DATA PROCESSING AGREEMENT

The parties conclude this Data Processing Agreement ("DPA"), which forms part of the Agreement between Customer and Supplier ("Glarish,Inc"), meaning the Digital Signage SaaS Agreement (the "Agreement") to reflect their agreement about the Processing of Personal Data, in accordance with the requirements of Data Protection Laws and Regulations, including the GDPR, and the CCPA to the extent applicable. To the extent Supplier, in providing the Services set forth in the Agreement, processes Personal Data on behalf of Customer, the provisions of this DPA apply.

References to the Agreement will be construed as including this DPA. Any capitalized terms not defined herein shall have the respective meanings given to them in the Agreement.

This DPA consists of two parts: (i) the main body of this DPA, and (ii) Attachments 1, 2, 3 and 4 hereto.

HOW TO EXECUTE THE DPA

To complete this DPA, Customer should:

a. Sign the main body of this DPA in the signature box below.

b. Complete any missing information and sign Attachment 1, Attachment 2, Attachment 3, and Attachment 4. Attachment 4 applies, if you are a Data Controller within the ambit of Article 3 GDPR.

Submit the completed and signed DPA to Supplier via email to support@glarish.com. Upon receipt of a validly completed DPA, this DPA will be legally binding (provided that Customer has not overwritten or modified any of the terms beyond completing the missing information).

HOW THIS DPA APPLIES

If the Customer entity signing this DPA is a party to the Agreement, then this DPA is an addendum to and forms part of the Agreement.

If the Customer entity signing this DPA has submitted Schedule A pursuant to the Agreement, then this DPA is an addendum to that Schedule A and applicable renewal terms.

If the Customer entity signing this DPA is not a party to the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is party to the Agreement executes this DPA.

If the Customer entity signing the DPA is not a party to the Agreement directly with Supplier, but is instead a customer indirectly via an Authorized Reseller or a Partner, this DPA is not valid and is not legally binding. Such entity should contact the Authorized Reseller or the Partner to discuss whether any amendment to its agreement with that Reseller or Partner may be required.

This DPA shall not replace any comparable or additional rights relating to Processing of Personal Data contained in the Agreement.

DATA PROCESSING TERMS

Customer and Glarish hereby agree to the following provisions with respect to any Personal Data Customer processed by Glarish in relation to the provision of the Services under the Agreement.

1. DEFINITIONS

"**Adequacy Decision**" means a European Commission Decision that a third country or an international organization ensures an adequate level of data protection within the meaning of Article

45 (9) GDPR in conjunction with Article 25 (6) of Directive 95/46/EC, or within the meaning of Article 45 (3) GDPR, as applicable;

"**Affiliate**" means, with respect to any entity, any other entity Controlling, Controlled by or under common Control with such entity, for only so long as such Control exists;

"**Authorized Affiliate**" means any of Customer's Affiliate(s), which (i) is subject to Customer's Binding Corporate Rules or to similar contractual clauses, including Standard Contractual Clauses or contractual clauses approved by a Supervisory Authority, where applicable, with the Customer to ensure adequate level of protection of Personal Data, (ii) is not established in a Restricted Third Country, and (iii) is permitted to use the Services pursuant to the Agreement between Customer and Supplier, but is not a signatory Party to the Agreement and is not a "Customer" as defined under the Agreement;

"**Behavioral Data**" means data that tracks or otherwise monitors a Data Subject's activities online or the Data Subject's product and service usage;

"**Binding Corporate Rules**" are binding internal rules that regulate the transfer of Personal Data within an organization which, where applicable, have been approved by EU data protection authorities as providing an adequate level of protection to Personal Data;

"**CCPA**" means the California Consumer Privacy Act (CAL. CIV. CODE § 1798.100 et. seq.) and its implementing regulations. "Control" means the direct or indirect ownership of more than 50% of the voting capital or similar right of ownership of an entity, or the legal power to direct or cause the direction of the general management and policies of that entity, whether through the ownership of voting capital, by contract or otherwise. Control and Controlling shall be construed accordingly;

"**Dashboard**" for applicable Services, means the user interface features of the hosted Software (as described in the Agreement);

"**Data Controller**" means the entity that determines the purposes and means of the Processing of Personal Data, as defined in the GDPR, and has the same meaning as "business," as that term is defined by the CCPA;

