Storage Services Data Processing Addendum

This Storage Services Data Processing Addendum (“**DPA**”) supplements any agreement (including but not limited to statements of work, attachments, schedules, exhibits) between PacketFabric, Inc. (“PacketFabric”) and Partner (“Partner”) for the purchase of services, products or other technology solutions from PacketFabric to the extent PacketFabric Processes Personal Data on behalf of Partner (and/or its End-User(s), as the context below may require) (collectively the “**Agreement**”).

This DPA applies to all activities related to the Agreement and in which employees of PacketFabric or third parties commissioned by PacketFabric may Process Personal Data on behalf of Partner. It contains, in conjunction with the Agreement, the documented instructions for the Processing of Personal Data as well as the subject-matter, duration, nature, purpose of the Processing, and shall govern the rights and obligations of the parties in connection with the Processing of Personal Data.

1. Definitions

1.1 For the purpose of this DPA (i) **“PacketFabric”** means the PacketFabric entity executing the Agreement and/or the respective PacketFabric Affiliates Processing Personal Data on behalf of Partner as per the Agreement; (ii) “**Partner**” means the entity that is an authorized PacketFabric customer, executing the Agreement and/or the respective Partner Affiliates on whose behalf PacketFabric is Processing Personal Data as per the Agreement; as the context requires, the reference to “Partner” in this DPA may include its “**End-Users**” (as defined in the Agreement); (iii) **“Affiliate”** means, with respect to either party, an entity that is directly or indirectly controlling, controlled by, or under common control with a signatory of this DPA. For purposes of this definition, **“control”** means the power to direct the management and policies of such party, directly or indirectly, whether through ownership of voting securities, by contract or otherwise; and the term **“controlled”** has the meaning correlative to the foregoing. Upon request, each party will provide any other party with a list of all respective Affiliates relevant for this DPA; (iv) “**Data Controller**” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; (v) “**Data Processor**” means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller; (vi) “**Personal Data**” means any information relating to an identified or identifiable natural person (“**Data Subject**”)or household; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; (vii) “**Processing**”, “**Process**”, “**Processed**” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; (viii) **“GDPR”** means the European General Data Protection Regulation (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 the EU GDPR as saved into UK law by virtue of section 3 of the UK's European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 (collectively referred to for these purposes as the "UK GDPR"); and the Swiss Federal Data Protection Act of 19 June 1992 and its corresponding ordinances ("Swiss DPA"); (ix) the e-Privacy Directive (Directive 2002/58/EC) or any applicable national data protection laws made under or pursuant to or that apply in conjunction with (x) (in each case, as superseded, amended or replaced from time to time); (xi) “**Sell**” means any sharing or disclosure of Personal Data to a third party in exchange for monetary or other valuable consideration; (xii) ‘**Privacy Shield**” means agreement between the European Union (EU) and the United States of America (US) allowing for the transfer of personal data from the EU to US; (xiii) “**Alternative transfer mechanism**” means the alternative data export solution like Binding Corporate Rules or any new version of or successor to the SCCs or Privacy Shield adopted pursuant to applicable European Data Protection Law for the transfer of partner data as prescribed by applicable European Data Protection Laws.

