Data Processing Agreement

This Protection and Data Processing Agreement ("DPA") supplements the Service Agreement or other written or electronic agreement between Wish Collaboration and Customer for the purchase of telecommunication and other services from Wish Collaboration (hereinafter defined as "Services") (the "Agreement"). This DPA reflects the Parties' agreement with respect to Wish Collaboration's Processing of Customer Content, including any Personal Data contained therein, on behalf of Customer while Customer makes use of the Wish Collaboration Services. The Customer enters this DPA on behalf of itself, and to the extent required under Data Protection Laws and Regulations, on behalf of its Authorized Affiliates, to the extent such entities qualify as a Controller. As used herein, any references to the: (a) "Customer' shall include Customer and its Authorized Affiliates; and (b) "Agreement" will be construed as including this DPA. All capitalized terms not defined herein shall have the meaning given to them in the Agreement. This DPA consists of distinct parts: the main body of the DPA and, as applicable, Schedules 1, 2, 3, and 4. By executing this DPA, Wish Collaboration and Customer agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

Customer and Wish Collaboration's signature and acceptance of the Standard Contractual Clauses and their Appendices (as populated by the information located in this DPA and its Schedules), to the extent that the Standard Contractual Clauses are applicable and required for the lawful transfer and Processing of Personal Data.

{Client}

Name:

Title:

Email:

Address:

Date:

Wish Collaboration

Name:

Title:

Email:

Address:

Date:

HOW THIS DPA APPLIES

This DPA is executed by and between the Parties. Customer's Authorized Affiliates will also be covered by this DPA, provided that Customer is responsible for the acts and omissions of its Authorized Affiliates. For the avoidance of doubt, the Customer entity that is the contracting party to the Agreement shall, on behalf of itself and its Authorized Affiliates: (a) remain responsible for coordinating, making, and receiving all communication with Wish Collaboration under this DPA; and (b) exercise any rights herein in a combined manner with Wish Collaboration under this DPA.

DATA PROCESSING TERMS

1. DEFINITIONS

- **"Affiliate"** means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

- **"Authorized Affiliate"** means any of Customer's Affiliate(s) which: (a) are subject to Data Protection Laws and Regulations; and (b) are authorized by Customer to use the Services pursuant to the Agreement between Customer and Wish Collaboration, but have not signed their own Order Form with Wish Collaboration and are not otherwise a "Customer" as defined under the Agreement.

- **"CCPA"** means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.

- **"Controller"** means the entity which determines the purposes and means of the Processing of Personal Data.

- **"Customer Content"** means any telephone numbers, email address, end user names, postal addresses, recordings, or similar data that Wish Collaboration maintains or processes on Customer and/or its end-users' behalf.

- **"Data Protection Laws and Regulations"** means all laws and regulations, including the laws and regulations of Brazil, the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom, and the United States and its states, in each case, to the extent applicable to the Processing of Personal Data under the Agreement.

- **"Data Subject"** means, as applicable: (i) the identified or identifiable person to whom Personal Data relates as defined by Data Protection Laws and Regulations; and/or (ii) a "Consumer" as the term is defined in the CCPA.

- **"Data Subject Request"** means a request from a Data Subject to exercise their right: (i) of access; (ii) of rectification; (iii) of restriction of processing; (iv) of erasure (e.g., a "right to be forgotten"); (v) of data portability; (vi) to know any first- or third-party sharing activities; (vii) to know Wish Collaboration's relevant processing activities; (viii) to review the consequences of any objections or consent withdrawals; (ix) to not be subject to automated individual decision making; and/or (x) to object to the processing.

- **"GDPR"** means the 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).

- **"LGPD"** means Brazil Law No. 13.709, the General Law on Protection of Personal Data, as amended.

- **"Wish Collaboration"** means Wish Collaboration Inc., and its Affiliates engaged in the Processing of Personal Data in connection with providing the Services to Customer.

