**Fast Cloud Consulting, Corp.**

# Data Processing Addendum

*For execution between Fast Cloud Consulting, Corp. and Customer*

**Effective Date: May 15, 2026**

Version: 1.0

## Recitals

This Data Processing Addendum (this "**DPA**") is entered into between Fast Cloud Consulting, Corp., a Delaware corporation ("**Processor**" or "**Company**"), and the customer identified in the executed Order Form or other agreement with the Company ("**Controller**" or "**Customer**"). This DPA is incorporated into and forms part of the Terms of Service or other written agreement between the parties (the "**Agreement**").

The parties acknowledge that, in the course of providing the Service to Customer, the Company processes personal data on behalf of Customer. This DPA governs the rights and obligations of the parties with respect to such processing.

**Scope notice:** This DPA applies to Personal Data processed by the Company through the FranFast Launchpad portal and through the public website. Personal Data processed within the FranFast Franchise Execution & Network Management Platform (which runs on the Salesforce cloud infrastructure) is governed by the Salesforce Data Processing Addendum entered into by Salesforce and Customer pursuant to the Salesforce Service Terms of Use (Exhibit A to the MSSA). The Company's role with respect to Salesforce-hosted Personal Data is that of a value-added reseller and implementation/managed services provider; Salesforce remains the data processor of the Salesforce Platform itself.

In the event of any conflict between the Agreement and this DPA, this DPA shall control with respect to data protection matters within the scope set forth above.

## 1. Definitions

For purposes of this DPA, the following definitions apply:

**"Applicable Data Protection Laws"** means all data protection and privacy laws applicable to the processing of Personal Data under this DPA, including without limitation the EU General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"), the United Kingdom Data Protection Act 2018, the California Consumer Privacy Act (Cal. Civ. Code § 1798.100 et seq.) and California Privacy Rights Act ("CCPA/CPRA"), and other applicable state, federal, and international privacy laws.

**"Controller," "Processor," "Data Subject," "Personal Data," "Processing," "Personal Data Breach," and "Supervisory Authority"** have the meanings ascribed to them in the GDPR.

**"Standard Contractual Clauses"** or "SCCs" means the standard contractual clauses for the transfer of personal data to third countries, adopted by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

**"Subprocessor"** means any third party engaged by the Processor to process Personal Data on behalf of the Controller in connection with providing the Service.

## 2. Scope and Roles

The parties acknowledge and agree that, with regard to the processing of Personal Data, Customer is the Controller and the Company is the Processor.

The Company will process Personal Data only on documented instructions from Customer, including with regard to transfers of Personal Data to a third country, unless required to do so by Applicable Data Protection Laws to which the Company is subject.

The subject matter, duration, nature, purpose, types of Personal Data, and categories of Data Subjects are described in Annex A.

## 3. Personnel and Confidentiality

The Company shall ensure that personnel authorized to process Personal Data are bound by appropriate confidentiality obligations and have received appropriate training on the protection of Personal Data.

The Company shall limit access to Personal Data to personnel who require such access in the course of performing the Company's obligations under the Agreement.

## 4. Security Measures

The Company shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation, the nature, scope, context, and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

The Company's security measures include, but are not limited to:

- Encryption of Personal Data in transit (TLS 1.2 or higher, configured to maintain a B or greater grade on the Qualys SSL Labs rating) and at rest (AES-256), implemented in accordance with NIST SP 800-57 and the Company's internal Cryptography Policy.
- Access controls and authentication, including multi-factor authentication for administrative access.
- Network segmentation, firewalls, and intrusion detection.
- Regular security testing and vulnerability scanning.
- Continuous compliance monitoring and an annual independent SOC 2 Type II examination.
- Personnel security, including background checks and security training.
- Documented incident response and business continuity procedures.

A more detailed description of the Company's technical and organizational measures is provided in Annex C.

