**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 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 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 of4 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 orvia 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 aData Transfer. Taking into account the nature of the processing, Company Group Member agrees that it isunlikely 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 (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 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 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 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**_____

Address _____

Signature _____

Name _____

Title _____

Date Signed _____

**CloudShare, Inc.**

Signature _____

Name Zvi Guterman

Title CEO

Date Signed _____

## 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 and the Standard Contractual Clauses.

*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.

*Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures*:
None.

*The frequency of the transfer*

On a continuous basis.

## 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**

## Section I

*Clause 1*

***Purpose and Scope***

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, is the Company and its Affiliates (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, is the Vendor (hereinafter the "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in **Annex 1** of the DPA.

(d) The Annexes referred to therein forms an integral part of these Clauses.

*Clause 2*

***Effect and invariability of the Clauses***

(e) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(f) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision [...].

*Clause 3*
***Third-party beneficiaries***

(g) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(h) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

*Clause 4*
***Interpretation***

(i) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(j) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(k) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

*Clause 5*
***Hierarchy***

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

*Clause 6*
***Description of the transfer(s)***

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in **Annex 1** of the DPA.

## Section II – Obligations of the Parties

*Clause 8*
***Data Protection Safeguards***

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under these Clauses.

**8.1 Instructions**

(l) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(m) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

**8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex 1 of the DPA, unless on further instructions from the data exporter.

**8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including Annex 1 of the DPA, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in **Annex 4** and personal data, the data exporter may redact part of the text of the Annexes to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

**8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

**8.5 Duration of Processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex 1 of the DPA. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

**8.6 Security of Processing**

(n) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of

pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex 4. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(o) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(p) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(q) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

### 8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex 1 of the DPA.

### 8.8 Onwards Transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

**8.9 Documentation and compliance**

(r) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(s) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(t) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(u) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(v) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

*Clause 9*
***Use of sub-processors***

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least fourteen days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.3 The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

*Clause 10*
***Data subject rights***

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, Vendor has set out in Annex 4 the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

*Clause 11*
***Redress***

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

*Clause 12*
***Liability***

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

*Clause 13*
***Supervision***

(a) The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

**Section III – Local laws and obligations in case of access by public authorities**

*Clause 14*
***Local laws and practices affecting compliance with the Clauses***

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any

requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards4;
(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three: , if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

*Clause 15*

***Obligations of the data importer in case of access by public authorities***

**15.1 Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

**15.2 Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## Section IV – Final provisions

*Clause 16*
***Non-compliance with the Clauses and termination***

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
(ii) the data importer is in substantial or persistent breach of these Clauses; or
(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

*Clause 17*
***Governing law***

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

*Clause 18*
***Choice of forum and jurisdiction***

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

## ANNEX 4: TECHNICAL AND ORGANIZATIONAL MEASURES

***Measures of pseudonymisation and encryption of personal data**:* 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

***Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services**:* CloudShare performs background checks on all new employees in accordance with local laws. The background check includes Criminal, Education, and Employment verification. All new hires are screened through the hiring process and required to sign Non-Disclosure and Confidentiality agreements.

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. Also, 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.

**Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident***:* Our DRP plan ensures our services' availability in case of a disaster. This plan is being constantly updated, tested and practiced achieving 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.

***Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing**:* 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.

***Measures for the protection of data during transmission and Measures for the protection of data during storage***: 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.

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.

***Measures for ensuring physical security of locations at which personal data are processed**:* 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.

***Measures for internal IT and IT security governance and management**:* 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's 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 the 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.

***Measures for certification/assurance of processes and products**:* Users of the platform can choose to authenticate via user password with a 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 policies 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 are 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.

***Measures for security incidents event management: 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.

Security Incident Event Management: SIEM system (Splunk) gathers extensive logs and metrics from all network devices and services. This system creates triggers that 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.