- **"Party"** or **"Parties"** means either the applicable Customer or Wish Collaboration entit(ies) individually, or together the Parties, who have entered into the Agreement and this DPA.
- **"Personal Data"** means any information relating to: (i) an identified or identifiable natural person (e.g., a Data Subject or Consumer); and/or (ii) an identified or identifiable legal entity (e.g., a household under CCPA), in each case, where such information is maintained on behalf of the Controller by the Processor within its Services environment and is protected similarly as personal data, personal information, or personally identifiable information under Data Protection Laws and Regulations.
- **"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, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **"Processor"** means the entity which Processes Personal Data on behalf of the Controller, including, as applicable, any "Service Provider' as the term is defined by the CCPA.
- **"Technical and Organizational Measures"** or **"TOMs"** means the applicable technical and organizational measures documentation located in Schedule 4 of this DPA.
- **"Standard Contractual Clauses"** means the standard contractual clauses, also known as "SCCs," attached to the European Commission's Implementing Decision (EU) 2021/914 found at https://eur-lex.europa.eu/eli/dec impl/2021/914/oj.
- **"Sub-processor"** means any Processor engaged by Wish Collaboration to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA.
- **"Supervisory Authority"** means an independent public authority established under applicable law to oversee compliance with Data Protection Laws and Regulations.

2. PROCESSING OF PERSONAL DATA

2.1 Roles of the Parties. The Parties agree that with regard to the Processing of Personal Data by Wish Collaboration on behalf of Customer, Customer is the Controller, Wish Collaboration is the Processor, and Wish Collaboration will engage Sub-processors as further detailed in Section 5 (Subprocessors) below.

2.2 Customer's Responsibilities. When using the Services, Customer shall Process Personal Data in accordance with Data Protection Laws and Regulations, including maintaining lawful basis (e.g., consent) and rights to use and provide Personal Data, as part of Customer Content. Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations.

2.3 Wish Collaboration's Responsibilities. Wish Collaboration shall treat Customer's Personal Data in a confidential manner, consistent with Section 6 of this DPA, and shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions, which are deemed given, for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement. As required under Article 28 of the GDPR, to the extent such Processing of Personal Data includes transfers of Personal Data to a third country or an international organization as legally required by European Union or Member State law to which Wish Collaboration is subject, Wish Collaboration shall inform the Customer of that legal requirement before initiating Processing,

unless the applicable European Union or Member State law prohibits such information on important grounds of public interest. Wish Collaboration shall immediately inform Customer if, in its opinion, it believes that any instructions of Customer conflict with or infringe the requirements of Applicable Data Protection Laws and Regulations.

2.4 Processing Details. The categories of Data Subjects, categories of Personal Data transferred, sensitive data transferred (if applicable), frequency of the transfer, nature, and purpose of Personal Data transfer and Processing, retention of Personal Data, and subject matter of the Processing are specified in Schedule 2 (Description of the Transfer) to this DPA.

3. RIGHTS OF DATA SUBJECTS

Unless legally prohibited from doing so, Wish Collaboration shall promptly notify Customer and/or direct the applicable Data Subject to Customer in the event that it receives a Data Subject Request. Taking into account the nature of the Processing, Wish Collaboration shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to requests related to a Data Subject's rights under Data Protection Laws and Regulations.

4. WISH COLLABORATION PERSONNEL

Wish Collaboration shall ensure that its personnel engaged in the Processing of Personal Data are: (a) informed of the confidential nature of the Personal Data and have executed written confidentiality agreements; (b) have received appropriate training on their responsibilities, specifically pertaining to security and privacy measures; and (c) only have access to Personal Data to the extent reasonably determined to be necessary in order to perform any obligations, responsibilities, or duties as further specified in this DPA and the Agreement. Further, to the extent permitted by applicable law, Wish Collaboration shall ensure that the confidentiality obligations specified in this Section 4 shall survive the termination of the personnel engagement.

5. SUB-PROCESSORS

5.1 Appointment of Sub-processors. Customer acknowledges and agrees that: (a) Wish Collaboration's Affiliates may be retained as Subprocessors; and (b) Wish Collaboration and its Affiliates may engage third-party Sub-processors in connection with the provision and operation of the Services. Prior to engaging any Sub-processors (whether a third-party or Wish Collaboration Affiliate), Wish Collaboration or a Wish Collaboration Affiliate shall carry out appropriate due diligence on the Sub-processor and enter into a written agreement with each Subprocessor which provides for sufficient guarantees from the Sub-processor to implement appropriate technical and organizational measures containing the same level of data protection obligations with respect to the protection of Customer Content in such a manner that the processing will meet the requirements of applicable Data Protection Laws and Regulations.

