DataObserv

Privacy Policy

Version 1.0 | Last Updated: June 26, 2026

This Privacy Policy describes how Zink Labs LLC ("we," "us," or "our") collects, uses, and protects information in connection with DataObserv (the "Service"), a data-observability platform that monitors a customer's data warehouse. When you connect a warehouse, you (the customer organization) are the controller of the data in that warehouse and we act as a processor on your documented instructions; our Data Processing Agreement governs that relationship and prevails over this Policy where they conflict.

1. Who We Are

Zink Labs LLC, a Florida limited liability company, doing business as ("d/b/a") DataObserv, is the entity responsible for the Service. For privacy questions or to exercise your rights, contact us at privacy@dataobserv.dev.

2. Information We Process

The categories below reflect what the Service actually accesses and stores. We follow the principle of data minimization: the core monitoring reads warehouse metadata, not your business records, and column profiling is opt-in.

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.

Important — your responsibility as controller: you decide which tables and columns the Service monitors and profiles. Do not point profiling at columns containing personal or sensitive data unless you have a lawful basis to do so, and grant the Service a least-privilege, read-scoped warehouse role. Query text and warehouse usernames are read from your warehouse's history views and may contain identifiers; restrict the monitored role accordingly.

3. How We Use Information

- Provide the Service: ingest warehouse metadata; compute freshness, volume, anomaly, schema-change, and cost metrics; raise alerts.
- Operate your account: authentication, organization and team management, billing, and support.
- Power optional AI features: the in-app assistant and table-profiling send your prompts and organization metadata (table/column names, freshness, anomalies, alerts, cost, schema) to AI sub-processors. Warehouse row data is not sent to AI providers.
- Secure and improve the Service: error diagnostics, abuse prevention, and reliability monitoring.
- Comply with law and enforce our agreements.

We do not sell your personal information and we do not use it for advertising or cross-context behavioral profiling.

4. AI Processing and Model Training

Optional AI features route prompts and organization metadata to the AI sub-processors listed in Section 6. We do not authorize these providers to train their models on your data, and we configure these integrations to use providers' non-training / zero-retention options where available. AI output can be inaccurate; it is informational and you remain responsible for decisions you make based on it.

5. Legal Bases (EEA/UK)

- **Contract:**Performance of a contract — to provide the Service you signed up for.
- **Legitimate interests:**Operating, securing, and improving the Service, and direct B2B communications.
- **Consent:**Where required for optional features or communications.
- **Legal obligation:**To meet our legal and regulatory obligations.

6. Service Providers (Sub-Processors)

We share data with the vetted service providers below strictly to operate the Service. They process data on our instructions under contractual confidentiality and security obligations. Your warehouse remains your own system; we read it as a processor and do not list it as 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.

We maintain a current list and provide advance notice of new sub-processors as described in the Data Processing Agreement.

7. International Transfers

We and our sub-processors are located in the United States. If you access the Service from the EEA, UK, or Switzerland, your data is transferred to the United States under appropriate safeguards (Standard Contractual Clauses and the UK Addendum, as applicable), described further in the Data Processing Agreement.

8. Data Retention

We retain account and billing data for the life of your account and as required by law. Observability metadata and computed metrics are retained per your plan and configuration. Encrypted warehouse credentials are retained only while a connection is active. On termination, we delete or return your data as described in the Data Processing Agreement; backups expire on a rolling schedule.

9. Your Rights

Depending on your location, you may have rights to access, correct, delete, or port your personal data, to object to or restrict processing, and to withdraw consent. Where we process warehouse data as a processor, we will refer or assist requests to the relevant customer (controller). To exercise rights, contact privacy@dataobserv.dev. EEA/UK users may also lodge a complaint with their supervisory authority.

California residents (CCPA/CPRA): we do not sell or share personal information for cross-context behavioral advertising. Zink Labs LLC currently operates below CCPA/CPRA applicability thresholds; we nonetheless honor access and deletion requests as described above.

10. Security

We apply technical and organizational measures appropriate to the risk, including encryption of warehouse credentials at rest (AES-256-GCM), encryption in transit (TLS), least-privilege read-scoped warehouse access, row-level tenant isolation, access logging, secret management, and documented incident-response and disaster-recovery procedures. No method of transmission or storage is perfectly secure.

11. Personal-Data Breach Notification

If a personal-data breach affecting your data occurs, we will notify affected customers without undue delay and, where we act as processor, assist you in meeting your notification obligations. Where required by Florida law (FIPA, Fla. Stat. 501.171), we will provide notice to individuals and, for breaches affecting 500 or more Florida residents, to the Florida Department of Legal Affairs within the statutory timeframe.

12. Children

The Service is a business tool not directed to individuals under 18, and we do not knowingly collect personal data from children.

13. Changes to This Policy

We may update this Policy. The "Last Updated" date above reflects the latest revision; material changes will be communicated as required by law and your continued use constitutes acceptance.

14. Contact Us

Zink Labs LLC

Privacy: privacy@dataobserv.dev

Security: security@dataobserv.dev

Web: https://dataobserv.dev