Runway Data Storage Locations

LAST UPDATED: APRIL 21ST, 2026

Applies to the Runway product at v2.cfo.ai. Republished from runway.cfo.ai/privacy/data-storage on October 5, 2026.

Overview

This page provides information about where your personal data is stored and processed when you use our services, in accordance with the General Data Protection Regulation (GDPR) and other applicable privacy laws.

Primary Data Storage Locations

Google Cloud Platform

Location: European Union (EU) and United States
Data Types: Application data, user profiles, transaction records, analytics data
Security Measures: Data encrypted in transit and at rest, SOC 2 Type II certified infrastructure
Data Transfer Safeguards: Standard Contractual Clauses (SCCs) for EU-US transfers

Merge (Third-Party Integration Platform)

Location: United States
Data Types: Integration logs, synchronized customer data, API connection data
Security Measures: Enterprise-grade encryption, regular security audits
Data Transfer Safeguards: Standard Contractual Clauses (SCCs), Privacy Shield successor framework compliance

Workato (Third-Party Integration Platform)

Location: United States, but Singapore upon request
Data Types: Workflow data, automated process logs, integration metadata
Security Measures: SOC 2 Type II compliance, end-to-end encryption
Data Transfer Safeguards: Binding Corporate Rules (BCRs), Standard Contractual Clauses (SCCs)

FiveTran (Third-Party Integration Platform)

Location: United States, but EU, Canada, Australia, Singapore, Indonesia, India, and Japan available on request
Data Types: Integration logs, synchronized customer data, API connection data
Security Measures: End-to-end encryption in transit and at rest, column blocking and hashing for PII protection, SOC 2 Type II, PCI DSS Level 1, HITRUST certification, customer-controlled data access
Data Transfer Safeguards: EU-US/UK-US/Swiss-US Data Privacy Framework certification, Standard Contractual Clauses (SCCs), Transfer Impact Assessments available

Snowflake (Data Storage)

Location: US
Data Types: Synchronized customer data
Security Measures: Dynamic data masking with RBAC, Time Travel recovery, end-to-end encryption, SOC Type II, FedRAMP, HITRUST CSF certifications
Data Transfer Safeguards: Data Privacy Framework certification, Standard Contractual Clauses incorporated into DPA, Transfer Impact Assessments

Elastic (Search)

Location: US
Data Types: Customer data, user data, application data
Security Measures: Encryption in transit (TLS) and at rest, role-based access controls, SSO authentication via Google Workspace, SOC 2 Type II compliance
Data Transfer Safeguards: Standard Contractual Clauses (SCCs) incorporated into Elastic's Data Processing Addendum (DPA)

Additional Service Providers

We may use other third-party services that store data in various locations including:

- **United States:** Analytics platforms, customer support tools, marketing automation
- **European Union:** Compliance monitoring, backup services
- **Other regions:** As disclosed in our Privacy Policy or through separate notice

Data Transfer Mechanisms

When your personal data is transferred outside the European Economic Area (EEA), we ensure appropriate safeguards are in place:

- **Standard Contractual Clauses (SCCs):** EU-approved contract terms that provide adequate protection
- **Adequacy Decisions:** Transfers to countries deemed adequate by the European Commission

- **Binding Corporate Rules:** Internal policies approved by data protection authorities
- **Explicit Consent:** Where legally required and obtained

Your Rights Regarding Data Location

Under GDPR, you have the right to:

- Know where your personal data is stored and processed
- Request that your data processing be restricted to specific locations (where technically feasible)
- Object to processing in certain locations
- Request data portability
- Access, rectify, or delete your personal data regardless of storage location

Data Residency Requests

If you require your data to be stored in a specific geographic location due to regulatory requirements or business needs, please contact us at security@cfo.ai. We will assess the feasibility of accommodating such requests on a case-by-case basis.

Security Across All Locations

Regardless of storage location, all personal data is protected by:

- Industry-standard encryption (AES-256)
- Multi-factor authentication
- Regular security assessments and penetration testing
- 24/7 monitoring and incident response
- Compliance with applicable local data protection laws

Changes to Storage Locations

We may change our data storage locations from time to time. When significant changes occur that may affect your rights, we will:

- Update this page with the new information

- Notify affected customers via email or account notifications
- Provide at least 30 days' notice where required by law

Contact Information

For questions about data storage locations or to exercise your privacy rights:

Privacy Team

Email: security@cfo.ai

Address: 440 N Barranca Ave, #7699, Covina, CA 91723
Phone: (646) 648-2769

Data Protection Officer

Email: annie.wu@cfo.ai

Regulatory Information

This page is maintained in compliance with:

- General Data Protection Regulation (GDPR)
- California Consumer Privacy Act (CCPA)
- Other applicable regional privacy laws

For our complete privacy practices, please refer to our Privacy Policy.

To review our list of service providers and subprocessors, please click here.

This page is reviewed and updated regularly to ensure accuracy. If you notice any discrepancies or have questions, please contact our Privacy Team.