## 5. Subprocessors

Customer authorizes the Company to engage Subprocessors to process Personal Data in connection with the Service. A current list of Subprocessors is maintained at https://www.franfast.io/subprocessors/ and is also reproduced in Annex B.

The Company shall: (a) enter into a written agreement with each Subprocessor that imposes data protection obligations no less protective than those in this DPA; (b) remain liable for the acts and omissions of each Subprocessor as if they were the Company's own; and (c) provide Customer with prior notice of any new Subprocessor at least thirty (30) days before the new Subprocessor begins processing Personal Data.

Customer may object to a new Subprocessor on reasonable grounds related to data protection by notifying the Company within thirty (30) days of notification. If the parties cannot resolve the

objection in good faith, Customer may terminate the affected Subscription as set forth in the Cancellation and Refund Policy.

## 6. Data Subject Rights

Taking into account the nature of the processing, the Company shall assist Customer by appropriate technical and organizational measures, insofar as possible, in fulfilling Customer's obligation to respond to requests by Data Subjects to exercise their rights under Applicable Data Protection Laws (including rights of access, rectification, erasure, restriction, portability, and objection).

If the Company receives a request from a Data Subject relating to Personal Data processed on behalf of Customer, the Company shall promptly forward the request to Customer and shall not respond to the Data Subject directly except as instructed by Customer or as required by law.

## 7. Personal Data Breach

The Company shall notify Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer's Personal Data, in accordance with the Company's internal Incident Response Plan and applicable Data Protection Laws. The notification shall include, to the extent known at the time:

- A description of the nature of the Personal Data Breach, including the categories and approximate number of Data Subjects and Personal Data records concerned.
- The likely consequences of the Personal Data Breach.
- The measures taken or proposed to be taken to address the Personal Data Breach and to mitigate its possible adverse effects.
- Contact information for the Company's data protection point of contact.

## 8. Data Transfers

To the extent that the Company processes Personal Data originating from the European Economic Area (EEA), the United Kingdom, or Switzerland in a country that has not been deemed by the relevant Supervisory Authority to provide an adequate level of protection, the Standard Contractual Clauses are hereby incorporated by reference and shall apply to such transfers, with the Company acting as data importer and Customer as data exporter.

The applicable SCC modules are identified in Annex D. The parties shall comply with their respective obligations under the SCCs.

**UK Transfers.** For transfers of Personal Data subject to the UK GDPR, the parties agree that the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner's Office ("UK Addendum") shall apply and is hereby incorporated by reference.

**Swiss Transfers.** For transfers of Personal Data subject to the Swiss Federal Act on Data Protection ("Swiss FADP"), references in the SCCs to "Member State" shall be interpreted to include Switzerland, and references to the GDPR shall be interpreted as references to the Swiss FADP where applicable.

**Data protection contact.** The Company's data protection and security contact for purposes of this DPA is: security@fastcloudconsulting.com.

## 9. Audit Rights

The Company shall make available to Customer all information necessary to demonstrate compliance with this DPA. Such information shall be provided in the form of:

- The Company's most recent SOC 2 Type II report (subject to the execution of a non-disclosure agreement).
- Other certifications, attestations, or evidence of compliance reasonably requested by Customer.

Customer may, at its expense and no more than once per year (except in the event of a Personal Data Breach affecting Customer's Personal Data), conduct an audit of the Company's compliance with this DPA. Such audit shall be conducted with reasonable advance notice, during normal business hours, in a manner that does not disrupt the Company's operations, and subject to confidentiality obligations. Audits shall not include access to the Company's source code, penetration testing of the Company's systems, or access to information relating to other customers of the Company, except as otherwise required by Applicable Data Protection Laws.

## 10. Return or Deletion of Personal Data

Upon termination of the Agreement, the Company shall, at Customer's election, return all Personal Data to Customer or delete all Personal Data in its possession, except to the extent retention is required by applicable law. Customer shall make its election within sixty (60) days following termination, consistent with the Company's internal Data Retention Matrix. If Customer does not provide instructions within such period, the Company may delete Personal Data in accordance with its standard data retention policies.

