Data Processing Addendum

VERSION 2.0 · EFFECTIVE OCTOBER 1, 2026

How to execute this DPA

This DPA is already part of the Master Subscription Agreement through Section 4.4 of that agreement, so it applies to every customer without a separate signature. Customers who need a signed copy for their records can countersign it:

(a) This DPA has been signed on behalf of StitchOps, Inc.

(b) Complete the Customer information and sign the signature page. Use the full legal entity name shown on your Order Form.

(c) Send the signed DPA to **privacy@stitchops.io**. The countersigned DPA takes effect when StitchOps receives it.

(d) Changes or deletions made to this DPA by Customer are not accepted unless StitchOps agrees to them in writing. Negotiated terms belong in a signed amendment.

About this DPA

This Data Processing Addendum ("DPA") forms part of the StitchOps Master Subscription Agreement at **https://www.stitchops.io/legal/msa**, or another written agreement between StitchOps and Customer that governs Customer's use of the Service (the "Agreement"). Capitalized terms not defined in this DPA have the meanings given in the Agreement. This DPA consists of the main body, the Standard Contractual Clauses incorporated by reference, and Annexes I through IV.

Customer enters into this DPA for itself and, where Data Protection Laws require, on behalf of its Affiliates that act as Controllers of Personal Data processed under the Agreement.

1. Definitions

1.1 **"CCPA"** means the California Consumer Privacy Act, Cal. Civ. Code Section 1798.100 and following, as amended by the California Privacy Rights Act of 2020, and its regulations.

1.2 **"Controller"** means the entity that determines the purposes and means of Processing Personal Data.

1.3 **"Data Protection Laws"** means all laws that apply to the Processing of Personal Data under the Agreement, including the GDPR, the UK GDPR, the Swiss FADP, and U.S. Privacy Laws.

1.4 **"Data Subject"** means the identified or identifiable natural person to whom Personal Data relates.

1.5 **"GDPR"** means Regulation (EU) 2016/679, the General Data Protection Regulation.

1.6 **"Personal Data"** means any information relating to an identified or identifiable natural person that is included in Customer Data, including information defined as "personal information" or "personally identifiable information" under Data Protection Laws.

1.7 **"Processing"** means any operation performed on Personal Data, whether or not by automated means, such as collection, recording, organization, storage, retrieval, use, disclosure, combination, restriction, erasure, or destruction. "Process" has a corresponding meaning.

1.8 **"Processor"** means the entity that Processes Personal Data on behalf of a Controller.

1.9 **"Restricted Transfer"** means a transfer of Personal Data (a) from the European Economic Area to a country without an adequacy decision of the European Commission, (b) from Switzerland to a country not recognized as adequate under the Swiss FADP, or (c) from the United Kingdom to a country not covered by adequacy regulations under Section 17A of the UK Data Protection Act 2018.

1.10 **"Security Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data Processed by StitchOps or its Subprocessors.

1.11 **"Standard Contractual Clauses"** means the clauses approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, Module Two (Controller to Processor) and Module Three (Processor to Processor).

1.12 **"Subprocessor"** means any Processor engaged by StitchOps to Process Personal Data on behalf of Customer.

1.13 **"Swiss FADP"** means the Swiss Federal Act on Data Protection of 25 September 2020.

1.14 **"UK Addendum"** means the International Data Transfer Addendum to the Standard Contractual Clauses, version B1.0, issued by the UK Information Commissioner under Section 119A of the UK Data Protection Act 2018.

1.15 **"UK GDPR"** means the GDPR as it forms part of the law of the United Kingdom.

1.16 **"U.S. Privacy Laws"** means the privacy laws of the United States and its states that apply to the Processing of Personal Data under the Agreement, including the CCPA.

2. Scope and Roles

2.1 **Scope.** This DPA applies when StitchOps Processes Personal Data on behalf of Customer in providing the Service and Professional Services. The subject matter, nature, purpose, and duration of the Processing, and the types of Personal Data and categories of Data Subjects, are described in Annex I.

2.2 **Roles.** Customer is the Controller and StitchOps is a Processor. Where Customer acts as a Processor for a third party Controller, StitchOps is Customer's Subprocessor. For the CCPA and similar U.S. Privacy Laws, Customer is the "business" and StitchOps is the "service provider" or "processor."

2.3 **Customer responsibilities.** Customer will comply with Data Protection Laws in its use of the Service, including giving any required notices to Data Subjects and having a lawful basis for the Processing. Customer is responsible for the accuracy, quality, and legality of Personal Data and the means by which Customer obtained it.

