Data Processing Agreement

Kestra Labs LLC • Last Updated: March 1, 2026

This Data Processing Agreement ("DPA") is entered into between the Customer ("Data Controller") and Kestra Labs LLC ("Data Processor") and supplements the Terms of Service.

1. Scope of Processing

Kestra Labs processes Customer Data solely for the purpose of providing the gateway service: evaluating access policies, resolving credentials, proxying API requests, applying PII redaction, and generating audit logs. Processing occurs only on Customer's documented instructions.

2. Categories of Data

Credential Data: SaaS API tokens and keys stored in the vault. **Transit Data:** SaaS API responses passing through the gateway in real-time (not stored). **Metadata:** Request logs including timestamp, user identity, action, connector, policy decision, and latency. **Admin Data:** Dashboard configuration changes recorded in the Change Log.

3. Technical and Organizational Measures

Kestra Labs implements: AES-256 encryption at rest for all stored data, TLS 1.3 encryption in transit, per-request memory-only credential decryption with sub-second lifespan, three-tier credential isolation (managed, customer-key, zero-trust mTLS), immutable append-only audit logs, RBAC on internal systems with quarterly access reviews, SOC 2 Type II aligned controls, and ISO 27001 aligned information security management system.

4. Sub-Processors

Current sub-processors are listed on our Sub-Processors page. We provide 30 days advance notice before engaging new sub-processors. Customer may object to a new sub-processor within 14 days. If the objection cannot be resolved, Customer may terminate the affected services without penalty.

5. Data Subject Rights

Kestra Labs will assist Customer in responding to data subject requests (access, rectification, erasure, portability) within 10 business days of notification. Costs for extraordinary requests are borne by Customer.

6. Data Breach Notification

Kestra Labs will notify Customer of any confirmed personal data breach without undue delay and within 72 hours of confirmation. Notification will include: nature of the breach, categories and approximate number of affected records, likely consequences, and measures taken to address the breach.

7. Audit Rights

Customer may audit Kestra Labs's compliance with this DPA once per calendar year with 30 days written notice. Audit scope covers security controls relevant to Customer Data. Alternatively, Customer may review our SOC 2 Type II report and ISO 27001 certification in lieu of an on-site audit.

8. Data Deletion

Upon termination of the Service, Kestra Labs will permanently delete all Customer Data within the timeframes specified in the Privacy Policy. Customer may request a data export before termination. Deletion is certified in writing upon request.

9. GDPR Specific Provisions

For processing subject to GDPR: Kestra Labs acts as processor under Article 28. Standard Contractual Clauses (Module 2: Controller to Processor) are incorporated by reference. Kestra Labs will process data only within the EEA and approved jurisdictions unless Customer explicitly authorizes otherwise.