5.2 Current Sub-processors and Notice of New Sub-processors. Customer approves the Sub-processors referenced in Schedule 1 of this DPA. Wish Collaboration or a Wish Collaboration Affiliate may remove, replace or appoint suitable alternate Sub-processors at its own discretion in accordance with this Section 5.2 and Section 5.3. Wish Collaboration shall inform Customer of any new Sub-processors by providing an updated disclosure via email by contacting the designated Customer contact person no less than fifteen (15) business days before authorizing such Sub- processor(s) to Process Personal Data in connection with the provision of the applicable Services.

5.3 Objection Rights. Customer may, in good faith, reasonably object to Wish Collaboration's or Wish Collaboration Affiliate's use of a new Sub-processor by notifying Wish Collaboration

promptly in writing (email acceptable) within fifteen (15) business days after Wish Collaboration's notice in accordance with the mechanism set out in Section 5.2. Such notice shall explain the Customer's good faith and reasonable grounds for the objection. In the event Customer objects to a new Sub- processor, Wish Collaboration will use commercially reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If the Parties are unable to resolve such objection or Wish Collaboration is otherwise unwilling to resolve or make available such change within a reasonable period of time, Customer may terminate the applicable Order Form(s) with respect to those Services which cannot be provided by Wish Collaboration without the use of the objected-to new Sub-processor by providing written notice to Wish Collaboration. Wish Collaboration will refund Customer any prepaid, unused fees covering the remainder of the term of such Order Form(s) following the effective date of termination solely with respect to such terminated Services, without imposing a penalty for such termination on Customer.

5.4 Liability. Wish Collaboration shall be liable for the acts and omissions of its Sub-processors to the same extent Wish Collaboration would be liable if performing the applicable Sub-processor services directly under the terms of this DPA.

6. SECURITY

6.1 Protection of Customer Content. 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, Wish Collaboration shall implement and maintain appropriate technical and organizational measures for the protection of the security (including protection against a Security Incident, as defined below), confidentiality, and integrity of Customer Content, as set forth in the applicable Technical and Organizational Measures (Schedule 4). Wish Collaboration regularly monitors compliance with these measures and will not take any action to, intentionally or negligently, materially decrease the overall security of the Services during a subscription term.

6.2 Third-Party Certifications and Audits. Wish Collaboration shall make available to the Customer all information necessary to demonstrate compliance with its obligations under applicable Data Protection Laws and Regulations by making available, upon Customer's request and no more than once annually: (a) any written technical documentation that Wish Collaboration makes available or generally provides to its customer base; and (b) information regarding Wish Collaboration's compliance with the obligations in this DPA, in the form of applicable third-party certifications and/or audits (including those specified in the applicable Technical and Organizational Measures). Where required under Data Protection Laws and Regulations, the preceding may also include relevant information and documentation about Wish Collaboration's Sub-processors, to the extent, such information is available and may be distributed by Wish Collaboration. Should additional audit activities be deemed reasonably necessary, for example, if there is: (i) a requirement under Data Protection Laws and Regulations; (ii) a Security Incident; (iii) a material adverse change or reduction to the relevant data protection practices for Wish Collaboration's Services; and/or (iv) a breach of the material terms of this DPA, Customer may contact Wish Collaboration to request an audit by the Customer directly or another auditor appointed by the Customer of the procedures relevant to the protection of Personal Data under this DPA. Before the commencement of any such audit, Customer and Wish Collaboration shall mutually agree upon the scope, timing, duration, and/or reimbursable expenses (if any and solely to the extent permitted by Data Protection Laws and Regulations) of the audit. Customer shall: (a) promptly provide Wish Collaboration with information regarding any noncompliance discovered during the course of an audit; and (b) use best efforts to minimize interference with Wish Collaboration's business operations when conducting any such audit.

6.3 Data Protection Impact Assessment. If, pursuant to Data Protection Laws and Regulations, Customer is required to perform a data protection impact assessment, prior consultation with a Supervisory Authority having appropriate jurisdiction, privacy impact assessment, or the equivalent construct, in connection with their use of the Services provided by Wish Collaboration under this DPA, Wish Collaboration shall provide reasonable cooperation and assistance to Customer in helping to fulfill these obligations, to the extent such information is available to Wish Collaboration.