"**Data Processor**" means the entity which Processes Personal Data on behalf of the Data Controller, as defined in the GDPR, and has the same meaning as "service provider," as that term is defined by the CCPA;

"**Data Protection Laws and Regulations**" means all laws and regulations applicable to the Processing of Personal Data as part of or in connection with the Services, including but not limited to (i) laws and regulations of the European Union, the European Economic Area and their member states, including the GDPR, and ii) Adequacy Decisions as either of (i) or (ii) may be amended and are in force from time to time;

"**Data Subject**" means the individual to whom Personal Data relates, as defined in the GDPR, and has the same meaning as "consumer" as that term is defined under the CCPA;

"**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), as may be amended from time to time;

"**Glarish**" means the Supplier;

"**Personal Data**" means data about a natural person processed by Glarish in relation to the provision of the Services under the Agreement, from which that person is identified or identifiable, as defined in the GDPR; for the avoidance of doubt, Personal Data includes but is not limited to Support Data, Behavioral Data and Unique Identifier Data, and has the same meaning as "personal information" as that term is defined under the CCPA;

"**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, transfer or otherwise making available, alignment or combination, blocking, erasure or destruction;

"**Restricted Third Country**" means a country to which a transfer of Personal Data, or from which access to Personal Data, would be prohibited by applicable Data Protection Laws and Regulations;

"**Standard Contractual Clauses**" means contractual clauses adopted by the European Commission based on Article 46 (5) GDPR in conjunction with Article 26 (4) of Directive 95/46/EC, or within the meaning of Article 46 (2) c) or d) GDPR, as applicable.

"**Software**" means the object code version of GLARISH software and/or any software to which Customer is provided access to as part of the Services, including any updates or new versions;

"**Supplier**" means the Glarish entity, which is a party to this DPA and the Agreement, namely Glarish,Inc., a US based company, having its registered office at 30 Regalo Drive, Mission Viejo, California, 92692.

"**Sub-processor**" means any non-Affiliate or Affiliate Data Processor, engaged by Glarish, who agrees to receive from Glarish or from any other Sub-processor of Glarish Personal Data exclusively intended for the Processing to be carried out on behalf of the Customer, in accordance with its instructions, the terms of this DPA, and the terms of the written Sub-processor contract;

"**Supervisory Authority**" means an independent public authority which is established by an EU Member State, pursuant to the GDPR;

"**Support Data**" means information that Glarish collects, when Customer submits a request for support services or other troubleshooting, including information about hardware, software and other details related to the support incident, such as authentication information, information about the

condition of the product, system and registry data about software installations and hardware configurations, and error-tracking files;

"**Unique Identifier Data**" means a unique persistent identifier associated with an individual or a networked device, including a customer number held in a cookie, a user ID, a processor serial number, or a device serial number.

2. PROCESSING OF PERSONAL DATA

2.1 Roles of the Parties. The parties acknowledge and agree that for the purposes of this DPA Customer is the Data Controller and Supplier is the Data Processor, that Supplier engages in the Processing, i.e. in the operation, maintenance and support of the Services, including acting as super-administrator of the accounts in Glarish Software, Glarish is entitled to engage Subprocessors pursuant to the requirements set forth in Clause 5 of this DPA. Customer may permit the use of the Services to Authorized Affiliate(s) pursuant to the conditions set out in Clause 14 and 15 of this DPA.

2.2 Customer's Processing of Personal Data. Customer shall, in its use of the Services, Process Personal Data in accordance with Data Protection Laws and Regulations. For the avoidance of doubt, Customer's instructions to the Glarish for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. In addition, Customer shall have sole responsibility for the accuracy, reliability, quality, and legality of Personal Data, and the means by which Customer acquired Personal Data, including providing any required notices to, and obtaining any necessary consent from, its employees, agents or third parties to whom it extends the benefits of the Services or whose Personal Data are Processed in Customer's Use of the Services. It is expressly stated that Customer is solely responsible (i) for the legality of the purposes of the Processing, (ii) for the necessity of the Processing to serve these purposes, (iii) to inform any and all Data Subjects, whose Personal Data is processed by using the Services, about the scope, the purpose, the duration and the means of the Processing, their rights with respect to the Processing (iv) to acquire the consent of the

Data Subjects, whose Personal Data is being processed by using the Services, where applicable v) to conduct a Data Protection Impact Assessment Study (DPIA) within the meaning of Article 35 and 36 GDPR, where applicable.