3. Processing Instructions

3.1 **Instructions.** StitchOps will Process Personal Data only on Customer's documented instructions. The Agreement, this DPA, the Order Forms, and the workflows Customer configures and approves in the Service are Customer's complete instructions. Additional instructions must be agreed in writing.

3.2 **Unlawful instructions.** StitchOps will tell Customer if it believes an instruction violates Data Protection Laws, and is not required to follow that instruction. StitchOps will also tell Customer if it can no longer meet its obligations under this DPA.

3.3 **Confidentiality.** StitchOps will keep Personal Data confidential and will not Process it for its own purposes, including for advertising, profiling, or training AI models.

4. Where Processing Happens

4.1 **Customer environment.** Where Digital Workers run on Execution Infrastructure that Customer provides, screen content and field values a Digital Worker handles while executing a workflow stay on that infrastructure. The Control Plane receives only the metadata it needs to orchestrate, monitor, and report on workflows, as described in Section 14.7 of the Agreement. Telemetry sent to the Control Plane does not include field values, screen images, or other screen content.

4.2 **Credentials.** By default, Credentials stay in Customer's own credential vault and are retrieved by Digital Workers at run time. StitchOps stores Credentials only at Customer's request, encrypted, as described in Section 3.3 of the Agreement. Credential values are never sent to an AI model.

4.3 **AI Features.** AI Features are optional, as described in Section 3.6 of the Agreement. By default, any model used by an AI Feature, including AI assisted workflow building, runs on the Digital Worker or through Inference Services that Customer provides, and Customer's provider Processes that data under Customer's own agreement with it, not as a StitchOps Subprocessor. A model provider StitchOps engages Processes Personal Data to run AI Features only if Customer elects StitchOps Provided Inference with that provider, and only the model providers Customer elects do so. StitchOps may also use a Subprocessor to monitor and troubleshoot AI Features. Each is a Subprocessor under Section 7. Neither StitchOps nor any such provider uses Personal Data to train AI models.

4.4 **Hosting location and data in the Control Plane.** StitchOps hosts the Control Plane on Amazon Web Services in the United States, primarily in the US West (Oregon) region with a standby deployment in US East (N. Virginia) for failover. The database services it uses are listed at **https://www.stitchops.io/legal/subprocessors** and are also in the United States. The Control Plane stores workflow definitions and configuration, execution metadata such as status, timing, and errors, and account details for Customer's administrators and Users of the Service, such as name and work email. It is not designed to store the Personal Data that workflows handle, such as HR records, or special categories of data such as health information. That data stays with the Digital Worker on Customer's Execution Infrastructure, under Customer's control, unless Customer configures a workflow to send it to the Control Plane, in which case the measures in Annex II apply to it.

5. StitchOps Personnel

StitchOps will ensure that personnel who Process Personal Data are bound by written confidentiality obligations, receive appropriate privacy and security training, and have access only to the Personal Data they need for their role.

6. Security Measures

6.1 **Measures.** StitchOps will maintain the technical and organizational measures described in Annex II to protect Personal Data against Security Breaches and to protect its confidentiality, integrity, and availability.

6.2 **No reduction.** StitchOps may update its measures as technology and threats change, but will not materially reduce the overall security of the Service during a subscription term.

7. Subprocessors

7.1 **Authorization.** Customer gives StitchOps general authorization to engage Subprocessors, including StitchOps Affiliates. StitchOps will (a) enter into a written agreement with each Subprocessor that imposes data protection terms at least as protective as this DPA, and (b) remain responsible for each Subprocessor's performance as if it were StitchOps' own, subject to the Agreement.

7.2 **List.** The current list of Subprocessors, with each one's purpose, location, and the types of data it Processes, is at **https://www.stitchops.io/legal/subprocessors**.

7.3 **Notice of new Subprocessors.** Customer may subscribe to notices of Subprocessor changes at **https://www.stitchops.io/legal**. StitchOps will give subscribers at least 30 days notice before a new Subprocessor begins Processing Personal Data.

7.4 **Objection.** Customer may object to a new Subprocessor on reasonable data protection grounds by writing to **privacy@stitchops.io** within that notice period. The parties will work in good faith to resolve the objection, including through a change to the Service or Customer's configuration that avoids the new Subprocessor. If they cannot resolve it within 30 days, Customer may terminate the affected part of the Service by written notice, and StitchOps will refund prepaid Fees for the terminated part covering the rest of the term.