7. NOTIFICATIONS REGARDING CUSTOMER CONTENT

Wish Collaboration maintains security incident management policies and procedures, as further specified in the Technical and Organizational Measures, and shall notify Customer, without undue delay, of any actual breach of its security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Content, including any Personal Data therein, transmitted, stored or otherwise Processed by Wish Collaboration or its Sub-processors of which Wish Collaboration becomes aware (a "Security Incident"). Notification provided under this Section 7 shall not be interpreted or construed as an admission of fault or liability by Wish Collaboration. Wish Collaboration shall make reasonable efforts to identify the cause of such Security Incident and take those steps as Wish Collaboration deems necessary and reasonable in order to remediate the cause of such a Security Incident to the extent the remediation is within Wish Collaboration's reasonable control. Additionally, Wish Collaboration shall provide Customer with relevant information about the Security Incident, as reasonably required to assist the Customer in ensuring Customer's compliance with its own obligations under Data Protection Laws and Regulations, such as to notify any Supervisory Authority or Data Subject in the event of a Security Incident.

8. DELETION AND RETURN OF CUSTOMER CONTENT

Following the termination or expiration of the Agreement or earlier upon Customer's written request, Wish Collaboration shall delete and make irretrievable Customer Content, including any Personal Data therein, unless European Union law or Member State law requires or permits further storage of such Customer Content and/or other Personal Data. Automatic data retention periods shall be in accordance with the procedures and timeframes specified in the applicable Technical and Organizational Measures. Wish Collaboration shall certify the deletion of Customer Content and, upon request, shall provide proof of such certification. Additionally, upon Customer's written request, Wish Collaboration shall either return, or otherwise direct Customer on how to conduct a self-service data export (where available) of any Customer Content or other Personal Data retained by Wish Collaboration to Customer or Customer's representatives.

9. LIMITATION OF LIABILITY

Each Party's and all of its Affiliates' liability, in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Wish Collaboration, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference to the liability of a Party means the total liability of that Party and all of its Affiliates under the Agreement and all DPAs together.

10. EUROPEAN-SPECIFIC PROVISIONS

The following provisions shall apply to the extent that: (i) Customer is located in the European Union/European Economic Area; or (ii) is located outside of the European Union/European Economic Area but remains subject to the GDPR:

10.1 GDPR. To the extent Wish Collaboration Processes Personal Data on behalf of Customer,

it shall do so in accordance with the requirements of GDPR directly applicable to Wish Collaboration in the provision of its Services.

10.2 Standard Contractual Clauses. The Standard Contractual Clauses shall apply in addition to the DPA for any transfers of Personal Data under this DPA from the European Union, the European Economic Area, and/or Switzerland to countries that do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations of the foregoing territories. The Standard Contractual Clauses, pursuant to this Section 10.2, shall be structured as follows: (i) Module Two (Controller to Processor) terms shall apply, and Modules One, Three, and Four shall be deleted in their entirety; (ii) Clause 7 shall be deleted in its entirety, and the Parties may add additional entities to this DPA by executing an additional DPA; (iii) in Clause 9, Option 2 shall apply (as detailed in Section 5 of this DPA); (iv) the Annexes of the EU Standard Contractual Clauses shall be populated with the information set out in the Schedules to this DPA.

10.3 Alternative Data Transfer Mechanism. For the avoidance of doubt, should the transfer mechanism identified in Section 10.2 be deemed invalid by a Supervisory Authority or court with applicable authority, the Parties shall endeavor in good faith to negotiate an alternative mechanism (if available and required) to permit the continued transfer of Personal Data.

11. CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

For Customers and/or Data Subjects who are residents of the State of California, Wish Collaboration shall not: (a) sell any Personal Data; or (b) receive any Personal Data as consideration for any services or other items provided or performed by Wish Collaboration as a Service Provider under this Agreement. Wish Collaboration shall not collect, retain, share or use any Personal Data except as necessary for a business purpose pursuant to a written contract (i.e., to provide and operate the Wish Collaboration services) and subject to the restrictions specified in Section 1798.140 (v) of the CCPA. Wish Collaboration agrees to refrain from taking any action that would cause any transfers of Personal Data to or from Customer to qualify as "selling personal information" under the CCPA or any other similar applicable privacy laws.

