DATA PROCESSING AGREEMENT

Version 2.1 · 24 September 2026 · Convergence Tech Inc. (Bitfab)

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

> [CUSTOMER - full legal name]
> [CUSTOMER - registered address line 1]
> [CUSTOMER - city, postcode, country]
> **(the "Customer")**

and

> Convergence Tech Inc., a Delaware corporation doing business as Bitfab
> 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 "Processor")**

(together, the "**Parties**")

WHEREAS

(A) The Customer acts as a Data Controller, or as a Processor on behalf of one or more Data Controllers. (B) The Customer wishes to subcontract certain Services, which imply the processing of personal data, to the 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 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 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 the Customer pursuant to or in connection with the Principal Agreement;

1.1.3 "**Contracted Processor**" means the Processor or 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 the GDPR together with any national laws implementing or supplementing it and, where applicable, the UK GDPR read with the Data Protection Act 2018 and the Swiss Federal Act on Data Protection, in each case as amended, replaced, or superseded from time to time;

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

1.1.8 "**Data Transfer**" means (a) a transfer of Customer Personal Data from the Customer to a Contracted Processor, or (b) an onward transfer of Customer Personal Data from a Contracted Processor to a Subprocessor, or between two establishments of a Contracted Processor;

1.1.9 "**Services**" means the services described in Schedule 1 (Description of Processing), which the Processor provides to the Customer under the Principal Agreement;

1.1.10 "**Subprocessor**" means any person, other than an employee of the Processor, appointed by or on behalf of the Processor to Process Customer Personal Data on behalf of the Customer in connection with this Agreement;

1.1.11 "**Standard Contractual Clauses**" or "**SCCs**" means the standard contractual clauses for the transfer of personal data to third countries annexed to European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as completed in Schedule 4 (Standard Contractual Clauses);

1.1.12 "**UK Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018, version B1.0, in force 21 March 2022;

1.1.13 "**Restricted Transfer**" means a Data Transfer that would be prohibited by Data Protection Laws in the absence of a transfer mechanism recognized by those laws.

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

1.3 A reference to a Schedule is a reference to a Schedule to this Agreement, and the Schedules form part of it.

2. Processing of Customer Personal Data

2.1 The Processor shall:

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

2.1.2 not Process Customer Personal Data other than on the Customer's documented instructions, including with regard to Data Transfers, unless Processing is required by Union or Member State law to which the Processor is subject, in which case the Processor shall inform the Customer of

that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest; and

2.1.3 inform the Customer without delay if, in the Processor's opinion, an instruction infringes Data Protection Laws. The Processor may suspend the affected Processing until the instruction is confirmed, withdrawn, or amended.

2.2 The Customer instructs the Processor to Process Customer Personal Data as described in Schedule 1 (Description of Processing). This Agreement, the Principal Agreement, and the Customer's configuration and use of the Services are the Customer's complete documented instructions to the Processor as at the Effective Date. Additional or different instructions require written agreement between the Parties.

2.3 The Customer is responsible for the lawfulness of the Customer Personal Data it transmits to the Services and for having a lawful basis for the Processing it instructs.

3. Processor Personnel

The Processor shall take reasonable steps to ensure the reliability of any employee, agent, or contractor of any Contracted Processor who may have access to Customer Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know or 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, the Processor shall in relation to 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 measures implemented by the Processor as at the Effective Date are set out in Schedule 2 (Technical and Organizational Measures).

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

4.3 The Processor may update the measures in Schedule 2 from time to time, provided that no update materially reduces the overall level of protection afforded to Customer Personal Data.

5. Subprocessing

5.1 **General authorization.** The Customer grants the Processor general written authorization to engage the Subprocessors listed in Schedule 3 (Subprocessors). The Processor shall not otherwise appoint, or disclose any Customer Personal Data to, a Subprocessor except in accordance with this section 5.

5.2 **Notice of changes.** The Processor shall give the Customer at least thirty (30) days' prior notice of the addition or replacement of a Subprocessor. Notice is given by email to the Customer's notice address under the Principal Agreement, and the public list at the URL in Schedule 3 is updated at the same time.