7.5 **Subprocessor agreements.** Copies of Subprocessor agreements that the Standard Contractual Clauses require StitchOps to provide may have commercial and unrelated terms removed, and will be provided on request.

8. Security Breach Notification

8.1 **Notice.** StitchOps will notify Customer without undue delay, and in any event within 72 hours, after confirming a Security Breach, consistent with Section 4.3 of the Agreement.

8.2 **Contents.** The notice will describe, as far as then known, the nature of the Security Breach, the categories and approximate number of Data Subjects and records affected, the likely consequences, the steps StitchOps has taken or proposes, any Credentials Customer should rotate, and a contact for more information. StitchOps will update Customer as it learns more.

8.3 **Response.** StitchOps will take reasonable steps to contain, investigate, and remediate the Security Breach, and will reasonably assist Customer in meeting its own notice obligations. A notice is not an admission of fault. This Section does not apply to incidents caused by Customer, its Users, or Customer's Execution Infrastructure.

9. Data Subject Requests and Assistance

9.1 **Data Subject requests.** StitchOps will give Customer the ability, through the Service or with reasonable help, to respond to requests from Data Subjects to exercise their rights. If StitchOps receives a request directly and can identify Customer, it will refer the Data Subject to Customer and will not respond itself unless Customer instructs it to or the law requires it.

9.2 **Impact assessments.** On Customer's written request, StitchOps will provide reasonable information and help for Customer's data protection impact assessments and consultations with Supervisory Authorities, to the extent Customer does not otherwise have the information.

10. Audits and Certifications

10.1 **Reports.** StitchOps maintains a SOC 2 Type 2 report and HIPAA and GDPR Article 5 attestations from an independent auditor covering the StitchOps hosted Control Plane, or successor independent audits of equivalent scope. On Customer's written request, and subject to the confidentiality terms of the Agreement, StitchOps will provide its current reports and reasonable answers to security questionnaires. Customer agrees these reports are the primary way StitchOps shows compliance with this DPA. Components that run on Customer's infrastructure, including Digital Workers, operate under Customer's own controls and are outside the scope of those reports.

10.2 **Onsite audits.** If the reports do not reasonably answer a question Customer must answer under Data Protection Laws, or a Supervisory Authority requires it, or after a Security Breach, Customer may audit StitchOps' relevant procedures. Customer will give at least 30 days written notice, and the parties will agree on scope, timing, duration, and confidentiality in advance. Audits are limited to once in any 12 month period except after a Security Breach or when a Supervisory Authority requires it, take place during Business Days, and do not include access to other customers' data. Customer bears its own costs and reimburses StitchOps' reasonable costs at StitchOps' then current Professional Services rates, agreed in advance.

10.3 **Standard Contractual Clauses.** The audits in Clause 8.9 of the Standard Contractual Clauses will be carried out as described in this Section 10.

11. Deletion and Return

11.1 **Return.** Customer may export Customer Data, including Personal Data, during the term and for 30 days after the Agreement ends, as described in Section 4.5 of the Agreement.

11.2 **Deletion.** Within 30 days after that export period ends, StitchOps will delete Personal Data from the Service, unless the law requires StitchOps to keep it.

Copies in backups are deleted on the normal backup cycle within 35 days and remain protected under this DPA until deleted.

11.3 **Certification.** On Customer's written request, StitchOps will certify the deletion in writing, which satisfies Clauses 8.5 and 16(d) of the Standard Contractual Clauses.

12. International Transfers

12.1 **Standard Contractual Clauses.** For a Restricted Transfer from the European Economic Area, the Standard Contractual Clauses are incorporated by reference with Customer as data exporter and StitchOps as data importer. By entering into this DPA, the parties are deemed to sign them, with these choices: (a) Clause 7, the docking clause, applies; (b) Clause 9, Option 2, general written authorization, with the notice period in Section 7.3; (c) Clause 11, the optional redress language, does not apply; (d) Clause 13, as set out in Annex I.C; (e) Clause 17, the law of Ireland; and (f) Clause 18, the courts of Ireland. Annexes I and II of this DPA complete the appendix to the clauses.

12.2 **Switzerland.** For Restricted Transfers from Switzerland, the Standard Contractual Clauses apply as modified by Annex III.

12.3 **United Kingdom.** For Restricted Transfers from the United Kingdom, the UK Addendum applies as completed by Annex IV.

12.4 **Onward transfers.** StitchOps will make onward transfers of Personal Data to Subprocessors only under safeguards that Data Protection Laws accept.

13. United States Privacy Laws

Where U.S. Privacy Laws apply, StitchOps will (a) not sell or share Personal Data, as those terms are defined in U.S. Privacy Laws; (b) not retain, use, or disclose Personal Data for any purpose other than the business purposes in the Agreement, or outside the direct business relationship with Customer; (c) not combine Personal Data with personal data it receives from others or collects itself, except as U.S.

Privacy Laws allow; (d) comply with U.S. Privacy Laws and give the same level of privacy protection they require; (e) tell Customer if it can no longer meet its obligations under them; and (f) allow Customer, on reasonable notice, to take reasonable steps to stop and remediate unauthorized use of Personal Data.

14. Health Information

Customer will not submit protected health information under HIPAA to the Service unless the parties have signed a Business Associate Agreement. Where they have, the Business Associate Agreement controls over this DPA for that information.

15. Government Access Requests

If a government authority asks StitchOps for Personal Data, StitchOps will (a) try to redirect the authority to Customer; (b) notify Customer promptly, unless the law prohibits it; (c) challenge requests it reasonably believes are unlawful or overbroad; and (d) disclose only the minimum the law requires. StitchOps has not received any such request to date.

16. Affiliates

Customer remains responsible for coordinating all communication with StitchOps under this DPA for itself and its Affiliates, and will exercise any rights under this DPA on their behalf in a combined manner. Use of the Service by Customer's Affiliates is subject to the Agreement.

17. Liability

Each party's liability under this DPA, together with its Affiliates and including all claims under any Standard Contractual Clauses, is subject to the limitations of liability in the Agreement, including Section 9.2 of the Master Subscription Agreement. Nothing in this Section limits a party's liability to Data Subjects under the Standard Contractual Clauses.

18. Order of Precedence and Updates

18.1 **Precedence.** For matters concerning Personal Data, this DPA controls over the Agreement. The Standard Contractual Clauses control over this DPA. The Agreement governs everything this DPA does not address.

18.2 **Updates.** StitchOps may update this DPA as described in Section 15.10 of the Master Subscription Agreement, including at least 30 days notice before a material change, and no update will materially reduce Customer's protections during the then current term. Prior versions are kept at https://www.stitchops.io/legal/archive.

Signatures

StitchOps, Inc.

Signature: _____

Name: Thomas Bieser

Title: Chief Executive Officer and Cofounder

Date: _____

Customer

Legal entity name: _____

Signature: _____

Name: _____

Title: _____

Date: _____

Annex I. Description of Processing

A. List of parties. Data exporter: the entity named as Customer in the Agreement or this DPA, at the address and contact in its Order Form. Activities: use of the Service under the Agreement. Role: Controller, or Processor on behalf of a third party Controller. Signature: by entering into this DPA, the data exporter is deemed to sign this Annex.

Data importer: StitchOps, Inc., 2707 Arapahoe Avenue #180, Boulder, CO 80302, United States. Contact: Kyle Harris, Chief Technology Officer and Data Protection Officer, privacy@stitchops.io. Activities: providing the Service and Professional Services under the Agreement. Role: Processor, or Subprocessor where Customer is a Processor.

B. Description of transfer.

(a) **Categories of Data Subjects.** As determined by Customer, typically Customer's employees, contractors, and other workforce members; job applicants and former workers whose records are in Customer's HR systems; and Users authorized to use the Service.

(b) **Categories of Personal Data.** In the Control Plane: account details for Customer's administrators and Users of the Service (such as name, work email, and role), workflow definitions and configuration, execution metadata such as status, timing, and errors, and any data Customer configures a workflow to send to the Control Plane. On the Digital Worker, in Customer's environment and under Customer's control: the data Customer's workflows handle, as Customer determines, typically identity and contact details, employment details from HR sources, and account identifiers, group memberships, roles, and entitlements in Customer Systems. Credentials, only where Customer asks StitchOps to store them.

(c) **Sensitive data.** None is required to use the Service. Customer may choose to Process special categories of data, such as health information, only as

permitted by Section 14 of this DPA and Section 2.6(b) of the Agreement, with the safeguards in Annex II.

(d) **Frequency.** Continuous during the term of the Agreement, as workflows run.

(e) **Nature of the Processing.** Executing, orchestrating, scheduling, monitoring, and reporting on the automated workflows Customer configures across Customer Systems, including through browser, desktop, and API automation.

(f) **Purpose.** To provide the Service and Professional Services under the Agreement.

(g) **Retention.** For the term of the Agreement, then as described in Section 11 of this DPA.

(h) **Transfers to Subprocessors.** For the purposes, locations, and data listed at https://www.stitchops.io/legal/subprocessors, for the term of the Agreement.

C. Competent supervisory authority. Where the data exporter is established in an EU Member State, the supervisory authority responsible for the data exporter. Where the data exporter is not established in the EU but has appointed a representative under Article 27(1) GDPR, the supervisory authority of the Member State where the representative is established. Otherwise, the supervisory authority of a Member State where the affected Data Subjects are located.

Annex II. Technical and Organizational Measures

The StitchOps Cloud, where the Control Plane runs, is covered by StitchOps' SOC 2 Type 2 examination (Security, Availability, Confidentiality, Processing Integrity, and Privacy) and its HIPAA and GDPR Article 5 attestations, performed by Sensiba LLP. Digital Workers, StitchOps Edge deployments, and customer managed credential vaults run on Customer's infrastructure under Customer's own controls, which keeps the Personal Data workflows handle in Customer's environment. Customer is responsible for securing, patching, and controlling access to that infrastructure. The measures below describe both. The full reports are available under NDA through the Trust Center at **https://trust.stitchops.io**.

(a) **Architecture.** Digital Workers connect outbound only over TLS 1.2 or higher and need no inbound ports. Screen content and field values stay on the Execution Infrastructure where the Digital Worker runs. Telemetry is free of content: no field values, screen images, or personal data from Customer Systems.

(b) **Encryption.** Data is encrypted in transit with TLS 1.2 or higher. Credentials that StitchOps stores at Customer's request are encrypted at rest using AWS Key Management Service envelope encryption and are resolved on the Digital Worker at run time. Other Customer Data in the Control Plane is encrypted at rest using AES 256.

(c) **Tenant isolation.** Every API request is scoped to a single tenant, and Customer Data is logically separated by tenant.

(d) **Access control.** Access to production systems is limited to named personnel who need it, requires multifactor authentication, and is logged. Customers can have their Users sign in through Customer's own identity provider using single sign on.

(e) **AI controls.** AI Features are optional and can be turned off for a tenant or a workflow. Credential values are never sent to an AI model, and Personal Data is not used to train AI models.

(f) **Change and vulnerability management.** StitchOps maintains a vulnerability management program and has independent penetration tests performed at least annually, with findings remediated by severity.

(g) **Logging and monitoring.** Workflow executions record status, timing, and redacted inputs and outputs for each step.

(h) **Incident response.** StitchOps maintains a documented incident response process and notifies customers as described in Section 8.

(i) **Backup and recovery.** Control Plane data is backed up at least daily, encrypted, and copied to a second AWS region. Backups are kept for no more than 35 days. StitchOps tests restoring from backup at least annually. Because Personal Data that workflows handle stays on Customer's Execution Infrastructure, Customer's own backup practices govern that data.

(j) **Personnel.** Personnel sign confidentiality agreements and complete security and privacy training at onboarding and on the schedule StitchOps' SOC 2, GDPR, and HIPAA programs require.

(k) **Subprocessors.** StitchOps assesses the security of each Subprocessor before engaging it and binds it to written terms at least as protective as this DPA.

Annex III. Transfers from Switzerland

For transfers of Personal Data subject to the Swiss FADP, the Standard Contractual Clauses apply with these changes: (a) references to the GDPR, the EU, or Member State law are read as references to the equivalent Swiss law; (b) the Swiss Federal Data Protection and Information Commissioner is the competent supervisory authority for those transfers; and (c) Data Subjects habitually resident in Switzerland may bring claims in the courts of Switzerland.

Annex IV. Transfers from the United Kingdom

For Restricted Transfers from the United Kingdom, the UK Addendum is incorporated by reference and completed as follows. Table 1, the parties: as set out in Annex I.A. Table 2, the selected clauses and modules: the Standard Contractual Clauses as chosen in Section 12.1 of this DPA. Table 3, the appendix information: Annex I (parties and description of transfer), Annex II (technical and organizational measures), and the Subprocessor list at **https://www.stitchops.io/legal/subprocessors**. Table 4: the data importer may end the UK Addendum as set out in its Section 19. Part 2, the mandatory clauses: those of the UK Addendum template B1.0 issued by the UK Information Commissioner, as revised under its Section 18.

StitchOps, Inc., a Delaware corporation, 2707 Arapahoe Avenue #180, Boulder, CO 80302. Questions: legal@stitchops.io