2.3 Glarish's Processing of Personal Data.

a. Glarish shall treat Personal Data as Confidential Information and shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and this DPA; (ii) Processing initiated by Authorized Affiliates or Authorized Users in their use of the Service; and (iii) Processing to comply with other documented, reasonable instructions provided by Customer (for example, via email) where such instructions are consistent with the terms of the Agreement. b. Customer takes full responsibility to keep the amount of Personal Data provided to Glarish to the minimum necessary for the performance of the Services. c. Glarish shall not be required to comply with or observe Customer's instructions, if such instructions would violate the GDPR, the CCPA or the Data Protection Laws and Regulations. Glarish shall immediately inform Customer if, in its opinion, an instruction infringes the GDPR or the CCPA or the Data Protection Laws and Regulations . d. Glarish shall process Personal Data, if required to do so by European Union or Member State law to which Glarish is subject; in such a case, Glarish shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. Glarish shall promptly notify Customer of any legally binding request for disclosure of 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.

2.4 Scope of the Processing. The subject-matter of Processing of Personal Data by Glarish is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Attachment 1 to this DPA.

3. RIGHTS OF DATA SUBJECTS

3.1 Complaints or Notices related to Personal Data. In the event Glarish receives any official complaint, notice, or communication that relates to Processing of Personal Data for or on behalf of the Customer or either party's compliance with Data Protection Laws and Regulations, to the extent legally permitted, Glarish shall promptly notify Customer and, to the extent applicable, Glarish shall provide Customer with commercially reasonable cooperation and assistance in relation to any such complaint, notice, or communication. Customer shall be responsible for any reasonable costs arising from Glarish's provision of such assistance.

3.2 Data Subject Requests. To the extent legally permitted, Glarish shall promptly notify Customer, if Glarish receives a request from a Data Subject to exercise the Data Subject's right to consent, and to withdraw the consent, right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("Data Subject Request"), and for the avoidance of doubt, similar requests as provided by the CCPA. Factoring into account the nature of the Processing, Glarish shall assist Customer by appropriate organizational and technical measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Glarish shall, upon Customer's request, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent that Glarish is legally permitted to do so, and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from Glarish's provision of such assistance.

4. GLARISH'S PERSONNEL

4.1. **Confidentiality.** Glarish shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Glarish shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2. Reliability. Glarish shall take commercially-reasonable steps to ensure the reliability of its personnel engaged in the Processing of Personal Data.

4.3. Limitation of Access. Glarish shall ensure that Glarish's access to Personal Data is limited to those personnel assisting in the provision of the Services in accordance with the Agreement, and that access is limited to those personnel that is necessary for the provision of the Services.

4.4. Data Protection Officer. Glarish shall appoint, a Data Protection Officer, if and whereby such appointment is required by Article 37 of the GDPR. Any such appointed person and Glarish's personnel responsible for privacy issues, may be reached at privacy@glarish.com

5. SUB-PROCESSORS

5.1 Appointment of Sub-processors. Customer acknowledges and agrees that:

i. Glarish is entitled to retain its current and future Affiliate(s) as Sub-processors. Glarish shall inform the Customer of any intended changes to its Affiliates, acting as Sub-processors.

ii. Glarish may engage any third parties from time to time to process Personal Data in connection with the provision of Services.

5.2 List of Sub-processors. Current non-Affiliate Sub-processors, are listed in Attachment 3 to this DPA, and Customer hereby authorizes the use of such Sub-processors to assist Glarish with the performance of Glarish's obligations under the Agreement and this DPA. Glarish shall inform the

Customer of any intended changes to such List by sending an email. Additionally, the list of non-affiliate Sub-processors is also available in the Services Dashboard. DocuSign Envelope

5.3. Objection Right for New Sub-processors. Customer, in order to exercise its right to object to Supplier's use of a new Sub-processor, whether Affiliate or not, shall notify the Supplier promptly in writing within ten (10) business days after receipt of Supplier's notice about its intention to use a new Sub-processor. Personal Data shall by no means be processed by the Sub-processor against which the Customer has explicitly objected. If Supplier and Customer cannot find a mutually agreeable resolution to address the Customer's objection within a reasonable time period, which shall not exceed thirty (30) days, the Customer may terminate the Services. The Supplier shall refund Customer any prepaid fees covering the remainder of the Service following the effective date of termination with respect to such terminated Service. Customer shall return at Customer's own delivery expenses any hardware (i.e. GLARISH media player) provided by Glarish through authorized retailers.