5.3 **Objection.** The Customer may object to a new Subprocessor in writing, on reasonable data-protection grounds, within the notice period. The Parties shall work in good faith to resolve the objection. If they cannot resolve it, the Customer may terminate the affected Services on written notice and receive a pro rata refund of fees prepaid for the terminated portion of the Services.

5.4 **Flow-down.** Before a Subprocessor Processes any Customer Personal Data, the Processor shall enter into a written contract with that Subprocessor imposing data protection obligations no less protective than those in this Agreement, in particular the obligations required by Article 28(3) of the GDPR and appropriate technical and organizational measures under Article 32 of the GDPR.

5.5 **Liability.** The Processor remains fully liable to the Customer for the performance of each Subprocessor's data protection obligations.

6. Data Subject Rights

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

6.2 The Processor shall:

6.2.1 promptly notify the 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 the Customer or as required by applicable laws to which the Processor is subject, in which case the Processor shall, to the extent permitted by those laws, inform the Customer of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 The Processor shall notify the Customer without undue delay, and in any event within seventy-two (72) hours, after the Processor becomes aware of a Personal Data Breach affecting Customer Personal Data. The Processor becomes aware once it has a reasonable degree of certainty that a security incident has occurred that led to Customer Personal Data being compromised. Notification is not conditional on the Processor having completed its investigation, and is not an acknowledgement of fault or liability.

7.2 The notification shall provide the Customer with sufficient information to allow the Customer to meet any obligation to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws, including, to the extent then known: the nature of the breach, the categories and

approximate number of Data Subjects and records concerned, the likely consequences, the measures taken or proposed to address the breach and mitigate its effects, and a contact point at the Processor. Where the information is not available at once, the Processor shall provide it in phases without further undue delay.

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

8. Data Protection Impact Assessment and Prior Consultation

The Processor shall provide reasonable assistance to the Customer with any data protection impact assessments, and prior consultations with supervisory authorities or other competent data privacy authorities, which the 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 the information available to, the Contracted Processors.

9. Deletion or Return of Customer Personal Data

9.1 **Customer's election.** On cessation of any Services involving the Processing of Customer Personal Data (the "**Cessation Date**"), the Processor shall, at the Customer's election, return the Customer Personal Data to the Customer or delete it. The Customer may notify its election in writing at any time before, or within thirty (30) days after, the Cessation Date. Return is made in a commonly used, machine-readable format, through the export functionality of the Services or another method the Parties agree.

9.2 **Timing.** Where the Customer elects deletion, or makes no election within the period in section 9.1, the Processor shall delete and procure the deletion of all copies of Customer Personal Data from live systems promptly, and in any event within ten (10) business days of the later of the Cessation Date and the end of that election period. Where the Customer elects return, the Processor shall make the Customer Personal Data available within that same period and delete it within ten (10) business days after the return is complete.

9.3 **Backups.** Copies held in encrypted backups are deleted on the Processor's ordinary rolling backup cycle, which does not exceed thirty-five (35) days. Until deleted, those copies remain subject to this Agreement, and the Processor shall not Process them for any purpose other than storage and restoration of the backup as a whole.

9.4 **Retention required by law.** The Processor may retain Customer Personal Data to the extent, and for as long as, required by Union, Member State, or other applicable law to which the Processor is subject. Where it does, the Processor shall inform the Customer of the retention and its legal basis unless that law prohibits it, isolate and protect the retained data, Process it only for the purpose that requires retention, keep it confidential, and delete it once the retention requirement ends.

9.5 **Certification.** The Processor shall provide written certification to the Customer that it has complied with this section 9 within ten (10) business days of completing the deletion or return, identifying any Customer Personal Data retained under section 9.4 and the basis for that retention.

10. Audit Rights

10.1 Subject to this section 10, the 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 Customer Personal Data by the Contracted Processors.

