Data Processing Agreement

FunctionFly™ LLC

Last updated: June 2026

This Data Processing Agreement ("DPA") forms part of the Terms of Service between FunctionFly™ LLC ("Processor") and the customer ("Controller") for enterprise deployments requiring GDPR compliance.

1. Definitions

In this DPA, the following terms have the meanings given below:

"Applicable Data Protection Law" means the General Data Protection Regulation (EU) 2016/679 ("GDPR") and applicable national implementing laws.

"Personal Data" means any information relating to an identified or identifiable natural person as defined in Applicable Data Protection Law.

"Processing" has the meaning given in Applicable Data Protection Law.

"Controller" means the natural or legal person which, alone or jointly with others, determines the purposes and means of Processing.

"Processor" means a natural or legal person that processes Personal Data on behalf of the Controller.

"Subprocessor" means any processor engaged by the Processor to process Personal Data on behalf of the Controller.

"Data Subject" means an identified or identifiable natural person whose Personal Data is processed.

"Security Incident" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

2. Subject Matter and Scope of Processing

2.1 Subject Matter

The Processor provides a cloud platform service for publishing, discovering, running, and managing serverless functions and related developer tools. The Processing of Personal Data under this DPA is limited to the data described in this Section 2.

2.2 Nature and Purpose of Processing

The Processor shall process Personal Data for the following purposes:

- Providing and maintaining the FunctionFly™ platform service
- Account management and authentication
- Billing and subscription management
- Function execution, logging, and monitoring
- Security, abuse prevention, and fraud detection
- Compliance with legal obligations

2.3 Categories of Personal Data

The Processor may process the following categories of Personal Data:

- Account information (name, email, company, job title)
- Authentication and session data (IP address, user agent, login timestamps)
- Billing and transaction metadata
- Function execution metadata (timestamps, function identifiers, error logs)
- API usage logs and quota events
- Support communications when you contact us

2.4 Categories of Data Subjects

This DPA covers Processing of Personal Data relating to:

- Controller's users and employees who use the FunctionFly™ platform
- API consumers and agents acting on behalf of the Controller
- Any other individuals whose data the Controller submits to the Service

2.5 Duration

Processing under this DPA shall continue for the duration of the Terms of Service. Upon termination, the Processor will delete or return Personal Data according to Section 4 and the controller's

instructions, except where retention is required by law.

3. Processor Obligations

3.1 Compliance with Law

Process Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data to a third country, unless required to do otherwise by Applicable Data Protection Law.

3.2 Personnel

Ensure that personnel authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.3 Confidentiality

Not disclose Personal Data to third parties except to Subprocessors as specified in this DPA, or as required by law. The Processor shall require Subprocessors to maintain at least the same confidentiality obligations.

3.4 Security Measures

Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, as described in Section 7 of this DPA and our Security Policy.

3.5 Subprocessors

Not engage additional Subprocessors without the Controller's prior general written authorization. The Controller grants general authorization for the engagement of Subprocessors listed in our Privacy Policy subprocessor list.

3.6 Assistance to Controller

Taking into account the nature of the Processing, assist the Controller by appropriate technical and organizational measures for the fulfillment of the Controller's obligations to respond to requests to exercise Data Subject rights.

3.7 Deletion or Return

At the Controller's choice, delete or return all Personal Data after the end of the provision of services, and delete existing copies unless retention is required by Applicable Data Protection Law.

4. Subprocessors

4.1 Authorized Subprocessors

The Controller authorizes the Processor to engage the Subprocessors listed in our Privacy Policy for the processing of Personal Data. This list may be updated from time to time; the Processor will provide notice of material changes.

4.2 Subprocessor Obligations

The Processor shall ensure that Subprocessors are bound by data processing terms no less protective than this DPA. The Processor remains fully liable to the Controller for the performance of Subprocessors' obligations.

4.3 Objection Right

If a Controller has a reasonable objection to a new Subprocessor, the Controller may terminate the affected services by providing written notice within 30 days of being notified of the addition.

5. International Data Transfers

5.1 Transfer Mechanisms

Personal Data may be transferred internationally. When transferring Personal Data outside the European Economic Area (EEA), the Processor implements the following safeguards:

- Standard Contractual Clauses (SCCs) approved by the European Commission
- Adequacy decisions for transfers to countries with equivalent privacy protections
- Binding Corporate Rules for intra-group transfers
- Explicit consent where required by Applicable Data Protection Law

5.2 Data Location

Personal Data may be stored and processed in data centers located in the United States, European Union, and other jurisdictions as described in our Privacy Policy.

6. Data Subject Rights

The Processor shall assist the Controller in fulfilling its obligations to respond to Data Subject requests for:

- Right of access

- Right to rectification
- Right to erasure ("right to be forgotten")
- Right to restrict processing
- Right to data portability
- Right to object

The Controller is responsible for directing Data Subjects to submit requests through the Controller's systems. The Processor will provide reasonable assistance within 30 days of receiving documented instructions from the Controller.

7. Security

7.1 Technical and Organizational Measures

The Processor implements appropriate technical and organizational security measures including:

- Encryption: TLS 1.3 for data in transit; AES-256 for data at rest
- Access controls: Role-based access control, MFA for administrative access
- Monitoring: 24/7 security monitoring, intrusion detection, SIEM integration
- Incident response: Documented procedures for security incidents
- Vulnerability management: Regular security assessments and patches

7.2 Security Documentation

Full security architecture details are available in our Security Policy and Trust Center.

8. Security Incident Notification

8.1 Notification Obligation

The Processor shall notify the Controller without undue delay (and in any event within 72 hours) after becoming aware of a Security Incident affecting Personal Data.

8.2 Information Provided

When notifying the Controller of a Security Incident, the Processor shall provide:

- Description of the nature of the Security Incident
- Categories and approximate number of affected Data Subjects
- Categories and approximate number of affected Personal Data records

- Contact point for further information
- Likely consequences of the Security Incident
- Measures taken or proposed to address the Security Incident

8.3 Exclusions

Notification obligations do not apply when the Processor determines that the Security Incident is unlikely to result in a risk to the rights and freedoms of Data Subjects, or when notification would involve disproportionate effort.

9. Audits

9.1 Audit Rights

The Controller may audit the Processor's compliance with this DPA by requesting:

- Copies of SOC 2 Type II audit reports (available upon request under NDA)
- Documentation of security policies and procedures
- Information about the Processor's security certifications

9.2 On-Site Audits

For enterprise customers requiring on-site audits, the Processor will cooperate with reasonable audit requests. The Controller shall provide at least 30 days' prior written notice. Audits shall be conducted during business hours without disrupting the Processor's operations.

9.3 Audit Costs

The Controller shall bear the costs of any audit. If an audit reveals material non-compliance, the Processor shall bear its own costs and remedy the non-compliance within a reasonable timeframe.

10. General Provisions

10.1 Order of Precedence

This DPA forms part of the Terms of Service. In case of conflict between this DPA and the Terms of Service, this DPA shall prevail for matters related to data protection.

10.2 Governing Law

This DPA shall be governed by the same law as the Terms of Service.

10.3 Contact

For questions about this DPA or to request an executed copy, contact: privacy@functionfly.com

10.4 Mutual Execution

This DPA may be executed electronically. The Processor will provide a countersigned copy upon request from the Controller.