Data Processing Addendum – United Kingdom Version

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 andeffect.

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

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

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

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

1.1.8 "**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;

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

1.1.10 "**Restricted Transfer**" means:

1.1.10.1 a transfer of Company Personal Data from any Company Group Member to a Contracted Processor; or

1.1.10.2 an onward transfer of Company Personal 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;

1.1.11 "**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;

1.1.12 "**Standard Contractual Clauses**" means the contractual clauses set out in Annex 3, amended as indicated (in square brackets and italics) in that Annex and under section 13.4;

1.1.13 "**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; and

1.1.14 "**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 Company Personal 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 of Company Personal Data

3.1 Vendor and each Vendor Affiliate shall:

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

3.1.2 not Process Company Personal 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 Company Personal Data; and

3.2.1.2 in particular, transfer Company Personal 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 Company Personal 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 Company Personal Data, or (b) a Processor when it Processes Company Personal 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.

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 Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company 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.

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 Company 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. 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 Company Personal Data that will be processed.

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 (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 Company Personal 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 Company PersonalData.

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 Company Personal 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 therequest.

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 Company Personal 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 Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

10. Deletion or return of Company Personal 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 Company Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those Company Personal 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 Company Personal 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 Company Personal 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 Company Personal Data and shall ensure that such Company Personal 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 and 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 Company Personal 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 Affiilate 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 is responsible for filling out all information required in Annex 3 and its appendices and executing same.

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 COMPANY PERSONAL DATA

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

Subject matter and duration of the Processing of Company Personal Data

The subject matter and duration of the Processing of the Company Personal 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 Company Personal 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 Company Personal 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 Company Personal 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.

ANNEX 3: STANDARD CONTRACTUAL CLAUSES

These Clauses are deemed to be amended from time to time, to the extent that they relate to a Restricted Transfer which is subject to the Data Protection Laws of a given country or territory, to reflect (to the extent possible without material uncertainty as to the result) any change (including any replacement) made in accordance with those Data Protection Laws (i) by the Commission to or of the equivalent contractual clauses approved by the Commission under EU Directive 95/46/EC or the GDPR (in the case of the Data Protection Laws of the European Union or a Member State); or (ii) by an equivalent competent authority to or of any equivalent contractual clauses approved by it or by another competent authority under another Data Protection Law.

If these Clauses are not governed by the law of a Member State, the terms "Member State" and "State" are replaced, throughout, by the word "jurisdiction".

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

Address:

(the data **exporter**)

And
Name of the data importing organisation: CloudShare, Inc.
Address: 351 California Street, Suite 1600, San Francisco, CA 94104
Tel.: +1-650-331-3417; e-mail: support@CloudShare.com

(the data **importer**)
each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Background

The data exporter has entered into a data processing addendum (“DPA”) with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the data importer’s execution of, and compliance with, the terms of these Clauses.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; *If these Clauses are governed by a law which extends the protection of data protection laws to corporate persons, the words "except that, if these Clauses govern a transfer of data relating to identified or identifiable corporate (as well as natural) persons, the definition of "personal data" is expanded to include those data" are added.*

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC; *If these Clauses are not governed by the law of a Member State, the words "and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC" are deleted.*

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result

of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC; *If these Clauses are not governed by the law of a Member State, the words "within the meaning of Directive 95/46/EC" are deleted.*

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:
Name (written out in full):
Title:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature……………………………………….

On behalf of the data importer:
For CloudShare, Inc.:
Name (written out in full):Zvi Guterman
Title: CEO
Address: 351 California Street, Suite 1600, San Francisco, CA 94104
Other information necessary in order for the contract to be binding (if any):

Signature……………………………………….

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties
The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter
The data exporter is:

Data importer
The data importer is:
CloudShare, Inc.

Data subjects
The personal data transferred concern the following categories of data subjects:

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.

Categories of data
The personal data transferred concern the following categories of data:

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

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data:
None.