2. Processing Personal Data on behalf of Partner

2.1 Any Processing of Personal Data by PacketFabric under this DPA shall occur only:
2.1.1 on behalf of Partner; and
2.1.2 in accordance with the Agreement; and
2.1.3 for the purpose of fulfillment of Partner’s instructions.
2.2 Without limiting the generality of Sections 2.1.1 through 2.1.3, PacketFabric agrees that it shall not: (i) Sell the Personal Data; (ii) retain, use, or disclose the Personal Data for any purpose other than for the specific purpose of performing functions under the Agreement, including retaining, using, or disclosing the Personal Data for a commercial purpose other than performing functions under the Agreement; (iii) retain, use, or disclose the Personal Data outside of the direct business relationship between PacketFabric and Partner. PacketFabric hereby certifies that it understands the restrictions set forth in this Section 2.2 and will comply with them.
2.3 Partner’s instructions for the Processing of Personal Data shall comply with applicable data protection laws and regulations. Partner shall have sole responsibility for the legitimacy, adequacy and accuracy of Personal Data and the means by which Partner acquired or collected Personal Data. If PacketFabric considers that an instruction of Partner may violate applicable data protection regulations, it shall notify Partner accordingly without any undue delay. This subsection 2.3 does not create an obligation of PacketFabric to actively monitor Partner’s instructions for legal compliance.
2.4 This DPA and the Agreement are Partner’s complete and final instructions at the time of signature of this DPA to PacketFabric for the Processing of Personal Data. However, such instructions may be amended, supplemented, or replaced by Partner in documented form at any time (new instruction). If such new instructions from Partner exceed the scope of the Agreement, they shall be considered as request to amend the Agreement and the parties shall commence good faith negotiations on this change request.
2.5 If, for any reason, PacketFabric is unable to comply with an agreed instruction, PacketFabric will inform Partner of this fact without undue delay. Partner may then suspend the transfer of Personal Data to PacketFabric, restrict the access to it, request all Personal Data to be returned to Partner and / or terminate the Agreement as per the terms of the Agreement.
2.6 PacketFabric will Process Personal Data as necessary to perform the services and / or deliver products and / or other technology solutions pursuant to the Agreement and as further instructed by Partner in its use of the above.
2.7 PacketFabric will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing or required / allowed by applicable law.

2.8 The categories of data subjects affected by the Processing of Personal Data on behalf of Partner within the scope of this DPA result from the Agreement and in particular from Partner's individual usage of services / products / or other technology solutions provided by PacketFabric. They typically include: employees, agents, advisors, freelancers of Partner (who are natural persons), etc.
2.9 The types of Personal Data affected by the Processing on behalf of Partner within the scope of this DPA result from the Agreement and in particular from Partner's individual usage of (and input into) the services / products / or other technology solutions provided by PacketFabric. They typically include: name, contact information (company, title / position, email address, phone number, physical address), connection data, location data, video / call (recordings) data and metadata derived thereof, etc.

3. PacketFabric's personnel

3.1 PacketFabric shall:
3.1.1 ensure all employees involved in Processing of Personal Data on behalf of Partner have committed themselves to confidentiality in writing or are under an appropriate statutory obligation of confidentiality, are prohibited from Processing Personal Data without authorization and have received appropriate training on their responsibilities;
3.1.2 appoint in country / global data protection officer, to the extent required by the applicable law, and publish the contact details.

4. Security of processing

4.1 PacketFabric has implemented and shall maintain technical and organizational security measures that are appropriate with respect to the Processing of Personal Data that is undertaken on behalf of Partner. PacketFabric shall ensure a level of security appropriate to the risk of varying likelihood and severity for the rights and freedoms of natural persons and regularly check their abidance.
4.2 PacketFabric shall be entitled to modify its technical and organizational measures as long as an at least equivalent level of security appropriate to the risk of varying likelihood and severity for the rights and freedoms of natural persons is maintained. Additional technical and organizational measures and information concerning such measures may be specified in the Agreement.