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

11. Data Transfer

11.1 **Authorized transfers.** The Customer authorizes the Processor to transfer Customer Personal Data to the United States and to the Subprocessor locations identified in Schedule 3, subject to the remainder of this section 11.

11.2 **EEA transfers.** Where a Restricted Transfer of Customer Personal Data subject to the GDPR takes place, the Parties are bound by the SCCs, which are incorporated into this Agreement in full and completed as set out in Schedule 4, Part A. Module Two (Controller to Processor) applies where the Customer acts as a Controller. Module Three (Processor to Processor) applies where the Customer acts as a Processor on behalf of a third-party Controller.

11.3 **UK transfers.** Where a Restricted Transfer of Customer Personal Data subject to the UK GDPR takes place, the UK Addendum applies to the SCCs and is completed as set out in Schedule 4, Part B.

11.4 **Swiss transfers.** Where a Restricted Transfer of Customer Personal Data subject to the Swiss Federal Act on Data Protection takes place, the SCCs apply with the modifications set out in Schedule 4, Part C.

11.5 **Precedence.** In the event of a conflict between the SCCs and any other term of this Agreement or the Principal Agreement, the SCCs prevail.

11.6 **Alternative mechanism.** If the Processor adopts an alternative transfer mechanism recognized under Data Protection Laws, including an adequacy decision or a certification under the EU-US Data Privacy Framework and its UK and Swiss extensions, that mechanism applies to the transfer in place of the SCCs to the extent it lawfully covers the transfer, and the Processor shall notify the Customer.

11.7 **Text of the SCCs.** The full text of the SCCs is published at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj. By signing this Agreement each Party is taken to have signed the SCCs, including

their Annexes, as completed in Schedule 4. On the Customer's request the Processor will provide a separately executable copy of the SCCs completed with the Parties' details.

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, or (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, or to such other address as notified from time to time by the Parties changing address. Notices to the Processor are sent to ankur@bitfab.ai.

12.3 **Order of precedence.** On matters relating to the Processing of Customer Personal Data, the SCCs prevail over this Agreement, and this Agreement prevails over the Principal Agreement.

13. Governing Law and Jurisdiction

13.1 This Agreement is governed by the laws of the State of Delaware, United States of America, except that the SCCs are governed by the law identified in Schedule 4 as required by Clause 17 of the SCCs.

13.2 Any dispute arising in connection with this Agreement which the Parties are not 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, and subject to Clause 18 of the SCCs where the SCCs apply.

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below (the "**Effective Date**").

Customer	**Processor · Convergence Tech Inc.**
Signature	Signature
Name	Name: Ankur Toshniwal
Title	Title: Chief Executive Officer
Date signed	Date signed

Schedule 1 · Description of Processing

Article 28(3) GDPR. This Schedule is also Annex I.B to the SCCs.

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 through Bitfab SDKs, and stores, indexes, displays, and, where the Customer configures it, automatically grades or replays those traces.
Duration of the processing	The term of the Principal Agreement, plus the deletion or return periods set out in section 9 of this Agreement.
Nature and purpose of the processing	The Processor receives, stores, indexes, queries, displays, and, where the Customer configures it, runs automated evaluations, extractions, or replays over Customer Personal Data, solely to provide the Service to the Customer. Where the Customer enables database snapshots, the Processor also copies and stores a snapshot of a Customer database the Customer connects, so that a trace can be replayed against the database state at capture time.
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 (for example user IDs, names, email addresses, IP addresses); application interaction data (for example prompts, completions, tool calls, session and 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); and, where the Customer enables database snapshots, the contents of the Customer database the Customer connects.
Special categories of Personal Data	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. Protected Health Information subject to HIPAA requires a separate executed Business Associate Agreement.
Categories of Data Subjects	The Customer controls who its end users are. Data Subjects may include the Customer's customers, end users, employees, contractors, and website visitors.
Frequency of the transfer	Continuous, for as long as the Customer's instrumented applications send traces to the Service and the Customer uses the dashboard.
Retention period	Customer Personal Data is retained for the term of the Principal Agreement, subject to any shorter retention the Customer configures, and is then deleted or returned under section 9.
Subject matter and duration for Subprocessors	As set out in Schedule 3, for the duration of the relevant Subprocessor engagement and no longer than the periods above.
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. This Schedule is also Annex II to the SCCs.