5.4. Contractual relationships. Glarish shall only engage and disclose Personal Data to non-Affiliate Sub-processors that are parties to written agreements with Glarish containing data protection obligations no less protective that the obligations of this DPA. Glarish agrees and warrants, upon request of the Customer, to send promptly a copy of any Sub-processor contract to the Customer, and to make available to the Data Subject upon request a copy of the DPA, or any existing Subprocessing contract, unless the DPA or contract contain commercial information, in which case it may remove such commercial information, with the exception of Attachment 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 Customer.

5.5. Liability. Glarish shall be liable for the acts and omissions of its non-Affiliate Sub-processors to the same extent Glarish would be liable, if performing the services of each Sub-processor directly under the terms of this DPA.

6. LOCATION OF FACILITIES

The parties agree that the Software, including the Portal, and all Personal Data, including their back ups, will be hosted and/or stored at facilities located in data centers in the EU and/or the USA. If Glarish proposes to host or store the Software, including the Portal, or backups, and any Personal Data, at facilities located outside the USA or the European Economic Area ("Foreign Facility"), then Glarish shall provide prior written notice to Customer providing the details of such proposal ("Relocation Notice"). Customer may, at its sole discretion, object to the proposed Foreign Facility. If the parties cannot agree on a resolution within sixty (60) days following Customer's objection, then Customer may terminate this Agreement. Glarish shall not allow the Software, including the Portal, or backups of the Software, nor any Personal Data, to be hosted at and/or stored by a Foreign Facility unless and until such time as agreed to by Customer in writing.

7. SECURITY

Taking into account the state of 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, Glarish shall implement appropriate organizational and technical measures to ensure a level of security, appropriate to the risk (including protection from accidental or unlawful destruction, loss alteration, unauthorized disclosure of, or access to Personal Data Processed under this DPA), as set forth in Attachment 2 to this DPA. Glarish shall regularly monitor compliance with these measures. Glarish shall not materially decrease the overall security of the Services during Customer's subscription term. Attachment 2 may be amended from time to time, upon parties' written agreement, to meet higher standards of safety and privacy. In such case Attachment 2 shall be replaced. Customer represents that after its assessment of the requirements of the Data Protection Laws and Regulations, Customer considers that the security measures set out in Attachment 2 are appropriate to protect Personal Data against accidental or unlawful destruction or accidental loss,

alteration, unauthorized disclosure or access, 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 Personal Data to be protected having regard to the state of the art and the cost of their implementation.

8. DATA INCIDENT MANAGEMENT AND NOTIFICATION

Glarish has in place reasonable and appropriate security incident management policies and procedures, specified in Attachment 2 of this DPA, and shall notify Customer without undue delay after becoming aware of an unlawful or accidental destruction, alteration or damage or loss, unauthorized disclosure of, or access to Personal Data, transmitted, stored or otherwise Processed by Glarish or its nonAffiliate Sub-processors of which Glarish becomes aware ("Personal Data Incident"), as required under Article 33 of the GDPR. Glarish shall make reasonable efforts to identify the cause of such Personal Data Breach, and take those steps as it deems necessary and reasonable in order to remediate the cause of such a Personal Data Breach, to the extent that the remediation is within Glarish's reasonable control.

9. CERTIFICATIONS AND AUDITS

9.1 Audits. Upon Customer's request, and subject to the confidentiality set forth in the Agreement, Glarish shall make available to the Customer that is not a competitor of Glarish all information necessary to demonstrate compliance with the obligations of Glarish under this DPA, and allow for and contribute to audits, including on-site audits, conducted by the Customer or by Customer's independent, third-party auditor, in possession of the required professional qualifications bound by a duty of confidentiality, that is not a competitor of Glarish. The parties agree that the audits shall be carried out in accordance with the following specifications: Customer may contact Glarish to request an on-site audit of the architecture, systems, and procedures relevant to the protection of Personal Data. Customer shall reimburse Glarish for any time expended by Glarish or its third party Sub-

processors for any such on-site audit at the Glarish's then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Glarish shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Glarish or its third party Sub-processors. Customer shall promptly notify Glarish and provide information about any actual or suspected noncompliance discovered during an audit.

