, alerts, cost, schema). Does not receive warehouse row data.
OpenAI, L.L.C.	United States	Text embeddings and assistant model fallback; receives schema-metadata text. Does not receive warehouse row data.
Anthropic, PBC	United States	AI model provider (table-profiling fallback); receives column names and types. Does not receive warehouse row data.
Resend (Plus Five Five, Inc.)	United States	Transactional email delivery (team invitations, notifications, verification); processes recipient email addresses.
Functional Software, Inc. (Sentry)	United States	Application error and performance monitoring; may process user/organization identifiers contained in error telemetry.
GitHub, Inc.	United States	Source-control and CI/CD; processes deployment metadata only.
Cloudflare, Inc.	United States	Network/DNS and edge security; processes request metadata in transit.