5. Sub-processors (sub-contractors) and international Personal Data transfers

5.1 Sub-processor obligations - PacketFabric may engage sub-processors (sub-contractors) to Process Personal data on behalf of Partner and shall comply with any applicable data privacy law regarding the engagement of sub-processors (sub-contractors). PacketFabric shall make sure that at least equivalent data protection obligations, as set out in this DPA, are imposed on all sub-processors Processing Personal Data on behalf of European Economic Area or Switzerland ("**EEA / CH**") based Partner's by way of a contract or other legal act, in particular providing sufficient guarantees to implement appropriate technical and organizational measures.
5.2 Objections - Only applicable for EEA / CH based Partner's: A list of sub-processors that may be engaged by PacketFabric to Process Personal Data on behalf of EEA / CH based Partners can be requested by emailing legal@PacketFabric.com. Any objections of this list of sub-processors shall be sent by e-mail to legal@PacketFabric.com (i) referencing the full legal name (and other credentials) of Partner and the affected Agreement, (ii) including the copy of the respective purchase order, and (iii) providing the reason for the objection. If Partner exercises its right to objection, PacketFabric shall at its choice and sole discretion:
5.2.1 refrain from using the objected sub-processor to Process Personal Data on behalf of Partner and confirm this to Partner in writing, or
5.2.2 contact Partner and seek for an agreement on mitigation of the reason for the objection. If an agreement between the parties is reached, Partner shall revoke the objection, or
5.2.3 have the right to terminate the Agreement entirely or only with respect to the Processing on behalf of Partner for which the objected new sub- processor shall be engaged.
5.3 International Transfers and Scope - PacketFabric shall comply with any applicable data privacy law regarding international transfers of Personal Data. For any transfer of Personal Data from the EEA / CH to a country outside the EEA / CH the requirements of Chapter V GDPR must be fulfilled.
5.3.1 The transfers of Personal Data between PacketFabric Affiliates shall be governed by PacketFabric's Binding Corporate Rules. The PacketFabric Binding Corporate Rules (Processor) Policy is available by requesting via email to legal@PacketFabric.com and is incorporated herein by reference.
5.3.2 If PacketFabric transfers Personal Data originating from the EEA / CH to third party sub-processors (i.e., PacketFabric's sub-contractors that are not PacketFabric Affiliates) located in countries outside the EEA / CH that have not received a binding adequacy decision by the European Commission, such transfers shall be subject to (i) the terms of Standard Contractual Clauses (as per European Commission's Decision 2010/87/EU); or (ii) other appropriate transfer mechanisms that provide an adequate level of protection in compliance with the GDPR which shall be automatically incorporated by reference and form an integral part of this DPA, as follows:

- PacketFabric as a Controller. In relation to partner data that is protected by the EU GDPR and is processed in accordance with Section 2 of this DPA, the EU SCCs shall apply, completed as follows:

- Module One will apply;
- in Clause 7, the optional docking clause will apply;
- in Clause 11 *(Redress)*, the optional language will not apply;
- in Clause 17 *(Governing Law)*, Option 1 will apply, and the EU SCCs will be governed by English law;
- in Clause 18(b) *(Member State)*, disputes shall be resolved before the Supreme court of UK
- Annex I of the EU SCCs shall be deemed completed with the information set out in Schedule 1 of this DPA; and
- Subject to Sections 4.1. and 4.2. (Security & Audits) of this DPA, Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule 3 to this DPA.

- PacketFabric as a processor. In relation to partner data that is protected by the EU GDPR and is processed in accordance with Section 2 of this DPA, the EU SCCs shall apply, completed as follows:
- Module Two (Section 2.1.1.) or Three (Section 2.1.2.) will apply;
- in Clause 7, the optional docking clause will apply;
- in Clause 9 *(Use of sub-processors)*, Option 2 will apply, and the time period for prior notice of Sub-processor changes is identified in Section 4. above;
- in Clause 11, the optional language will not apply;

- in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the EU GDPR;
- in Clause 18(b), disputes shall be resolved before the courts of England and Wales
- Annex I of the EU SCCs shall be deemed completed with the information set out in Schedule 2 of this DPA; and
- Subject to Section 4 of this DPA, Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule 3 to this DPA;

- <u>Transfers relating to the UK and Switzerland.</u> Subject to UK Standard Contractual Clauses below, in relation to partner data that is protected by the UK GDPR or Swiss DPA, the EU SCCs as implemented under sub-paragraphs (i) and (ii) above will apply with the following modifications :
-
- references to "Regulation (EU) 2016/679" shall be interpreted as references to UK Privacy Laws or the Swiss DPA (as applicable);
- references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of UK Privacy Laws or the Swiss DPA (as applicable);
- references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to the "UK" or "Switzerland", or "UK law" or "Swiss law" (as applicable);
- the term "member state" shall not be interpreted in such a way as to exclude data subjects in the UK or Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., the UK or Switzerland);
- Clause 13(a) and Part C of Annex I are not used and the "competent supervisory authority" is the United Kingdom Information Commissioner or Swiss Federal Data Protection and Information Commissioner (as applicable);
- references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Information Commissioner" and the "courts of England and Wales" or the "Swiss Federal Data Protection and Information Commissioner" and "applicable courts of Switzerland" (as applicable);
- in Clause 17, the Standard Contractual Clauses shall be governed by the laws of England and Wales (as applicable); and
- with respect to transfers to which UK Privacy Laws apply, Clause 18 shall be amended to state "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may bring legal proceeding against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts", and with respect to transfers to which the Swiss DPA applies, Clause 18(b) shall state that disputes shall be resolved before the applicable courts of England and Wales.
- with respect to transfer to which the Swiss DPA applies, the SCCs also protect the data of legal entities until the entry into force of the revised Swiss Federal Data Protection Act.

- <u>UK Standard Contractual Clauses.</u> Only to the extent that and for so long as the EU SCCs as implemented in accordance with paragraphs “PacketFabric as a controller” and “Transfers relating to the UK and Switzerland” above cannot be used to lawfully transfer partner data protected by the UK GDPR to PacketFabric, the UK SCCs shall be incorporated into and form an integral part of this DPA and shall apply to transfers governed by the UK GDPR. For the purposes of the UK SCCs, the relevant Annexes of the UK SCCs shall be populated using the information contained in Schedules 1, 2 and 3 (as applicable) of this DPA.

- <u>Conflicts.</u> Neither party intend to contradict or restrict any of the provisions set forth in the SCCs and, accordingly, if and to the extent the SCCs conflict with any provision of the Agreement (including this DPA), the SCCs shall prevail to the extent of such conflict.
- <u>Privacy Shield.</u> Although PacketFabric does not rely on the Privacy Shield as a legal basis for transfers of partner data in light of the judgment of the Court of Justice of the EU in Case C-311/18, for so long as PacketFabric is self-certified to the Privacy Shield it shall continue to process partner data in compliance with the Privacy Shield Principles and agrees to notify Partner if it makes a determination that it can no longer meet its obligation to provide the level of protection as is required by the Privacy Shield Principles.

6. Requests from Data Subjects

6.1 PacketFabric shall, in accordance with applicable laws, promptly notify Partner if PacketFabric receives a request from Data Subject to exercise his rights, such as: right of access, right to rectification, restriction of Processing, erasure (“right to be forgotten”), data portability, object to the Processing, or right not to be subject to an automated individual decision making, etc. Taking into account the nature of the Processing, PacketFabric shall assist Partner by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Partner’s obligation to respond to Data Subject request under applicable data protection laws and regulations, including complying with a Personal Data deletion request if required by law. In addition, to the extent Partner, in its use of the services and / or products and / or other technology solutions provided by PacketFabric, does not have the ability to address Data Subject Request, PacketFabric shall upon Partner’s request assist Partner in responding to such Data Subject request, to the extent PacketFabric is legally permitted to do so and the response to such Data Subject request is required under applicable data protection laws and regulations. To the extent legally permitted, Partner shall be responsible for any costs arising from PacketFabric’s provision of such assistance.

7. Notification and incidents

7.1 PacketFabric shall:

7.1.1 Notify Partner of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized use of or disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed on behalf of the Partner ("**Personal Data Breach**") without undue delay after becoming aware of it , but in no event, more than forty-eight (48) hours after it becomes aware of any actual or reasonably suspected security breaches or unauthorized or attempted access to Personal Data within the Portal or control of PacketFabric;

7.1.2 Promptly provide Partner with full cooperation and assistance in respect of any Personal Data Breach and all information in PacketFabric's possession concerning the Personal Data Breach, including the following: (i) the possible cause and consequences of the breach; (ii) the categories of Personal Data involved; (iii) a summary of the possible consequences for the relevant Data Subjects; (iv) a summary of the unauthorized recipients of Personal Data; and (v) the measures taken by PacketFabric to mitigate any related risk and / or loss or damage or (potential loss or damage);

7.1.3 Not make any announcement or publish or otherwise authorize any broadcast of any notice or information about a Personal Data Breach (the "**Breach Notice**") without the prior written consent from Partner; and prior written approval by Partner of the content, media and timing of the Breach Notice unless such Beach Notice is mandatory under the applicable law.

8. Assistance to Partner

8.1 Upon written request of Partner and subject to reasonable remuneration which shall be subject to a separate agreement, PacketFabric shall assist Partner in ensuring compliance with any obligations applicable to Partner as per Articles 32 (Security of processing) 35 (Data protection impact assessment) and 36 (Prior consultation) GDPR, considering the nature of processing and the information available to PacketFabric. To the extent any other applicable data privacy law requires PacketFabric to assist Partner in ensuring compliance with such law, PacketFabric shall provide the mandatory assistance to Partner, subject to a separate agreement.

9. Return and deletion of Partner Personal Data

9.1 Personal Data (including any copy of it) shall be returned or deleted and not be kept longer than is required for the Processing purposes, unless (i) a longer retention period is required by applicable law or (ii) Partner instructs PacketFabric in writing (a) to keep certain Personal Data longer and PacketFabric agrees to follow such instruction or (b) return or delete certain Personal Data earlier.

9.2 The return or deletion of any data storage medium provided by Partner to PacketFabric shall be conducted without undue delay (i) after termination / expiration of the Processing activity or (ii) earlier as instructed by Partner.

10. Audits

10.1 Upon prior written request by Partner PacketFabric shall supply Partner with all information necessary to effectively perform an audit on PacketFabric's compliance with the terms of this DPA.

10.2 Upon prior written notice and within a reasonable term PacketFabric shall grant Partner access to its data Processing facilities, data files and documentation relevant for the Processing activities during its usual business hours without disturbances to the normal course of operations for the purpose of auditing PacketFabric's compliance with the terms of this DPA. For clarity purposes PacketFabric is not under an obligation to provide Partner with an access to its systems which Process Personal Data of other PacketFabric's customers / partners (Data Controllers). The engagement of a third- party auditor to conduct the audit on behalf of Partner shall be subject to PacketFabric's prior written consent, which may only be refused on due cause, and to an executed written confidentiality agreement between the third-party auditor, Partner and PacketFabric. Partner will provide PacketFabric any audit report(s) generated in connection with any audit under this Section 10.2. Partner may use the audit report(s) only for the purposes of meeting its regulatory audit requirements and / or confirming compliance with the requirements of this DPA. The audit report(s) shall constitute confidential information of the parties under the terms of the Agreement. This right to audit may be exercised once a year unless any specific cause requires exceptional further audits.

11. Miscellaneous

11.1 The term of this DPA corresponds to the term of the Agreement. The terms which by their nature are intended to survive termination or expiration of this DPA, will continue and survive any termination or expiration of this DPA.

11.2 Notwithstanding anything to the contrary in the Agreement, in the event of a conflict between the terms of this DPA and the terms of the Agreement, the terms of this DPA shall prevail.

SCHEDULE 1

Controller to Controller (C 2 C) TRANSFERS
Description of Processing Activities / Transfer

Annex 1(A) List of Parties:

Data Exporter	Data Importer
Name: the party identified as the "PARTNER" in the Agreement and this DPA.	**Name:** PacketFabric, Inc.
Contact Person's Name, position and contact details: As set out in the Agreement and/or Portal.	**Contact Person's Name, position and contact details:** Legal Department, legal@PacketFabric.com
Activities relevant to the transfer: See Annex 1(B) below	**Activities relevant to the transfer:** See Annex 1(B) below
Role: Controller	**Role:** Controller

Annex 1(B) Description of transfer:

Categories	Description
Categories of data subjects:	Data subjects include individuals that use PacketFabric services and/or products and may include: Representatives of PARTNER (administrators) End-users of the PARTNER (internal and external).
Categories of personal data:	Personal data may include: Account registration and management data (such assuch as name, contact details, company, geographic area, preferences, job title and password, billing data, data related to PARTNER communications and support (such as name, contact details and the content of communications), and usage data (including feedback or any other information related to utilization of services and/or products that you provide to PacketFabric)
Sensitive data:	Depending on the services and/or products selected by PARTNER, PARTNER may choose to run workloads containing sensitive data.
If sensitive data is transferred, the restrictions or safeguards shall apply:	Such restrictions or safeguards must fully take into consideration the nature of the data and the risks involved, for example, strict purpose limitation, access restrictions (including access only for staff have followed specialized training), keeping arecord of access to the data, restrictions for onward transfers or additional security measures.
Frequency of transfer:	Frequency of transfer depends on PARTNER's use of services and/or products.
Nature of processing:	PacketFabric's services and/or products are separated into two broad categories of: a) PacketFabric's transmission of the Customer's Data (referred to as Cloud Router Service, Core Service, Transporter, or Type 2 Service); and b) PacketFabric's storage of Customer's Data (referred to as Storage Service). These are set out in detail in the Agreement.
Purpose(s) of the data transfer and further processing:	PacketFabric will process the personal data for the following business purposes (i) account registration, (ii) order and purchase, (iii) PARTNER communications

	and support, (iv) promotions, (v) to operate and enhance PacketFabric offerings, and (vi) as further described in the Agreement.
Retention period:	See section “Return and deletion of PARTNER Personal Data” of this DPA.

Annex 1(C) <u>Competent supervisory authority</u>:

The competent supervisory authority, in accordance with Clause 13 of the New EU SCCs (Supervision), must be (i) the supervisory authority applicable to the data exporter in its European Economic Area (EEA) country of establishment or, (ii) where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) of the GDPR, or (iii) where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are located.

With respect to the processing of personal data to which the UK GDPR applies, the competent supervisory authority is the Information Commissioners Office (ICO).

With respect to the processing of personal data to which the Swiss DPA applies, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

SCHEDULE 2

(Controller to Processor AND Processor to Processor TRANSFERS)
Description of the Processing Activities / Transfer

Annex 1(A) List of Parties:

Data Exporter	**Data Importer**
Name: the party identified as the "PARTNER" in the Agreement and this DPA.	**Name:** PacketFabric, Inc.
Contact Person's Name, position and contact details: As set out in the Agreement and/or Portal.	**Contact Person's Name, position and contact details:** Legal Department, legal@PacketFabric.com
Activities relevant to the transfer: See Annex 1(B) below	**Activities relevant to the transfer:** See Annex 1(B) below
Role: Controller or Processor	**Role:** Processor

Annex 1(B) Description of transfer:

Categories	**Description**
Categories of data subjects:	There are two main categories of data subjects: 1) Personal data collected from PARTNER's end-users; 2) Personal data submitted as part of PARTNER data.
Categories of personal data:	Personal data collected from PARTNER's end-users Depending on the services and/or products selected by PARTNER, PacketFabric may process the following categories of personal data: 1) Name Username Email address; 2) Online identifiers such as IP addresses Geolocation data (based on IP address); 3) Personal data submitted as part of PARTNER Data Depending on the services and/or products selected by PARTNER, PARTNER may run workload. Such PARTNER workloads could include any information that is located in the PARTNER's environment, subject to PacketFabric's Acceptable Use Policy referred to in the Agreement.
Sensitive data:	Depending on the services and/or products selected by PARTNER, PARTNER may choose to run workloads containing sensitive data.
If sensitive data is transferred, the restrictions or safeguards shall apply:	Access Restrictions: PacketFabric does not access the workloads submitted by the PARTNER. The PARTNER must take into consideration the nature of the data and the risks involved prior to choosing to running workloads containing sensitive data. PacketFabric's Technical and Organizational Measures can be found in Schedule 3 below. Such restrictions or safeguards must fully take into consideration the nature of the data and the risks involved, for example strict purpose limitation, access restrictions (including access only for staff who have been provided specialized training by PARTNER), keeping a record of

	access to the data, restrictions for onward transfers or additional security measures.
Frequency of transfer:	PARTNER Data is transferred in accordance with PARTNER's documented lawful instructions as described in Section 2 of this DPA.
Nature of processing:	PARTNER Data transferred will be processed in accordance with the Agreement and this DPA.
Purpose(s) of the data transfer and further processing:	Solely for providing the services and/or products to PARTNER.
Retention period:	See section "Return and deletion of PARTNER Personal Data" of this DPA.

Annex 1(C) Competent supervisory authority:

The competent supervisory authority, in accordance with Clause 13 of the New EU SCCs (Supervision), must be (i) the supervisory authority applicable to the data exporter in its European Economic Area (EEA) country of establishment or, (ii) where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) of the GDPR, or (iii) where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are located.

With respect to the processing of personal data to which the UK GDPR applies, the competent supervisory authority is the Information Commissioners Office (ICO).

With respect to the processing of personal data to which the Swiss DPA applies, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

SCHEDULE 3

Technical and Organizational Measures

The following technical measures are in place across the services to protect the personal data processed by PacketFabric:

1) Encryption of personal data:

a) Encryption in transit: PARTNER Data is encrypted while in transit over any public network or wireless network via Transport Layer Security (TLS) using TLS 1.2 or greater, Internet Protocol Security (IPSEC), or Secure File Transfer Protocol (SFTP).
b) Encryption at rest: PARTNER data at rest is encrypted at customer discretion, using AES-256 Encryption.
c) Employee laptop encryption: Employee laptops are encrypted using full disk AES- 256 encryption.

2) Measures for ongoing confidentiality, integrity, availability and resilience of processing systems and services:

a) Confidentiality obligations: PacketFabric personnel are required to agree to confidentiality obligations before undertaking work for PacketFabric or accessing any PacketFabric facilities and/or systems.
b) Data handling and training's: PacketFabric requires security and privacy awareness training for all PacketFabric employees as well as acknowledgement and agreement to acceptable use and security policies for PacketFabric systems and data by all PacketFabric personnel.
c) Password policy: Password management systems enforce password policy requirements across applications, such as password complexity, rotation frequency, and account lockout after multiple failed login attempts.
d) Operational security & vulnerability response: PacketFabric monitors a variety of communication channels for operational and capacity management, security vulnerabilities, and PacketFabric's security and compliance team will promptly react to known operational issues and/or security vulnerabilities.
e) Network controls: PacketFabric utilizes firewalls and related technologies for access control between PacketFabric's networks and the Internet. Firewall access is restricted to a small set of administrators with appropriate seniority and authority. Firewalls are established with minimum rights necessary to accomplish tasks by role and access is authorized on a "deny by default" policy.
f) Network separation: PacketFabric maintains network separation based on company policy and system requirements.
g) Server operating system: PacketFabric uses a hardened operating system implementation customized for the PacketFabric storage services.
h) Backups: data in storage services can be replicated in multiple locations at customer discretion.

3) Measures for ensuring the ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident:

a) Business continuity plan: PacketFabric maintains internal practices, plans or procedures that are designed to reasonably ensure the services are uninterrupted during the term of the Agreement. PacketFabric will follow its business continuity plan in order to maintain the applicable service levels set forth in the documentation.
b) Backups: See Section 2(h) of this schedule.

4) Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

a) Certifications: PacketFabric has obtained AICPA SOC2 certification for its storage services and will maintain such certification or similar certification by a certifying third party auditor.
b) Software development lifecycle: The storage services are developed using a standardized and reviewed secure software development life cycle to reduce the risk of introducing security vulnerabilities into the storage services.
c) Penetration testing & vulnerability scans: PacketFabric has annual penetration testing performed by qualified third-party auditors. PacketFabric performs periodic vulnerability scans of its production infrastructure. Vulnerabilities identified are routinely documented, tracked, and resolved by the respective service team with oversight by the PacketFabric compliance.