1. **Encryption.** Data in transit is protected with TLS 1.2 or higher on all external endpoints. Data at rest is protected with AES-256 or equivalent for the primary database and object storage at the Subprocessor layer.
2. **Access control.** Single sign-on and multi-factor authentication for personnel with access to production systems. Role-based access on a least-privilege basis, reviewed periodically. Customer-tenant isolation enforced at the application layer, with 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 are held in a managed secret store and are not committed to source control.
4. **Resilience and recovery.** The managed Postgres provider (Neon) provides point-in-time recovery. Backups are verified regularly.
5. **Vulnerability management.** Automated dependency scanning and patching. Application error and performance monitoring 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 is delivered 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 the Processor becoming aware of the breach, 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. Measures no less protective than those in this Schedule apply to Processing carried out by a Subprocessor.
10. **Data minimization.** The Customer controls what data its instrumentation sends to the Service. The Processor retains Customer Personal Data only for the configured retention period.
11. **Deletion and disposal.** On the Cessation Date, Customer Personal Data is deleted or returned under section 9 of this Agreement.

Schedule 3 · Subprocessors

Article 28(4) GDPR. This Schedule is also Annex III to the SCCs. The current list is published at https://www.bitfab.ai/trust. Changes are notified under section 5.2.

Subprocessor	Purpose	Customer Personal Data processed	Location of processing
Amazon Web Services, Inc. (AWS)	Object storage (S3) for large trace payloads; key management	Any Personal Data contained in trace payloads	United States
Google LLC (Google Cloud Platform)	Supporting cloud infrastructure	Any Personal Data contained in traces processed by that infrastructure	United States
Neon Inc.	Managed Postgres database for traces, metadata, and account data; per-organization database snapshot storage	All structured Customer Personal Data	United States (configurable region)
Vercel Inc.	Web application hosting and edge network	Request metadata (headers, IP address); trace content in transit	United States
Upstash, Inc.	Managed Redis for ephemeral session and event state	Session, user, and organization identifiers; short-lived agent event payloads	United States
Inngest Inc.	Background job execution and scheduling	Job payloads referencing trace identifiers	United States
Axiom, Inc.	Structured application logging and log retention	Request metadata, user and organization identifiers, error details. Trace content is not logged.	United States
Functional Software, Inc. (Sentry)	Error and performance monitoring	Error diagnostics including user identifiers. Trace content is scrubbed.	United States
PostHog Inc.	Product analytics on the Bitfab dashboard	Dashboard usage events and user identifiers. No trace content.	United States
Stripe, Inc.	Payment processing and billing	Billing contact and account data. No trace content.	United States
OpenAI, L.L.C.	LLM inference for Service features (engaged only where the Customer configures graders, agents, or extractions)	Trace content submitted to the model for that feature	United States
Anthropic PBC	LLM inference for Service features (engaged only where the Customer configures graders, agents, or extractions)	Trace content submitted to the model for that feature	United States

Subprocessor	Purpose	Customer Personal Data processed	Location of processing
Google LLC (Gemini API, Vertex AI)	LLM inference for Service features (engaged only where the Customer configures graders, agents, or extractions)	Trace content submitted to the model for that feature	United States
Ardent (tryardent.com)	Database snapshot connector, engaged only where the Customer enables database snapshots: copies a Customer database the Customer connects into Processor-managed infrastructure	The contents of the Customer database the Customer connects, which may include Personal Data	United States

Where a Subprocessor is described as engaged only for a specific feature, it Processes Customer Personal Data only if the Customer enables that feature.

Schedule 4 · Standard Contractual Clauses

Completion of the SCCs, the UK Addendum, and the Swiss modifications referred to in section 11.