Processing operations
The personal data transferred will be subject to the following basic processing activities:

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

DATA EXPORTER

[*Populated with details of, and deemed to be signed on behalf of, the data exporter:*]
Name:………………………………
Authorised Signature ……………………
DATA IMPORTER: CloudShare, Inc.

[*Populated with details of, and deemed to be signed on behalf of, the data importer:*]
Name: Zvi Guterman
Authorised Signature ……………………

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

The following information is also found in the CloudShare SLA Support and Security exhibit.

III. Security

A. Physical Security

Facilities:
CloudShare servers are hosted at Tier III, SSAE-16, PCI DSS, or ISO 27001 compliant facilities identified in Annex 2 to the Data Processing Addendum. Our cage space is physically and logically separated from other data center customers. The co-location facilities are powered by redundant power, each with UPS and backup generators. CloudShare reserves the right to change or add hosting sites that meet the same level of security and reliability, including the possibility of using virtual sites such as those provided by Google, MicroSoft Azure, or Amazon Web Services.

On-Site Security:
Our data center facilities feature a secured perimeter with multi-level security zones, 24/7 manned security, CCTV video surveillance, multifactor identification with biometric access control, physical locks, and security breach alarms.

Monitoring:
All systems, networked devices, and circuits are constantly monitored by both CloudShare and the co-location providers.

Location:
CloudShare has data centers in the EU (Amsterdam), the United States (Miami) and Singapore. Customers can choose to locate their data in any of them.

B. Network Security:

Dedicated Security Team:
Our Security Team is on call 24/7 to respond to security alerts and events.

Protection:
Our network is protected by redundant layer 7 firewalls (Check Point Security blades and Fortinet's Fortigate NGFW), best-in-class router technology, secure HTTPS transport over public networks, regular audits, and network intrusion detection/prevention technologies (IDS/IPS) that monitor and block malicious traffic and network attacks.

Architecture:
Our network security architecture consists of multiple security zones of trust. More sensitive systems, like our database and backend servers, are protected in our most trusted zones.
Each environment has its own dedicated L2 segment completely separated from other environments and consequently any other Customer.
Other systems are housed in zones commensurate with their sensitivity, depending on function, information classification, and risk. Depending on the zone, additional security monitoring and access controls will apply. DMZs are utilized between the Internet, and internally, between the different zones of trust.

Network Vulnerability Scanning:
We constantly scan all traffic flowing through our networks that allows us to quickly identify potentially vulnerable systems or malicious activity coming to or from our network.

Third Party Penetration Tests:
Each year CloudShare hires a third party security expert firm to perform a wide range of penetration tests across our systems. Each finding is fixed while more severe ones are being handled within days.

Security Incident Event Management:
SIEM system (Splunk) gathers extensive logs and metrics from all network devices and services. This system creates triggers which notify our security team based on pre-determined rules, heuristics and correlated events. A response by the team soon follows.

Intrusion Detection and Prevention:
IPS is deployed in major ingress and egress junctions monitoring for potential risks. This system is configured to generate paged alerts upon incidents which are configured with dynamic thresholds when new threats are published.

DDoS Mitigation:
Apart from internal techniques and procedures, a third party contractor is being contracted on-demand to mitigate larger scale and more complex distributed attacks.

Logical Access:
Access to the CloudShare Production Network is restricted by an explicit need-to-know basis, utilizes least privilege, is frequently audited and monitored, and is controlled by our Operations Team. Employees accessing the CloudShare Production Network are required to use multiple factors of authentication.

Security Incident Response:
Employees get security incident mitigation, preventions and response process training. Escalation paths and channels of communication are updated and refreshed. When a system alert is triggered it is escalated to a 24/7 team which covers Ops, network and security.

C. Encryption:

Communications between the customer and CloudShare servers are being encrypted via HTTPS and TLS.
CloudShare web application is HTTPS only while transferring files into and out of CloudShare Cloud Folders can be done via FTPS.