9.2 Certifications. Glarish shall also allow and provide third-party certifications and audit results upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement. Glarish shall make available to Customer that is not a competitor of Glarish (Customer's independent third-party auditor that is not a competitor of Glarish) a copy of Glarish's then most recent third-party certifications or audit results, as applicable.

10. RECORDS AND COOPERATION WITH THE SUPERVISORY AUTHORITY

10.1. Records. Where applicable, Glarish shall maintain a record, in electronic form, of all categories of processing activities carried out on behalf of the Customer, as per Article 30 (2) GDPR.

10.2. Cooperation with the Supervisory Authority. Where applicable, Glarish shall, upon request, cooperate with the Supervisory Authority in the performance of its tasks, as per Article 31 of the GDPR.

11. RETURN AND DELETION OF PERSONAL DATA

Glarish shall, at the choice of the Customer, return Personal Data, to Customer or delete existing copies after the end of the provision of the Services and certify to the Customer that it has done so in accordance with the procedures specified in Attachment 2 to this DPA, unless mandatory laws require

storage of Personal Data. In that case Glarish warrants that it shall guarantee the confidentiality of the Personal Data and shall not actively process Personal Data transferred anymore.

12. DATA PROTECTION IMPACT ASSESSMENT

Upon Customer's request, Glarish shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under Article 35 of the GDPR to carry out a Data Protection Impact Assessment ("DPIA") related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Glarish. Glarish shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this DPA, to the extent required under Article 36 of the GDPR.

13. DATA TRANSFERS

Transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to countries outside of the European Economic Area are made only in accordance with the following:

i. the transfer is to a jurisdiction for which an Adequacy Decision has been issued and subject to the terms of that Adequacy Decision;

ii. in the absence of an Adequacy Decision, the transfer is subject to the latest versions of the Standard Contractual Clauses approved by the European Commission from time to time, as published in the Official Journal of the European Union, and which themselves form part of this DPA (Attachment 4).

14. AUTHORIZED AFFILIATES

14.1 Contractual Relationship. The parties acknowledge and agree that, by executing the DPA, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliate(s), thereby establishing a separate DPA between Glarish and each such Authorized Affiliate subject to the provisions of the Agreement and this Clause and Clause 15 of this DPA. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Services and Content by Authorized Affiliate(s) must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

14.2. Communication. The Customer that is contracting party to the Agreement shall remain responsible for coordinating all communication with Glarish under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates. Customer informs Glarish of the Authorized Affiliate(s) to which Customer intends to permit the use of the Services, thereby giving Glarish the opportunity to object, in case the requirements set out in the Definition of an Authorized Affiliate under this DPA are not met.

14.3. Rights of Authorized Affiliates. Where an Authorized Affiliate becomes a party to the DPA with Glarish, it shall, to the extent required under applicable Data Protection Laws and Regulations, be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

i. Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Glarish directly by itself, the parties agree that (a) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized

Affiliate, and (b) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for all of its Authorized Affiliates together (as set forth, for example, in Section 13.3.ii below).

ii. The parties agree that the Customer that is the contracting party to the Agreement shall, when carrying out an on-site audit on the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on Glarish and its non-Affiliate Sub-processors by combining, to the extent reasonable possible, several audit requests carried out on behalf of different Authorized Affiliates in one single audit.

15. LIABILITY

For the avoidance of doubt, Glarish's total liability for all claims from the Customer and all of its Authorized Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Customer and all Authorized Affiliates, and in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA.

16. LEGAL EFFECT; TERMINATION; VARIATION

This DPA shall only become legally binding between Customer and Glarish when fully executed following the formalities steps set out in the Section "How to Execute this DPA" and will terminate when the Main Agreement terminates, without further action required by either party. The parties undertake not to vary or modify the DPA. This does not preclude the parties from adding clauses on business related issues, where required as long as they do not contradict the DPA.

