# DATA PROCESSING ADDENDUM

*Version 1.0*

This Data Processing Addendum ("DPA") forms part of the Master Software as a Service Agreement between Provider and Customer.

## 1. Roles

Where Provider processes Personal Data on Customer's behalf, Customer is the Controller, Business, or equivalent, and Provider is the Processor, Service Provider, Contractor, or equivalent, as applicable under relevant Data Protection Law.

## 2. Processing Instructions

Provider will process Personal Data only according to Customer's documented instructions, to provide the Services, to execute authorized Agent Actions, as described by the Agreement, or where required by law.

## 3. Processing Details

Subject Matter: SaaS, AI, autonomous-agent, integration, hosting, support, and related Services.

Duration: Subscription Term plus the applicable retention period.

Purposes: Hosting, workflow execution, AI processing, communications, analytics, integration processing, security, support, and Service operation.

Data Subjects: Customer employees, Authorized Users, contractors, customers, prospects, suppliers, event attendees, speakers, contacts, and other individuals represented in Customer Data.

Data Types: Names, contact information, business information, account data, CRM data, calendar information, communications, event data, identifiers, user activity, prompts, documents, and other Personal Data submitted by Customer.

## 4. Confidentiality

Provider personnel authorized to process Personal Data will be subject to confidentiality obligations.

## 5. Security

Provider will maintain technical and organizational measures including encryption at rest and in transit, MFA for privileged access, least privilege, role-based access, logical tenant isolation, monitoring and logging, vulnerability management, penetration testing, secure development, incident response, backups, disaster recovery, vendor-security management, employee security training, personnel-access controls, and business continuity.

## 6. SOC 2

Provider maintains a SOC 2 Type II program and independent examination. Provider will make the applicable report available subject to confidentiality requirements.

## 7. AI Processing

Provider will not use Customer Personal Data to train generalized AI models for use by other customers without Customer's written consent. Provider will require applicable third-party AI model providers to process Customer Personal Data solely to provide their services to Provider and not for generalized model training.

## 8. Subprocessors

Customer provides general authorization for Provider to use subprocessors. Provider will maintain a current subprocessor list, impose appropriate contractual privacy and security obligations, remain responsible for subprocessors as required by applicable law, and provide reasonable advance notice of material new subprocessors. Customer may object to a new subprocessor on reasonable data-protection grounds. The Parties will work in good faith to resolve the objection.

## 9. International Transfers

Provider will use legally recognized safeguards for international Personal Data transfers when required, including applicable Standard Contractual Clauses.

## 10. Data Residency

Customer's primary production Customer Data will be hosted in the region identified in the Order Form. Cross-border processing necessary for approved subprocessors, support, security, or Service functionality will remain subject to this DPA.

## 11. Data Subject Requests

Provider will provide reasonable assistance to Customer in responding to requests concerning access, correction, deletion, portability, restriction, objection, or other applicable privacy rights.

## 12. Security Incident Notification

Provider will notify Customer without undue delay and, where reasonably practicable, within forty-eight hours after confirming a Personal Data Breach affecting Customer Personal Data. Provider will provide reasonably available information sufficient to support Customer's legal obligations.

## 13. DPIA and Regulatory Assistance

Provider will provide reasonable assistance with data protection impact assessments, regulator consultations, breach response, privacy assessments, and other legally required compliance activities.

## 14. Audit Rights

Provider will make information reasonably necessary to demonstrate DPA compliance available to Customer. Independent reports, including SOC 2, may satisfy routine audit requirements. Customer may conduct additional audits as provided under the MSA.

## 15. Return and Deletion

Following termination: (1) Customer may export Customer Data during the applicable retention period; (2) Provider will delete production Customer Personal Data within 90 days, unless otherwise stated in the Order Form; and (3) residual backup copies may remain until overwritten through Provider's normal backup lifecycle. All retained backup data remains protected by this DPA.

## 16. U.S. Privacy Requirements

Where applicable, Provider will act only as Customer's Service Provider, Processor, or Contractor; not sell Customer Personal Data; not share Customer Personal Data for cross-context behavioral advertising; not retain, use, or disclose Customer Personal Data outside the purposes specified in the Agreement except as legally permitted; and provide the same level of privacy protection required by applicable law.

## 17. Conflict

For Personal Data matters, this DPA controls over conflicting provisions of the MSA.

## SIGNATURES

| PROVIDER | CUSTOMER |
|---|---|
| epp Technologies, Inc | [Customer Legal Name] |
| Signature: _____ | Signature: _____ |
| Name: _____ | Name: _____ |
| Title: _____ | Title: _____ |
| Date: _____ | Date: _____ |