12. BRAZILIAN GENERAL DATA PROTECTION LAW (LGPD)

For Customers and/or Data Subjects who are residents of the Federal Republic of Brazil, Wish Collaboration shall, where applicable: (a) provide its Services under the express obligations imposed by the LGPD on a Data Processor for the benefit of a Data Controller; and (b) as required under Articles 33 through 36 of the LGPD, transfer Personal Data on the basis of the Standard Contractual Clauses, as modified in accordance with the LGPD.

13. INTERNATIONAL TRANSFERS

For applicable jurisdictions outside of the European Economic Area, the Standard Contractual Clauses and/or standard contractual clauses that may be approved by a European Commission decision shall be utilized where required and/or permitted for the lawful transfer of Personal Data, provided that such terms shall be amended to align with Data Protection Laws and Regulations, as well as to reflect the appropriate Wish Collaboration contracting entity, choice of law, and location of disputes.

14. LEGAL EFFECT AND CONFLICT

This DPA shall become legally binding between Customer and Wish Collaboration upon execution of the Agreement. Once effective, this DPA shall be incorporated into and form part of the Agreement

or applicable Order Form. For matters not addressed under this DPA, the terms of the Agreement apply. With respect to the rights and obligation of the Parties vis-a-vis 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 the event of a conflict between the terms of the DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail.

List of Schedules:

Schedule 1: Approved Sub-Processors

Schedule 2: Description of the Transfer

Schedule 3: Provisions Related to the Standard Contractual Clauses

Schedule 4: Technical and Organizational Measures

SCHEDULE 1 - APPROVED SUB-PROCESSORS

Last Updated: January 1st, 2023

Customer authorizes the Sub-processors listed below to provide and operate the Wish Collaboration Services to which they have subscribed under their Agreement.

Co-location Hosting Providers

1.
Address:
Website:
Services:

2.
Address:
Website:
Services:

3.
Address:
Website:
Services:

4.
Address:
Website:
Services:

Cloud Hosting Providers

1.
Address:
Website:
Services:

2.
   Address:
   Website:
   Services:

Webcast Platform Providers:

1.
   Address:
   Website:
   Services:

Telephony/Bridging Providers:

1.
   Address:
   Website:
   Services:

2.
   Address:
   Website:
   Services:

3.
   Address:
   Website:
   Services:

SCHEDULE 2 – DESCRIPTION OF THE TRANSFER

The data importer (sub-processor) is a hosted audio-conferencing/teleconference services provider and may process personal data as the data exporter's sub-processor in the data exporter's audiocast and/or webcast services with dial-in teleconference and general meeting services. In this case, the data exporter's (processor) clients are the controllers. The data importer may process personal data upon the instructions of the data exporter.

Categories of data subjects whose personal data is transferred: Audiocast/Webcast (with dial-in teleconference) users.

Categories of personal data transferred: IP addresses, names, phone numbers of users calling the teleconference, call recordings, and the name of the company the user represents.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): The transfers are made when each audiocast with dial-in teleconference and/or general meeting is provided (one-off basis).

Nature of Processing: The nature of Processing may include, without limitation: Receiving data, including collection, accessing, retrieval, recording, and data entry; holding data, including storage, organization, and structuring; using data, including analysis, consultation, and testing; protecting data, including restricting, encrypting, and security testing; Returning data to the data exporter or data subject; and erasing data, including destruction and deletion.

Purpose(s) of the data transfer and further processing: The data exporter provides audiocast/webcast services with dial-in teleconference and general meeting services to its customers, where the users can participate in the event through a teleconference bridge provided by the importer. Thus, the purpose is to provide the services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: The personal data will be retained for 365 days unless otherwise agreed.

For transfers to (sub-) processors, also specify the subject matter, nature, and duration of Processing: Same as above.

SCHEDULE 3 – PROVISIONS RELATED TO THE STANDARD CONTRACTUAL CLAUSES

Identified Parties and Competent Supervisory Authority

Data Exporter

Name:

Address:

Contact Person's Name, Position, and Contact Details:

Activities Relevant to the Data Transferred Under the Standard Contractual Clauses: Processing personal data to provide, support, and improve the audio-conferencing/teleconference services to which the exporter has subscribed from the importer (so that the exporter can provide its services to its customers).