17. CONFLICT

This DPA is incorporated into and forms part of the Agreement. For matters not addressed under this DPA, the terms of the Agreement apply. With respect to the rights and obligation of the parties vis-àvis each other, in the event of a conflict between the terms of the Agreement and this DPA, the terms of this DPA will control. IN WITNESS WHEREOF, the parties have caused this Data Processing Addendum to be duly executed. Each party warrants and represents that its respective signatories, whose signatures appear below, are on the date of signature duly authorized.

CUSTOMER GLARISH

ATTACHMENT 1

Details of the Processing

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

Nature and Purpose of Processing

Glarish will Process Personal Data as necessary to perform the Services pursuant to the Agreement, and as further instructed by Customer in its use of the Services.

Duration of Processing

Subject to Clause 11 of the DPA, Glarish shall Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing. Unless otherwise agreed upon in writing, Glarish shall, at the choice of the Customer, return Personal Data, to Customer or delete existing copies after the end of the provision of the Services and certify to the Customer that it has done so in accordance with the procedures specified in Attachment 2 to this DPA, unless mandatory laws require the storage of Personal Data. In that case Glarish warrants that it shall guarantee the confidentiality of the Personal Data and shall not actively process Personal Data transferred anymore.

Categories of Data Subjects

- Customers
- Customer's Agents, Employees, Authorized Users

Type of Personal Data

- Identification data:

- name, address, email, phone number and access rights.

- Customer Content:
  - Images
  - Videos
  - Power point
  - Pdf files etc

ATTACHMENT 2

Description of the technical and organizational security measures implemented by Glarish in accordance with Article 28.3 of the GDPR, which form part of the DPA:

- **Personnel**

Confidentiality and reliability. Personnel engaged in the processing of Personal Data are reliable, are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, are regularly trained, and have executed written confidentiality agreements. Confidentiality obligations survive the termination of the personnel engagement. Access privileges are terminated upon termination of employment. All personnel with access right to Accounts are engaged full-time.

Segregation of Duty and Limitation of Access. Personnel's access to Personal Data is appropriate and necessary to their role. A Security Officer has been appointed in written and supervises compliance with security measures. Personnel have individual accounts for accessing systems with safe codes. Personnel is separated into three levels of access i) developers, ii) support/sales, and iii) others. Developers have access to the whole system, to ensure that everything is running smoothly. Support has limited access to the system, i.e. only when handling a support request. All others do not have access to Accounts.

Access Control and Authentication. a. A procedure for user account creation and deletion, with appropriate approvals is in place; b. Industry standard practices to identify and authenticate users who attempt to access information systems are utilized; c. De-activated or expired identifiers are not granted to other individuals; d. All Personnel actions are logged to an internal audit log. Providing support also appears to the Users of an Account, if the Account is on the Enterprise plan that provides for the "Audit logs" features.

- **Physical and Environmental Security**

Physical Access. Glarish utilizes facilities with access control (e.g. CCTV, smart security systmes, reception, access code), and with emergency and contingency plans for various disasters, including fire. Drills are in practice regularly.

Exposure of Documents. A Clean Desk Policy is implemented. All physical files are kept in cabinets or drawers. Photo copy and fax machines are not in common view.

Destruction of Documents. Papers with personal data are dispensed exclusively in paper shredders. After retention period, electronic data are not just deleted, but destroyed (including their back-ups) by overwriting with the use of special software, like file erasers, file shredders, file pulveritizers or, alternatively, for destruction on a daily basis, by formatting.

Portable Devices. Laptops are accessed only by secure codes.

- **Data Security**

Anti-virus. Glarish ensures that antivirus, anti-malware and anti-spyware software of the latest update are installed. Updates are installed at regular intervals. Glarish undertakes specific hardening activities, to minimize the architectural weaknesses of operating systems, application, and network devices.

Remote Access. Security of remote access to the system is based on encryption and safe protocols. Only direct communication between the device and the server is allowed, no traffic forwarding or between devices traffic is allowed.

Firewall. An industry-standard firewall is installed to inspect all connections routed to the system's environment.

Vulnerability and Penetration Tests. Glarish regularly performs vulnerability analysis aimed at specifying the status of exposure to known vulnerabilities, in relation to both the infrastructural and application environments, considering the systems in operation or in the development phase. These

checks take place periodically, every six months, supplemented by specific penetration tests, involving intrusion simulations which use different attack scenarios.

