DATA PROCESSING AGREEMENT

This Data Processing Agreement ("Agreement") forms part of the Contract for Services ("Principal Agreement") between

[CUSTOMER — full legal name] [CUSTOMER — registered address line 1] [CUSTOMER — registered address line 2 / city / postcode / country]

(the "Customer")

and

Convergence Tech Inc., a Delaware corporation 156 2nd Street, San Francisco, CA 94110, USA Registered office: 850 New Burton Road, Suite 201, Dover, DE 19904, USA (c/o Cogency Global Inc., registered agent)

(the "Data Processor")

(together as the "Parties")

WHEREAS

(A) The Customer acts as a Data Controller. (B) The Customer wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor. (C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1 "**Agreement**" means this Data Processing Agreement and all Schedules;

1.1.2 "**Customer Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of Customer pursuant to or in connection with the Principal Agreement;

1.1.3 "**Contracted Processor**" means a Subprocessor;

1.1.4 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.5 "**EEA**" means the European Economic Area;

1.1.6 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.7 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.8 "**Data Transfer**" means:

1.1.8.1 a transfer of Customer Personal Data from the Customer to a Contracted Processor; or

1.1.8.2 an onward transfer of Customer Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.9 "**Services**" means **the services described in Schedule 1 (Description of Processing)** the Customer provides.

1.1.10 "**Subprocessor**" means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Customer in connection with the Agreement.

1.2 The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Customer Personal Data

2.1 Processor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Customer Personal Data; and

2.1.2 not Process Customer Personal Data other than on the relevant Customer's documented instructions.

2.2 The Customer instructs Processor to process Customer Personal Data **as described in Schedule 1 (Description of Processing)**.

3. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Customer Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Customer Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and 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, Processor shall in relation to the Customer Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR. **The technical and organizational measures implemented by Processor as of the Effective Date are set out in Schedule 2 (Technical and Organizational Measures).**

4.2 In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Subprocessing

5.1 Processor shall not appoint (or disclose any Customer Personal Data to) any Subprocessor unless required or authorized by the Customer. **The Customer provides general written authorization for Processor to engage the Subprocessors listed in Schedule 3 (Subprocessors), and to engage additional Subprocessors subject to Processor giving the Customer at least thirty (30) days' prior written notice (which may be by email or by updating the public Subprocessor list at the URL set out in Schedule 3) of any intended changes. The Customer may object to any new Subprocessor on reasonable data-protection grounds within that notice period.**

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Processor shall assist the Customer by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer obligations, as reasonably understood by Customer, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

6.2.1 promptly notify Customer if it receives a request from a Data Subject under any Data Protection Law in respect of Customer Personal Data; and

6.2.2 ensure that it does not respond to that request except on the documented instructions of Customer or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Customer of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 Processor shall notify Customer without undue delay upon Processor becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information to allow the

Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Processor shall co-operate with the Customer and take reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

Processor shall provide reasonable assistance to the Customer with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Customer reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of Customer Personal Data

9.1 Subject to this section 9 Processor shall promptly and in any event within 10 business days of the date of cessation of any Services involving the Processing of Customer Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those Customer Personal Data.

9.2 Processor shall provide written certification to Customer that it has fully complied with this section 9 within 10 business days of the Cessation Date.

10. Audit rights

10.1 Subject to this section 10, Processor shall make available to the Customer on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Customer or an auditor mandated by the Customer in relation to the Processing of the Customer Personal Data by the Contracted Processors.

10.2 Information and audit rights of the Customer only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. Data Transfer

11.1 The Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Customer. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data. **The Customer hereby consents to the transfer of Customer Personal Data to the United States and to the Subprocessor locations identified in Schedule**

3, with the EU Commission's Standard Contractual Clauses (Module 2: Controller-to-Processor; Module 3: Processor-to-Processor as applicable) deemed incorporated by reference where required.

12. General Terms

12.1 **Confidentiality.** Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("**Confidential Information**") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law; (b) the relevant information is already in the public domain.

12.2 **Notices.** All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address. Notices to the Data Processor shall be sent to **ankur@bitfab.ai**.

13. Governing Law and Jurisdiction

13.1 This Agreement is governed by the laws of **the State of Delaware, United States of America**.

13.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of **the State of Delaware**, subject to possible appeal to **the federal courts located in the District of Delaware**.

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

Customer

Signature: _____

Name: **[CUSTOMER]**

Title: **[CUSTOMER]**

Date Signed: **[CUSTOMER]**

Processor — Convergence Tech Inc.