Role: Processor

Competent Supervisory Authority: The supervisory authority of the EEA Member State in which Customer is established or, if Customer is not established in the EEA, the EEA Member State in which Customer's representative is established or in which Customer's end-users or customers are predominantly located.

Data Importer

Name: Wish Collaboration

Address: 2800 Skymark Avenue Mississauga Ontario Canada M5G 2M4

Contact Person's Name, Position, and Contact Details: Luigi Calabrese CTO, privacy@wishcollaboration.com

Activities Relevant to the Data Transferred Under the Standard Contractual Clauses: Processing personal data to provide, support, and improve the audio-conferencing/teleconference services to which the exporter has subscribed from the importer (so that the exporter can provide its services to its customers).

Role: Sub-Processor

Competent Supervisory Authority: The supervisory authority of the EEA Member State in which Customer is established or, if Customer is not established in the EEA, the EEA Member State in which Customer's representative is established or in which Customer's end-users or customers are predominantly located.

SCHEDULE 4 – TECHNICAL AND ORGANIZATIONAL MEASURES

These Technical and Organizational Data Security Measures articulate the technical and organizational security measures implemented by Wish Collaboration ("Wish Collaboration") to support its Security Program.

Wish Collaboration has implemented and maintains a security program that leverages the ISO/IEC 27000-series of control standards as its baseline.

Access Control of Processing Areas (Physical)

Web applications, communications infrastructure, and database servers of Wish Collaboration are located in secure data centers. Wish Collaboration has implemented suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment (namely telephones, database and application servers. and related hardware) where Personal Data are processed or used.

Secure Physical Access Contol is accomplished by:

- Establishing security areas;
- Protection and restriction of access paths;
- Securing the data processing equipment and personal computers;
- Establishing access authorizations for employees and third parties, including the respective documentation;
- Regulations/restrictions on card-keys;
- Restricting physical access to the servers by using electronically-locked doors and separate cages within co-location facilities;
- Access to the data center where Personal Data is hosted is logged, monitored, and tracked via electronic and CCTV video surveillance by security personnel; and
- Data centers where Personal Data may be hosted are protected by security alarm systems and other appropriate security measures, such as user-related authentication procedures, including biometric authentication procedures (e. g., hand geometry), and/or electronic proximity identity cards with users' photographs.

Access Control to Data Processing Systems (Logical)

Wish Collaboration has implemented suitable measures to prevent its data processing systems from being used by unauthorized persons.

This is accomplished by:

- Establishing the identification of the terminal and/or the terminal user to the Wish Collaboration systems;
- An automatic time-out of user terminal if left idle, identification and password required to reopen;
- Automatic lockout of the user ID when several erroneous passwords are entered. Events are logged, and logs are reviewed on a regular basis;
- Utilizing firewall, router, and VPN-based access controls to protect the private service networks and back-end-servers;
- Continuously monitoring infrastructure security;
- Regularly examining security risks by internal employees and third-party auditors;
- Issuing and safeguarding of identification codes; and

- Role-based access control is implemented in a manner consistent with the principle of least privilege.
- Remote access to Wish Collaboration's services delivery network infrastructure is secured using two-factor authentication tokens.
- Access to host servers, applications, databases, routers, switches, etc., is logged.
- Access and account management requests must be submitted through internal approval systems.
- Access must be approved by an appropriate approving authority. In most cases, the approval for a request requires two approvals at a minimum: the employee's manager and the role approver or "owner" for the particular system or internal application.
- Passwords must adhere to the Wish Collaboration password policy, which includes minimum length requirements, enforcing complexity, and set periodic resets.
- Password resets are handled via the Wish Collaboration ticketing system. New or reset passwords are sent to the employee using an internal secure, encrypted email system or by leaving a voicemail for the employee.

Wish Collaboration employs intrusion detection systems and also uses commercial and custom tools to collect and examine its application and system logs for anomalies.

Access Control to Use Specific Areas of Data Processing Systems

Persons entitled to use the data processing system can only access Personal Data within the scope and to the extent covered by their respective access permission (authorization). Personal Data cannot be read, copied, modified, or removed without authorization.