Change Control. All changes to platform, application, and production infrastructure (for example software update, development of new software, antivirus installation or deinstallation) are tested, before implementing, in an isolated and updated environment not affecting real data or data of the production system, with the exception of users that have enrolled to the Beta Set Up. There are regular controls on installed software to verify that no software has been installed outside of the regular process. All changes are administered centrally only by specific users.

Data separation. Content uploaded in GLARISH Software shall be maintained logically separated from Glarish's corporate infrastructure and from Glarish's other Customers' content.

- **Log Retention Policy**

General. Log files are retained for all crucial systems. Glarish retains the following types of logs: Web Access Logs / Application Logs / Audit Logs (detailed). Following information are necessarily retained at a minimum:

a) identification of user who required access to personal data, date and time of the request, system for which access was requested, whether access has been granted or not.

b) Same information with regard to non-authorized access efforts

c) Printing requests of files with personal data

d) Modifications in crucial files of the system or in the users' rights

e) Changes in the parameters of apps and systems

f) Crucial events and of any action that may be considered as an attack or a security incident (e.g. port scanning). The retention of events is directly supervised by the Security Officer and the System Administrators.

Log files may only be assessed by the Security Officer and the system administrators. Deletion of log files has to be authorized by both the Security Officer and a member of the senior management.

Log Storage. All Logs are uploaded from each server to Google Cloud. Credentials and names used ensure that an attacker cannot access or alter the logs. Glarish uses versioning on Google Cloud to make sure previous content of updated logs are kept. Log files are stored on a Google Cloud bucket (or an Amazon S3 bucket) properly configured for encryption-at-rest using Google encryption scheme.

Log Rotation. All Logs are rotated on the server on 5-days basis, to facilitate support and debugging. Logs stored on Google Cloud are rotated on a 90-days basis.

- **Password Policy**

Access to all systems, applications and software is password protected. Admissible passwords comply with password configurations (eg minimum length, expiration, complexity etc.). Change of passwords is enforced regularly.

Passwords are not written, either physically or electronically, in their actual form. They are retained electronically in a non-readable form, whereas the retrieval of their initial form is be possible. After three attempts of unsuccessful access authorization, access is prohibited to the user.

Passwords are not kept in logs.

Industry standard procedures are implemented to deactivate passwords that have been corrupted or inadvertently disclosed.

- **Service Continuity and Disaster Recovery**

a. Glarish utilizes facilities (data centers), for Personal Data and their back-ups, providing adequate emergency and contingency plans and guarantees; b. Glarish has in place adequate data recovery procedures.

- **Incident Monitoring and Management**

Glarish monitors, analyses and responds to security incidents in a timely manner, and escalates as necessary. Glarish implements a specific Incident Management Procedure to guarantee the recovery of normal service operations as soon as possible in case of interruption.

- **Data Breach Policy**

Glarish has a Data Breach Policy in place to meet the requirements of Clause 8 of this DPA and of the GDPR, which includes but is not limited to i) internal reporting of potential Personal Data Breaches, ii) recovery of a Personal Data Breach, iii) risk assessment, iv) notification of Personal Data Breach to the Data Controller, the Supervisory Authority and the affected data subject, as applicable, v) evaluation and response measures to prevent similar breaches. Security Officer is responsible for the implementation and update of the Data Breach Policy.

- **Design of the Services**

Privacy. Every User, after signing up for the first time, has to accept Glarish's Privacy Policy. GLARISH application enables the Customer to assign specific rights (of view, access, modification, and deletion) based on the tasks and responsibilities of the Authorized Affiliate or the Authorized User. Deletion of Personal Data as well as deletion of the Account is possible by the process described in the Dashboard under section "Personal Data". Following security measures are accommodated: a) authentication of users before access; ii) encryption of passwords iii) activation of secure password policy by Customer in the Enterprise Plan; iv) change of passwords every six months; and iv) prevention of access after suspicious access attempts.

Customer's responsibility. Customer manages each user's access to and use of the Services by assigning to each user a credential and user type that controls the level of access to and use of the Services. Customer is responsible for protecting the confidentiality of its own and each user's login and password and managing each user's access to the Services.

