Privacy Policy

Kestra Labs LLC • Last Updated: March 1, 2026

1. Information We Collect

Account Information: Work email, name, company name, and billing details provided during registration. **Usage Data:** Dashboard interactions, API request metadata (timestamp, action, connector, decision, latency), and aggregate usage statistics. **Customer Credentials:** SaaS API keys/tokens stored in the vault, encrypted at rest per your selected tier.

2. Information We Do Not Collect

We do not store API response content — SaaS API responses transit the gateway in real-time and are relayed to the AI assistant without persistence. We do not track individual end-user behavior within SaaS applications. We do not collect personal data from your SaaS accounts beyond what transits the gateway. PII redacted by the redaction engine is masked before it reaches the AI assistant and is never stored in its unmasked form.

3. How We Use Information

Account information is used to provide the Service and communicate about your account. Usage metadata populates your admin dashboard (Status Board, Traffic Feed, Billing). Aggregated, anonymized usage statistics may be used to improve the Service. We do not sell, rent, or share your information with third parties for marketing purposes.

4. Data Retention

Account information: retained while your account is active, deleted within 90 days of account termination. Audit logs: retained per your tier (SOHO: 90 days, Team: 1 year, Enterprise: 7 years), then permanently deleted. Vault credentials: deleted within 72 hours of connector removal or account termination. Usage metrics: retained in aggregated form for 2 years.

5. Your Rights

Under GDPR and applicable data protection laws, you have the right to: access your personal data, correct inaccurate data, delete your account and associated data, export your audit logs, restrict processing, and object to processing. Contact privacy@kestralabs.com to exercise these rights. We respond within 30 days.

6. International Data Transfers

The Service infrastructure is hosted in AWS regions. Data may be processed in the United States and European Union. For EU customers, we maintain Standard Contractual Clauses (SCCs) as part of our DPA. Enterprise tier customers may select a single-region deployment to maintain data residency requirements.

7. Security

We implement encryption at rest (AES-256) and in transit (TLS 1.3), per-request memory-only credential decryption, role-based access controls on internal systems, and immutable append-only audit logs. See our Security page for the full compliance framework mapping.

8. Cookies

The admin dashboard uses essential session cookies only. We do not use tracking cookies, advertising cookies, or third-party analytics cookies. No consent banner is required because we use only strictly necessary cookies.