D. Availability and Continuity:

Uptime:
CloudShare maintains a publicly available system-status webpage that includes system availability details, scheduled maintenance, service incident history, and relevant security events.

Redundancy:
CloudShare's service is highly available and clustered in every tier to eliminate single points of failure. This includes the hardware level (Switches & Routers, Storage clusters with RAIDed arrays, Firewalls and Hypervisors) and software levels (Load balanced services and virtualized servers) and databases.

Disaster Recovery:
Our DRP plan ensures our services' availability in case of a disaster. This plan is being constantly updated, tested and practiced to achieve needed continuity.
Customers' Blueprints are backed up regularly on and off site. The Recovery Time Objective is 24 hours and the Recovery Point Objective is 24 hours.

Application Security – Secure Development:

Security training:
Annual code training for our software engineers is held and is mandatory. New engineers are trained on that before they write any code that goes into production. The training covers OWASP top security flaws, common attack vectors and our own security controls.

Database access Security controls:
Our ORM (NHibernate) layer has integrated data-scoping and data-visibility controls, preventing any possibility of cross-customer data flow regardless of attack vector. This scoping mechanism has precedence over any query or code directive.

QA:
Our code base is being tested and reviewed by our QA teams. They are also proficient with application security standards and identify, test and triage security vulnerabilities in code.

Separation of Environments:
Testing, Staging and Production environments are completely separated physically and logically from each other. No actual customer data is shared between the environments and is kept on data center premises only.

E. Application Vulnerabilities:

Dynamic Vulnerability Scanning:
We employ a number of third-party, qualified security tools to continuously scan our application. CloudShare is scanned weekly against the OWASP Top 10 security flaws. We maintain a part time dedicated in-house product security team to test and work with engineering teams to remediate any discovered issues.

Static Code Analysis:
Our source code repositories for our platform are continuously scanned for security issues via our integrated static analysis tooling

Security Penetration Testing:
In addition to our extensive internal scanning and testing program, each year CloudShare employs third-party security experts to perform detailed penetration tests on different parts of the application.

F. Product Security Features:

Authentication Options:
Users of the platform can choose to authenticate via user-password with configurable password policy (see below), or via oAuth SSO with LinkedIn or Facebook, or via any SAML based SSO service (with support for SAML 1.x and 2.x), or Microsoft ADFS integration for SSO.

Configurable Password Policy:
CloudShare enforces strong password polices to reduce the risk of brute force or dictionary attacks.

Secure Credential Storage:
CloudShare follows secure credential storage best practices by never storing passwords in human readable format, and only as the result of a secure, salted, one-way hash.

API Security & Authentication:
CloudShare API is SSL-only and you must be a verified user to make API requests. API authentication and authorization is done via HMAC based Authorization Request Header involving the user API Key, API ID, salted session ID and timestamp – to prevent any playback or MitM attacks.

Access Privileges & Roles:
Access to data within your CloudShare account is governed by access rights, and the customer can define granular access privileges. CloudShare has various permission levels for users accessing your CloudShare Environment, and this can be broken down into an overall Account Manager, Project Manager, Team Manager, Team Member, and End User.

IP Restrictions:
CloudShare can be configured to only allow access from specific IP address ranges the customer defines. This can be applied at the application level by our support personnel upon request. However, IP spoofing and VPNs remain a concern with regard to the effectiveness of such restrictions.

G. Security Awareness:

Policies:
CloudShare has developed a comprehensive set of security policies covering a range of topics. These policies are shared with, and made available to, all employees and contractors with access to CloudShare information assets.

Training:
All new employees attend Security Awareness Training, and the Security Team provides security awareness updates via email, Slack channel, and in presentations during internal meetings.

Background Checks:
CloudShare performs background checks on all new employees in accordance with local laws. The background check includes Criminal, Education, and Employment verification.

Confidentiality Agreements:
All new hires are screened through the hiring process and required to sign Non-Disclosure and Confidentiality agreements.

ANNEX 3: LIST OF MANDATED

AUDITORS None unless any are listed below