## 11. Liability

The liability of each party under or in connection with this DPA shall be subject to the limitations of liability set forth in the Agreement.

Nothing in this DPA shall limit or exclude either party's liability where such limitation or exclusion is prohibited by Applicable Data Protection Laws.

## 12. Term and Termination

This DPA shall commence on the effective date of the Agreement and shall continue for so long as the Company processes Personal Data on behalf of Customer pursuant to the Agreement. Termination of the Agreement shall result in termination of this DPA.

## 13. Governing Law

To the extent permitted by Applicable Data Protection Laws, this DPA shall be governed by the laws specified in the Agreement. Where Applicable Data Protection Laws (including the GDPR) require application of the laws of a different jurisdiction, the latter shall apply with respect to the matters governed by such laws.

## 14. Signature

This DPA is incorporated by reference into the Agreement and is binding upon the parties without separate signature. However, the parties may elect to execute this DPA separately as evidence of their agreement, in which case the signed copy shall control.

**Fast Cloud Consulting, Corp.**

Signed: _____

Name: _____

Title: _____

Date: _____

**Customer**

Signed: _____

Name: _____

Title: _____

Date: _____

# Annex A — Description of Processing

## Subject Matter

Provision of the public website at https://www.franfast.io and the FranFast Launchpad portal to Customer, including hosting, data storage, authentication, support, and other functionality necessary to deliver the Service as defined and scoped in this DPA. Subject matter related to the FranFast Franchise Execution & Network Management Platform (Salesforce-based) is excluded from this DPA and is governed by the Salesforce DPA executed by Salesforce and Customer.

## Duration

The duration of the Subscription, as set forth in the applicable Order Form, plus any post-termination retention period required by law or specified in the Agreement.

## Nature and Purpose

Processing necessary to provide the Service to Customer, including authentication, authorization, transaction processing, communications, support, security monitoring, and data backup.

## Categories of Personal Data

- Identity data: name, email address, job title, organization affiliation.
- Authentication data: hashed passwords, session tokens, multi-factor authentication artifacts.
- Activity data: log of actions performed within the Service, IP address, browser and device metadata.
- Configuration and content data: any Personal Data that Customer or its Authorized Users elect to enter into the Service.

## Categories of Data Subjects

- Customer's employees, contractors, and agents who are Authorized Users of the Service.
- Customer's franchisees, prospective franchisees, and other individuals whose information Customer chooses to process through the Service.

## Annex B — Subprocessors

The current Subprocessor list is maintained at https://www.franfast.io/subprocessors/. The list is reproduced here as a snapshot as of the Effective Date and may have been updated since.

*Refer to the live page for the current authoritative list.*

| Subprocessor | Service Provided | Data Hosting Region | Compliance | Purpose / Data Categories |
|---|---|---|---|---|
| Vercel, Inc. | Hosting & deployment platform (FranFast Launchpad) | United States (multi-region edge) | SOC 2 Type II | Hosts the FranFast Launchpad product; processes session traffic, including IP addresses and user agent strings. |
| Supabase, Inc. | Authentication, identity, database (Launchpad) | United States (us-east-2 / Ohio) | SOC 2 Type II | Manages user authentication credentials, session tokens, and Launchpad-resident application data; provides backend database services. |
| Amazon Web Services, Inc. (AWS) | Object storage for audit logs | United States (us-east-2 / Ohio) | SOC 1, SOC 2, SOC 3, ISO 27001, others | Stores platform logs forwarded from the Supabase Log Drain (auth events, API calls, database queries) for the configured retention period. |
| Resend (Resend.com, Inc.) | Transactional email delivery | United States | SOC 2 Type II | Sends authentication-related emails (account confirmation, password reset, magic link, email change). Processes recipient email address and metadata. |
| Google LLC — Google Cloud Platform (OAuth 2.0 Identity) | Single sign-on identity provider | Global | SOC 1, SOC 2, SOC 3, ISO 27001, others | Provides 'Sign in with Google' authentication. Processes identity assertions including email address, name, and profile picture for users who choose Google SSO. |
| Google LLC — Google Workspace | Internal corporate email and collaboration | Global | SOC 1, SOC 2, SOC 3, ISO 27001, others | Hosts Company employee email and internal documents; may incidentally process Customer support communications routed through Company email. |
| Stripe, Inc. | Payment processing | United States | PCI DSS Level 1, SOC 1, SOC 2 | Processes Customer payment transactions for Subscription fees. Payment card data is collected directly by Stripe and is not transmitted through or stored on Company systems. |
| GitHub, Inc. | Source code repository | United States | SOC 1, SOC 2, ISO 27001 | Hosts source code repositories and related |

| Subprocessor | Service Provided | Data Hosting Region | Compliance | Purpose / Data Categories |
|---|---|---|---|---|
| | | | | development workflows. Customer Data is not intentionally stored in GitHub repositories as part of normal Service operations. |
| Vanta, Inc. | Continuous compliance monitoring | United States | SOC 2 Type II | Monitors Company security and compliance posture. Does not process Customer Data; processes Company employee and infrastructure metadata. |

## Annex C — Technical and Organizational Measures

The Company implements the following technical and organizational measures (TOMs):

### C.1 Pseudonymization and Encryption

- Encryption in transit using TLS 1.2 or higher, configured to maintain a B or greater grade on the Qualys SSL Labs rating, for all Customer-facing endpoints.
- Encryption at rest using AES-256 for Customer Data stored in databases and object storage.
- Cryptographic implementation aligned with NIST SP 800-57 and the Company's internal Cryptography Policy, with documented key management practices including key rotation, role-based access to keys, and protection of keys at rest.
- Authentication credentials are hashed using industry-standard algorithms (e.g., bcrypt, Argon2).

### C.2 Confidentiality, Integrity, Availability, Resilience

- Role-based access control with principle of least privilege.
- Multi-factor authentication for administrative access.
- Network segmentation between production and non-production environments.
- Continuous monitoring of security events and anomalies.
- Documented business continuity and disaster recovery plans, tested periodically.

### C.3 Restoration of Availability and Access

- Automated database backups by the underlying platform provider.
- Documented restore procedures.
- Defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) targets.

### C.4 Regular Testing and Evaluation

- Annual independent SOC 2 Type II examination.
- Continuous compliance monitoring via Vanta.
- Periodic vulnerability scanning of source code and infrastructure.
- Annual penetration testing by qualified third party.

## Annex D — Standard Contractual Clauses

Where applicable to international transfers of Personal Data, the parties agree to the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as follows:

### Module Selection

- Module Two (Controller to Processor) applies where Customer is the Controller and the Company is the Processor.
- Module Three (Processor to Subprocessor) applies between the Company and its Subprocessors, as applicable.

### Docking Clause

Clause 7 (optional docking clause) is included.

### Subprocessors

Clause 9, Option 2 (general written authorization) applies. The list of authorized Subprocessors and the notice procedure are set forth in Section 5 of this DPA and at https://www.franfast.io/subprocessors/.

### Audits

Audit rights are set forth in Section 9 of this DPA.

### Choice of Forum

Pursuant to Clause 18 of the Standard Contractual Clauses, the parties agree that the courts of a Member State of the European Union, as mutually agreed by the parties, shall have jurisdiction to resolve disputes arising under the SCCs. In the absence of such agreement, the courts of Ireland shall apply by default.

### Annexes to the SCCs

The Annexes to the SCCs (description of processing, technical and organizational measures, list of subprocessors) are deemed incorporated from Annexes A, C, and B of this DPA, respectively.