Signature: _____

Name: **Ankur Toshniwal**

Title: **Chief Executive Officer**

Date Signed: _____

SCHEDULE 1 — DESCRIPTION OF PROCESSING (Article 28(3) GDPR)

Subject matter of the processing. Provision of **Bitfab**, an LLM observability and evaluation platform (the "Service"), under the Principal Agreement. The Service ingests execution traces (records of LLM calls and surrounding application context) sent by the Customer via Bitfab SDKs, and stores, indexes, displays, and (where the Customer configures it) automatically grades or replays those traces.

Duration of the processing. For the term of the Principal Agreement, plus the deletion period set out in Section 9 of this Agreement.

Nature and purpose of the processing. Processor receives, stores, indexes, queries, displays, and (where the Customer configures it) runs automated evaluations or extractions over Customer Personal Data, solely to provide the Service to the Customer.

Type of Personal Data. The Customer controls what Personal Data is sent to the Service. Such data may include, depending on the Customer's use:

- Identifiers and contact details (e.g., user IDs, names, email addresses, IP addresses);
- Application interaction data (e.g., prompts, completions, tool calls, session/trace metadata);
- Free-form content submitted by the Customer's end users that may contain Personal Data;
- Account data of the Customer's authorized users (name, email, login identifiers).

The Service is not designed to process Special Categories of Personal Data (Article 9 GDPR) or criminal-conviction data (Article 10 GDPR). The Customer shall not knowingly transmit such categories without prior written agreement.

Categories of Data Subjects. The Customer controls who its end users are. Such Data Subjects may include the Customer's customers, end users, employees, contractors, and website visitors.

Obligations and rights of the Customer. As set out in this Agreement, the Principal Agreement, and applicable Data Protection Laws.

SCHEDULE 2 — TECHNICAL AND ORGANIZATIONAL MEASURES (Article 32 GDPR)

1. Encryption. - Data in transit: TLS 1.2 or higher for all external endpoints. - Data at rest: AES-256 (or equivalent) for primary database and object storage at the Subprocessor layer.

2. Access control. - Single sign-on (SSO) and multi-factor authentication for personnel with access to production systems. - Role-based access on a least-privilege basis; access reviewed periodically. - Customer-tenant isolation enforced at the application layer; row-level scoping by organization identifier.

3. Network and infrastructure security. - Production workloads run within Subprocessor-managed cloud environments (see Schedule 3) protected by virtual private network controls, security groups, and managed firewalls. - Secrets stored in a managed secret store; not committed to source control.

4. Resilience and recovery. - Managed Postgres provider (Neon) provides point-in-time recovery. - Regular backup verification.

5. Vulnerability management. - Automated dependency scanning and patching. - Application error and performance monitoring (Sentry) with alerts to on-call personnel.

6. Personnel. - All personnel with access to Customer Personal Data are subject to written confidentiality obligations. - Security and privacy training on onboarding and at least annually thereafter.

7. Logging and monitoring. - Application-level audit logging of administrative actions on Customer Personal Data. - Centralized log aggregation with retention sufficient to support incident investigation.

8. Incident response. - Documented incident-response procedure covering detection, escalation, containment, eradication, recovery, and post-incident review. - Personal Data Breach notification to the Customer without undue delay and, in any event, within seventy-two (72) hours of confirmation, as required by Section 7 of this Agreement.

9. Subprocessor due diligence. - All Subprocessors are bound by written contracts containing data-protection terms no less protective than those of this Agreement, in line with Article 28(4) GDPR.

10. Deletion and disposal. - On Cessation Date, deletion of Customer Personal Data per Section 9 of this Agreement.

SCHEDULE 3 — SUBPROCESSORS

Public list URL. `https://www.bitfab.ai/trust`

Subprocessor	Purpose	Location of processing
Amazon Web Services, Inc. (AWS)	Object storage (S3); supporting cloud infrastructure	United States
Google LLC (Google Cloud Platform)	Cloud infrastructure	United States
Neon Inc.	Managed Postgres database	United States (configurable region)
Vercel Inc.	Web application hosting / edge	United States
Inngest Inc.	Background job execution and scheduling	United States
Clerk Inc.	Authentication and identity	United States
OpenAI, L.L.C.	LLM inference for Service features	United States
Anthropic PBC	LLM inference for Service features	United States
Google LLC (Gemini API)	LLM inference for Service features	United States
Stripe, Inc.	Payment processing and billing	United States
Twilio Inc. (SendGrid)	Transactional email delivery	United States
PostHog Inc.	Product analytics	United States
Functional Software, Inc. (Sentry)	Error and performance monitoring	United States

For non-EEA transfers (all of the above are US-based at present), the Parties rely on the EU Standard Contractual Clauses as described in Section 11.