Part A · EU Standard Contractual Clauses (Decision (EU) 2021/914)

The SCCs are incorporated into this Agreement in full and apply to every Restricted Transfer of Customer Personal Data subject to the GDPR, with the following elections. By signing this Agreement each Party is taken to have signed the SCCs and their Annexes.

Modules	Module Two (Controller to Processor) applies where the Customer acts as a Controller. Module Three (Processor to Processor) applies where the Customer acts as a Processor on behalf of a third-party Controller. Clauses that apply only to other Modules do not apply.
Data exporter	The Customer, as identified in the heading and signature block of this Agreement. Role: Controller (Module Two) or Processor (Module Three). Contact: the Customer's notice address under the Principal Agreement. Activities relevant to the transfer: Schedule 1.
Data importer	Convergence Tech Inc., 156 2nd Street, San Francisco, CA 94110, USA. Role: Processor. Contact: Ankur Toshniwal, ankur@bitfab.ai. Activities relevant to the transfer: Schedule 1.
Clause 7 (Docking clause)	Applies.
Clause 9(a) (Use of sub-processors)	Option 2 (general written authorization) applies. The agreed notice period for changes is thirty (30) days, as set out in section 5.2.
Clause 11(a) (Redress)	The optional independent dispute resolution wording does not apply.
Clause 13 and Annex I.C (Competent supervisory authority)	The supervisory authority of the Member State in which the Customer is established. Where the Customer is not established in the EEA, the supervisory authority of the Member State in which the Customer's Article 27 representative is established or, failing that, the supervisory authority of the Member State in which the relevant Data Subjects are located: `[CUSTOMER - competent supervisory authority]`.
Clause 17 (Governing law)	Option 1 applies. The SCCs are governed by the law of Ireland.
Clause 18(b) (Choice of forum and jurisdiction)	The courts of Ireland.
Annex I.A (List of Parties)	The data exporter and data importer rows above.
Annex I.B (Description of transfer)	Schedule 1.
Annex II (Technical and organizational measures)	Schedule 2.
Annex III (List of sub-processors)	Schedule 3, authorized under Clause 9(a) Option 2 (general written authorization).

Part B · UK International Data Transfer Addendum (version B1.0)

The UK Addendum applies to every Restricted Transfer of Customer Personal Data subject to the UK GDPR, completed as follows.

Table 1 (Parties)	Exporter and importer as set out in Part A, with the details in the heading and signature block of this Agreement. Start date: the Effective Date.
Table 2 (Selected SCCs, Modules, and Clauses)	The SCCs as completed in Part A, including Module Two and Module Three, the Clause 7 docking clause, Clause 9(a) Option 2 with a thirty (30) day notice period, and Clause 11(a) without the optional wording.
Table 3 (Appendix information)	Annex 1A: the Party details in Part A. Annex 1B: Schedule 1. Annex II: Schedule 2. Annex III: Schedule 3.
Table 4 (Ending the Addendum when the Approved Addendum changes)	Neither Party.
Construction	References in the SCCs to the GDPR are read as references to the UK GDPR, references to a Member State are read as references to the United Kingdom, the competent supervisory authority is the Information Commissioner, and the SCCs as amended by the UK Addendum are governed by the laws of England and Wales with the courts of England and Wales having jurisdiction.

Part C · Switzerland

Where a Restricted Transfer of Customer Personal Data subject to the Swiss Federal Act on Data Protection takes place, the SCCs apply with the following modifications:

- the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner, and for transfers subject to both the GDPR and the Swiss FADP, the authority in Part A also applies to the extent the transfer is governed by the GDPR;
- references to the GDPR are read as references to the Swiss FADP to the extent the transfer is governed by it;
- the term "Member State" is not read so as to prevent Data Subjects in Switzerland from bringing proceedings in their place of habitual residence, in accordance with Clause 18(c) of the SCCs; and
- until the entry into force of the revised Swiss FADP, the SCCs also protect the data of legal entities to the extent the Swiss FADP requires it.