Security. Secure Outbound Traffic. GLARISH Application uses no UDP listening port (UDP) . GLARISH Application does not use port forwarding, DMZ, or UPnP in the network. Glarish Application uses a full-duplex communication channels over a single TCP connection through a TLS/SSL encryption to encrypted all data sent to and from the server (including the initial handshake and response), which is the same encryption mechanism used for HTTPS connections (and uses the same encryption engine in the browser).

Digital Signature Verification for Core Software. Glarish developed a proprietary protocol that is not possible for an attacker to force the Media Player to play a different schedule file than the one generated by the system for this specific device. Two reasons: (1) the media player contains no core software information when disconnected from the certified server; (2) the core software is strictly associated with the board serial number.

HTTPS Certificate checks. Schedule Files, Configuration Files and Media Files are downloaded using HTTPS. SSL certificate check are enforced throughout the system.

Software Upgrading Verification Checks. Glarish adopts a virtual software upgrade through a proprietary technology that assures latest software upgrade at the any time. The software is downloaded through HTTPS.

Device Firewall. GLARISH Players have a standard firewall policy enabled by default, that only allows inbound SSH access. SSH can also be firewall for the LAN interface, leaving nothing accessible from the LAN, without any service disruption.

Proxy Authentication Support. GLARISH Players support using a Proxy installed and managed. The Proxy is required to support the "CONNECT" method for HTTPS connections. Glarish supports using authentication credentials for Proxies.

Customization Scripts. Device support customization scripts for altering default behavior are issued remotely as part of the Configuration file, which is digitally signed and secured.

Secure Software Initialization. The SD card that holds the Player software must be written through another computer as a disk image. A registered user can download the SD card image. The SD card can be inserted into the SD card slot of the media player.

USB connection fully disable for security. All USB connectors are fully disabled. The media player can only work through the internet.

Media Player Software protection from hacking. Any external change (hacking) of the software into the SD card would compromise the secure self-initialization of the media player and disable the the connection with the server.

Customer's responsibility. Customer is solely responsible for the safe connection of the GLARISH Player to internet.

- **Audit and Review**

Internal and external audit of all systems takes place on a six months basis. Technical and Organizational Security Measures are reviewed annually, and in case of a major change. Audit and Review include capacity planning of IT resources with view to future requirements based on workload and data storage requirements.

ATTACHMENT 3

The list of non -Affiliate Sub-processors approved by the Customer as of the effective date of the DPA is as set forth below;

Non – Affiliate Subprocessor Description of Processing Contact Information Location of Facilities (including back up)

Google Cloud provider www.google.com US

Stripe Payments www.stripe.com US

ATTACHMENT 4

EUROPEAN COMMISSION - DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship

Unit C.3: Data protection

Commission Decision C(2010)593 - 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: …… (Customer)

Address:
……

Tel.: …… ; fax: …… ; e-mail:……

(the data exporter)

And

Name of the data importing organisation: Glarish,Inc. ……

Address: ……

Tel.:…… ; fax: …… ; e-mail: ……

(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.

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[1] ;

(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;

(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.

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

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;

(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[2]

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;

---

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(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, namely……..……..……

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 Clauses3 . 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, namely ……..……..……

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.

---

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

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):…….……..……..……..……..……..……..……..……..…

Position: ……..……..……..……..……..……..……..……..……

Address: ……..……..……..……..……..……..……..……..……

Signature……..……..……..……..

On behalf of the data importer: ……..……..……..……..……..……..……..……..……

Name (written out in full): ……..……..……..……..……..……..……..……..……

Position: ……..……..……..……..……..……..……..……..……

Address: ……..……..……..……..……..……..……..……..……

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

Customer

Data importer
Glarish,Inc.

Data subjects
• Customers

• Customer's Agents, Employees, Authorized Users

Categories of data

- Identification data:
    - name, address, email, phone number and access rights.
- Customer Content:
    - Images
    - Videos
    - Power point
    - Pdf files etc

Special categories of data (if appropriate)

Not applicable

Processing operations

Collection, storage, transfer, as necessary for the provision of the Services based on the Agreement

DATA EXPORTER

Name:…….…….……(Customer)

Authorised Signature …….……

DATA IMPORTER

Name: Glarish,Inc.

Authorised Signature …….……

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

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

Same as those described in Attachment 2 to this DPA.

Liability

The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

a) the data exporter promptly notifying the data importer of a claim; and

b) the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim.