

Data Processing Addendum

GDPR

This Data Processing Addendum ("**Addendum**") forms part of the Software-as-a-Service Agreement ("**Principal Agreement**") between: (i) CloudShare, Inc. ("**Vendor**") acting on its own behalf and as agent for each Vendor Affiliate; and (ii) the entity identified as Company on the signature page, ("**Company**") acting on its own behalf and as agent for each Company Affiliate.

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Principal Agreement. Except where the context requires otherwise, references in this Addendum to the Principal Agreement are to the Principal Agreement as amended by, and including, this Addendum.

1. Definitions

1.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "**Applicable Laws**" means (a) European Union or Member State laws with respect to any Customer Data in respect of which any Company Group Member is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Customer Data in respect of which any Company Group Member is subject to any other Data Protection Laws;

1.1.2 "**Company Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Company, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.3 "**Company Group Member**" means Company or any Company Affiliate;

1.1.4 "**Contracted Processor**" means Vendor or a Subprocessor;

1.1.5 "**Controller-to-Processor Clauses**" means the standard contractual clauses between controllers and processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021;

1.1.6 "**Customer Data**" means the "personal data" (as defined in the GDPR) that is uploaded to the Services under Company Group Member's accounts.

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

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

1.1.9 "**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;

- 1.1.10 "GDPR" means EU General Data Protection Regulation 2016/679;
 - 1.1.11 "**Processor-to-Processor Clauses**" means the standard contractual clauses between processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021;
 - 1.1.12 "**Restricted Transfer**" means:
 - 1.1.12.1 a transfer of Customer Data from any Company Group Member to a Contracted Processor; or
 - 1.1.12.2 an onward transfer of Customer Data from a Contracted Processor to a Contracted 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) in the absence of the Standard Contractual Clauses in Annex 3;
 - 1.1.13 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Vendor for Company Group Members pursuant to the Principal Agreement;
 - 1.1.14 "**Standard Contractual Clauses**" means (i) the Controller-to-Processor Clauses, or (ii) the Processor-to-Processor Clauses, as applicable in accordance with Sections 3.5.2 and 3.5.3;
 - 1.1.15 "**Subprocessor**" means any person (including any third party and any Vendor Affiliate, but excluding an employee of Vendor or any of its sub-contractors) appointed by or on behalf of Vendor or any Vendor Affiliate to Process Personal Data on behalf of any Company Group Member in connection with the Principal Agreement;
 - 1.1.16 "**Third Country**" means a country outside the EEA not recognised by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR); and
 - 1.1.17 "**Vendor Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Vendor, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.
- 1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processor**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.
 - 1.3 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Authority

Vendor warrants and represents that, before any Vendor Affiliate Processes any Customer Data on behalf of any Company Group Member, Vendor's entry into this Addendum as agent for and on behalf of that Vendor Affiliate will have been duly and effectively authorised (or subsequently ratified) by that Vendor Affiliate.

3. Processing and Transfers of Customer Data

3.1 Vendor and each Vendor Affiliate shall:

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

3.1.2 not Process Customer Data other than on the relevant Company Group Member's documented instructions, unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case Vendor or the relevant Vendor Affiliate shall to the extent permitted by Applicable Laws inform the relevant Company Group Member of that legal requirement before the relevant Processing of that Personal Data. The relevant Company Group Member's documented instructions include processing in accordance with the Principal Agreement; no additional instructions are required for such processing.

3.2 Each Company Group Member:

3.2.1 instructs Vendor and each Vendor Affiliate (and authorises Vendor and each Vendor Affiliate to instruct each Subprocessor) to:

3.2.1.1 Process Customer Data; and

3.2.1.2 in particular, transfer Customer Data to any country or territory,

as reasonably necessary for the provision of the Services and consistent with the Principal Agreement; and

3.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 3.2.1 on behalf of each relevant Company Affiliate.

3.3 Annex 1 to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Customer Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). Company may make reasonable amendments to Annex 1 by written notice to Vendor from time to time as Company reasonably considers necessary to meet those requirements. Nothing in Annex 1 (including as amended pursuant to this section 3.3) confers any right or imposes any obligation on any party to this Addendum.

3.4 **Data Processing Scope and Roles:** Company Group Member may be either of the following (a) a Controller of Customer Data, or (b) a Processor when it Processes Customer Data on behalf of its end-users or potential purchasers. Consequently, Vendor is a Processor where Company Group Affiliate is Controller or Processor, or a Subprocessor when Company Group Affiliate is acting as a Processor on behalf of its end-users or potential purchasers; (ii) The subject matter of the Processing is Vendor's provision and Company Group Affiliate's use of the Services and the detection, prevention and resolution of security and technical issues as provided for in the applicable Principal Agreement. It is not the intention of either party that Vendor be a Controller; at all times Company and its Affiliates are either Processors or Subprocessors.

3.5 Transfers of Personal Data

3.5.1 **Application of Standard Contractual Clauses.** The Standard Contractual Clauses will only apply to Customer Data that is transferred, either directly or via onward transfer, to any Third Country, (each a "**Data Transfer**").

3.5.2 When Company Group Member is acting as a controller, the Controller-to-Processor Clauses will apply to a Data Transfer.

3.5.3 When Company Group Member is acting as a processor, the Processor-to-Processor Clauses will apply to a Data Transfer. Taking into account the nature of the processing, Company Group Member agrees that it is unlikely that CloudShare will know the identity of Company Group Member's controllers because CloudShare has no direct relationship with Company Group Member's controllers and therefore, Company Group Member will fulfil CloudShare's obligations to Company Group Member's controllers under the Processor-to-Processor Clauses.

4. Vendor and Vendor Affiliate Personnel

Vendor and each Vendor Affiliate 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 Data, ensuring in each case that access is strictly limited to those individuals who need to know/access the relevant Customer 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.

5. Security

5.1 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, Vendor and each Vendor Affiliate shall in relation to the Customer 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. Vendor is part of the EU/US and Swiss/US Data Privacy Shield Program and will either maintain such status or maintain privacy and security practices consistent with such program. Company has assessed Vendor's security measures and determined them to be adequate for the type of Customer Data that will be processed. Vendor's security measures are described in its SLA, Support & Security Exhibit at <https://www.cloudshare.com/cloudshare-agreements>.

5.2 In assessing the appropriate level of security, Vendor and each Vendor Affiliate has taken into account the fact that the Principal Agreement is not intended to be used for the processing of human resources data and it is the expectation of the parties that the Principal Agreement will be used only for very limited levels of Personal Data belonging to third parties consistent with the description in Annex 1. Should Company or Company Group Members utilize the services in the Principal Agreement for the processing of human resources data or the collection and/or processing of more than the minimum Personal Data belonging to third parties necessary to fulfill the description in Annex 1, Company will be responsible for damages associated with data security breaches for such information.

5.3 The Principal Agreement and this Addendum are not intended to shift security responsibility for Company or Company Group Member's applications that are hosted or processed in accordance with the Principal Agreement. Company remains responsible for security issues associated with such applications, as opposed to security issues associated with Vendor's processing in accordance with the Principal Agreement and this Addendum. As an example, if Vendor is hosting Company's application and Company's application has a security flaw such as an undisclosed master password coded by developers, Company, not Vendor, is responsible for security breaches associated with such security flaw.

6. Subprocessing

6.1 Each Company Group Member authorises Vendor and each Vendor Affiliate to appoint (a) and

permit each Subprocessor appointed in accordance with this section 6 to appoint) Subprocessors in accordance with this section 6 and any restrictions in the Principal Agreement.

- 6.2 Vendor and each Vendor Affiliate may continue to use those Subprocessors already engaged by Vendor or any Vendor Affiliate as at the date of this Addendum, subject to Vendor and each Vendor Affiliate in each case as soon as practicable meeting the obligations set out in section 6.4. Subprocessors existing as of the date of this Addendum are set forth in Annex 2.
- 6.3 Vendor shall give Company prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within thirty (30) days of receipt of that notice, Company notifies Vendor in writing of any objections (on reasonable grounds) to the proposed appointment:
- 6.3.1 Vendor shall work with Company in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Subprocessor; and
- 6.3.2 where such a change cannot be made within thirty (30) days from Vendor's receipt of Company's notice, notwithstanding anything in the Principal Agreement, Company may by written notice to Vendor with immediate effect terminate the Principal Agreement to the extent that it relates to the Services which require the use of the proposed Subprocessor.
- 6.4 Vendor and each Vendor Affiliate shall ensure that each Subprocessor performs the obligations under sections 3.1, 4, 5, 7.1, 8.2, 9 and 11.1, as they apply to Processing of Customer Data carried out by that Subprocessor, as if it were party to this Addendum in place of Vendor. Where applicable, this may include a prohibition against accessing Customer Data.

7. Data Subject Rights

- 7.1 Taking into account the nature of the Processing, Vendor and each Vendor Affiliate shall assist each Company Group Member by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company Group Members' obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.
- 7.2 Vendor shall:
- 7.2.1 promptly notify Company if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Customer Data; and
- 7.2.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of Company or the relevant Company Affiliate or as required by Applicable Laws to which the Contracted Processor is subject, in which case Vendor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.

8. Personal Data Breach

- 8.1 Vendor shall notify Company without undue delay upon Vendor or any Subprocessor becoming aware of a Personal Data Breach affecting Customer Data, providing Company with sufficient information to allow each Company Group Member to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws. As appropriate, and when such information becomes available, such notification shall include a description of the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned, and the measures taken or proposed to be taken to address the Personal Data Breach. The parties understand that not all such information will be available at the time of initial notification and that some of the



information may be available only to Company or Company's Group Member due to the fact that Company and Company Group Members are the data controllers and Vendor is only the data processor.

- 8.2 Vendor shall co-operate with Company and each Company Group Member and take such reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation

Vendor and each Vendor Affiliate shall provide reasonable assistance to each Company Group Member with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required of any Company Group Member 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 Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

10. Deletion or return of Customer Data

- 10.1 Subject to sections 10.2 and 10.3 Vendor and each Vendor Affiliate shall promptly and in any event within 180 days of the date of cessation of any Services involving the Processing of Customer Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those Customer Data. Such deletion may include deletion through erasure of an encryption key and deletion of backup copies shall be performed through Vendor's and Vendor Affiliates' ordinary course of overwriting and deletion of backups.

- 10.2 Company has the ability to retrieve its own Customer Data from within its applications through self-service prior to the Cessation Date. Accordingly, subject to section 10.3, Vendor is only required to provide a copy of Customer Data to Company by secure file transfer in a non-Company-proprietary format if it has prevented such retrieval access. Any request for a provision of a copy must be received within fifteen (15) days after the Cessation Date with the copy to be provided only if Vendor has access to the Customer Data and if so, within thirty (30) days of receipt of such request.

- 10.3 Vendor and each Contracted Processor may retain Customer Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Vendor and each Vendor Affiliate shall ensure the confidentiality of all such Customer Data and shall ensure that such Customer Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

- 10.4 Vendor shall provide written certification to Company that it and each Vendor Affiliate has fully complied with this section 10 upon written request made within thirty (30) days of the Cessation Date; such certification will be provided within thirty (30) days after completion of the copy or deletion obligations.

11. Audit rights

- 11.1 Subject to sections 11.2 to 11.4, Vendor and each Vendor Affiliate shall make available to each Company Group Member on request all information necessary to demonstrate compliance with this Addendum. If Vendor and/or Vendor Affiliates have their compliance included in standard third-party audits to international standards such as ISO (International Organization for Standardization) or SOC (Service Organization Control) they shall make such reports available on a confidential basis to any Company Group Member upon request and Company Group Member shall use such audit reports in lieu of an individual audit. If such audit reports are not available, Vendor and/or Vendor Affiliates shall allow for and contribute to audits, by any Company Group Member or an auditor mandated by any Company Group Member in relation to the Processing of the Customer Data by the Contracted Processors. The cost of audits

performed by any Company Group Member shall be borne solely by the Company Group Member.