5) Measures for user identification and authorization:

a) User roles: PARTNER has primary control over the creation, deletion, and suspension of user roles within the PARTNER's environment of the storage services.
b) Access management: Access management procedures define the request, approval, access provisioning and die-provisioning processes. PacketFabric logical access procedures restrict user access (local or remote) based on user job function for applications and databases (role/profile based appropriate access), and systems to ensure segregation of duties and are reviewed, administered, and documented based on on-boarding, resource re-assignment, or termination of personnel. Periodic PacketFabric user access reviews are routinely performed to ensure access is appropriate
c) Firewalls: Firewalls are used and configured to prevent unauthorized access to the environment.

6) Measures for the protection of Data during transmission:

Encryption in transit: See Section 1 of this Schedule.

7) Measures for the protection of data during storage:

a) Encryption at rest: See Section 1. of this Schedule.

b) Access control and privilege management: PacketFabric employs systems and processes to limit physical and logical access based on least privileges and according to job responsibilities designed to ensure that PARTNER data can only be accessed by authorized PacketFabric personnel. PacketFabric maintains an access control policy and that is regularly reviewed based on business and information security requirements.

c) Multi-factor authentication: Multi-factor authentication is enabled for PacketFabric user access to the environment.

8) Measures for ensuring physical security of locations at which personal data are processed:

Hosting infrastructure and data center security: PacketFabric currently uses; (i) its own secure co-location data center environment; (ii) infrastructure provided by Amazon Web Services, Microsoft Azure, and Google Cloud Platform, for the infrastructure of its storage services. PacketFabric reviews and audits the applicable third party security and compliance of these infrastructure and data center providers for environmental and physical security controls once every year.

9) Measures for ensuring events logging:

Events Logging: PacketFabric produces and regularly reviews event logs recording user activity, exceptions, faults, and information security events.

10) Measures for ensuring system configuration, including default configuration:

System Configuration and Code Review Process. PacketFabric's change management includes a system configuration and code review process within an established review board and in accordance with a defined policy for justification and escalation for approval.

11) Measures for internal IT and IT security governance and management:

a) Certifications: See Section 4. of this Schedule.

b) Information risk governance: PacketFabric has a governance, risk, and compliance organization and reviews, maintains, and ensures adherence to formal IT security and data handling policies for internal IT systems and PacketFabric personnel.

c) Information security roles & responsibilities: All the information security responsibilities are defined and allocated. Conflicting duties and areas of responsibilities have been segregated to reduce opportunities for unauthorized or unintentional modification or misuse of PacketFabric's assets.

12) Measures for certification/assurance of processes and products:

Third party audits: See Section 10 of the DPA read with Section 4 of this Schedule.

13) Measures for ensuring data minimization:

a) Product privacy assessments: Product privacy assessments are performed when introducing any new product that involves processing of personal data.

b) Access Restrictions: Restrict access to personal data to the parties involved in the processing in accordance with the "need to know" principle and according to the function behind the creation of differentiated access profiles.

14) Measures for ensuring Data quality:

a) Exercise of rights: See Section 5.3.2. of the DPA (processor and controller roles).

b) Secure development environment: Development environments are protected from malicious or accidental development and update of code that may compromise confidentiality, integrity, and availability of the platform.

15) Measures for ensuring limited data retention:

Data retention: See Annex 1(B) in Schedules 1 and 2 of this DPA.

16) Measures for ensuring accountability:

a) Product privacy assessments. See Section 13. of this Schedule

b) Software development life-cycle: See Section 14. of this Schedule.

17) Measures for allowing data portability:

a) Exercise of Rights: See Section 6 of this DPA.

b) Return of PARTNER Content. See Section 9 of this DPA.

ANNEX

The Standard contractual clauses have been updated by the European commission and can be downloaded from the following link:-

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en