- 11.2 Information and audit rights of the Company Group Members only arise under section 11.1 to the extent that the Principal Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).
- 11.3 Company or the relevant Company Affiliate undertaking an audit shall give Vendor or the relevant Vendor Affiliate reasonable notice of any audit to be conducted under section 11.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:
 - 11.3.1 to any individual unless he or she produces reasonable evidence of identity and authority;
 - 11.3.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Company or the relevant Company Affiliate undertaking an audit has given notice to Vendor or the relevant Vendor Affiliate that this is the case before attendance outside those hours begins; or
 - 11.3.3 for the purposes of more than one audit or inspection, in respect of each Contracted Processor, in any calendar year, except for any additional audits or inspections which:
 - 11.3.3.1 Company or the relevant Company Affiliate undertaking an audit reasonably considers necessary because of genuine concerns as to Vendor's or the relevant Vendor Affiliate's compliance with this Addendum; or
 - 11.3.3.2 A Company Group Member is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory,

where Company or the relevant Company Affiliate undertaking an audit has identified its concerns or the relevant requirement or request in its notice to Vendor or the relevant Vendor Affiliate of the audit or inspection.

12. Restricted Transfers

- 12.1 The parties anticipate no Restricted Transfers. Should Company or any Company Group Member initiate a Restricted Transfer, it is solely responsible for establishing, as a data exporter, appropriate means to ensure compliance with applicable data and privacy protection laws. Should Vendor or any Vendor Affiliate wish to initiate any Restricted Transfers, they must comply with the requirements for Subprocessing and must have appropriate agreements in place, which may, as appropriate, include the Standard Contractual Clauses.

13. General Terms

- 13.1 This Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement

- 13.2 Nothing in this Addendum reduces Vendor's or any Vendor Affiliate's obligations under the Principal Agreement in relation to the protection of Personal Data or permits Vendor or any Vendor Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Principal Agreement. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.
- 13.3 Subject to section 13.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Principal Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.
- 13.4 Company may propose any variations to this Addendum or the Standard Contractual Clauses which Company reasonably considers to be necessary to address the requirements of any Data Protection Law.
- 13.5 If Company gives notice under section 13.4:
 - 13.5.1 Vendor and each Vendor Affiliate shall promptly co-operate (and ensure that any affected Subprocessors promptly co-operate) to ensure that equivalent variations are made to any agreement put in place for any Restricted Transfers; and
 - 13.5.2 Company shall not unreasonably withhold or delay agreement to any consequential variations to this Addendum proposed by Vendor to protect the Contracted Processors against additional risks associated with the variations made under section 13.4 and/or 13.5.1.
- 13.6 If Company gives notice under section 13.4, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Company's notice as soon as is reasonably practicable.
- 13.7 Neither Company nor Vendor shall require the consent or approval of any Company Affiliate or Vendor Affiliate to amend this Addendum pursuant to Section 13.4 or otherwise.
- 13.8 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.



IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Principal Agreement with effect from the date Company returns an executed copy to CloudShare via email at contracts@cloudshare.com.

Company _____

Address _____


Signature _____

Name _____

Title _____

Date Signed _____

CloudShare, Inc.

Signature _____ 

Name Zvi Guterman

Title CEO

Date Signed _____ Jan 17, 2022

ANNEX 1: DETAILS OF PROCESSING OF CUSTOMER DATA

This Annex 1 includes certain details of the Processing of Customer Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Customer Data

The subject matter and duration of the Processing of the Customer Data are set out in the Principal Agreement and this Addendum, but generally include user email, IP and local activity within the CloudShare platform

The nature and purpose of the Processing of Customer Data

Hosting Company applications; processing associated with such hosting, generally focused on providing hands on IT labs for Company's applications through virtual machines with Company applications.

The types of Customer Data to be Processed

Non-human-resources data associated with hosting Company's applications for demonstration and training purposes, generally limited to user email, IP, and local activity within the CloudShare platform.

The categories of Data Subject to whom the Customer Data relates

Data Subjects are employees of Company or Company Affiliate's customers or potential customers using the applications for business purposes. Consumer data are not involved.

The obligations and rights of Company and Company Affiliates

The obligations and rights of Company and Company Affiliates are set out in the Principal Agreement and this Addendum.

ANNEX 2: SUBPROCESSORS

The following are Vendor's Subprocessors as of the date of this Addendum:

- Equinix, Inc. – Miami, Florida
- Iron Mountain, Amsterdam, Netherlands
- Telin (Telekomunikasi Indonesia International Pte Ltd), Singapore, through a sublease from Purepeak LTD)

Role: Data Center providing co-location services; Vendor owns its own equipment within a segregated cage. This role may not qualify as subprocessing as there is no control of Vendor's equipment or access to Customer Data by the data center provider.