This is accomplished by:

- Employee policies and training in respect of each employee's access rights to Personal Data;
- Users have unique login credentials -- role-based access control systems are used to restrict access to particular functions;
- Monitoring activities that add, delete or modify the Personal Data;
- Effective and measured disciplinary action against individuals who access Personal Data without authorization;
- Release of Personal Data to only authorized persons;
- Controlling access to account data and customer Personal Data via role-based access controls (RBAC) in compliance with the security principle of "least privilege";
- Internal segmentation and logical isolation of Wish Collaboration's employees to enforce least-privilege access policies;
- Requirements-driven definition of the authorization scheme and access rights, as well as their monitoring and logging;
- Regular review of accounts and privileges (typically every 3-6 months, depending on the particular system and sensitivity of data it provides access to);
- Control of files; controlled and documented destruction of data; and policies controlling the retention of backup copies.

Availability Control

Wish Collaboration has implemented suitable measures to ensure that Personal Data is protected from accidental destruction or loss.

This is accomplished by:

- Global and redundant service infrastructure that is set up with full disaster recovery sites;
- Constantly evaluating data centers and Internet service providers (ISPs) to optimize performance for its customers regarding bandwidth, latency, and disaster recovery isolation;
- Situating data centers in secure co-location facilities that are ISP carrier-neutral and provide physical security, redundant power, and infrastructure redundancy;
- Service level agreements from ISPs to ensure a high level of uptime;
- Rapid failover capability; and
- Maintaining full capacity disaster recovery (DR) sites and annually testing DR centers by shutting down primary sites for at least 24 hours unless the product runs in active/active configuration.
- Implements systems and processes to detect and defend against DDoS attacks.

Transmission Control

Wish Collaboration has implemented suitable measures to prevent Personal Data from being read, copied, altered, or deleted by unauthorized parties during the transmission or transport of the data.

This is accomplished by:

- Use of adequate firewall and encryption technologies to protect the gateways and pipelines through which the data travels;
- Sensitive Personal Data is encrypted during transmission using up to date versions of TLS or other security protocols using strong encryption algorithms and keys;
- Certain types of customer Sensitive Personal Data and other confidential customer data (e.g., payment card numbers) are encrypted at rest within the system;
- Protecting web-based access to account management interfaces by employees through encrypted TLS
- End-to-end encryption of screen sharing for remote access, support, or real-time communication;
- Use of integrity checks to monitor the completeness and correctness of the transfer of data.

Input Control

Wish Collaboration has implemented suitable measures to ensure that it is possible to check and establish whether and by whom Personal Data has been input into data processing systems or removed.

This is accomplished by:

- Authentication of the authorized personnel;
- Protective measures for Personal Data input into memory, as well as for the reading, alteration, and deletion of stored Personal Data, including by documenting or logging material changes to the customer account data or account settings;
- Segregation and protection of all stored Personal Data via database schemas, logical access controls, and/or encryption;
- Utilization of user identification credentials;
- Physical security of data processing facilities;
- Session time outs.

Separation of Processing for Different Purposes

Wish Collaboration has implemented suitable measures to ensure that Personal Data collected for different purposes can be processed separately.

Documentation

Wish Collaboration keeps documentation of technical and organizational measures in case of audits and for the conservation of evidence. Wish Collaboration takes reasonable steps to ensure that persons employed by it and other persons at the workplace are aware of and comply with the technical and organizational measures outlined in this document. Wish Collaboration, at its election, may make non-confidential portions of audit reports available to customers to verify compliance with the technical and organizational measures undertaken in this Program.

Monitoring

Wish Collaboration does not access Customer Personal Data, except to provide services to the Customer which Wish Collaboration is obligated to perform, to monitor, analyze and improve the services, in support of the Customer experience, as required by law, or on request by Customer; Wish Collaboration has implemented suitable measures to monitor access restrictions of Wish Collaboration's system administrators and to ensure that they act in accordance with instructions received.

This is accomplished by:

- Individual appointment of system administrators;
- Adoption of suitable measures to register system administrators' access logs to the infrastructure and keep them secure, accurate, and unmodified for a reasonable period of time;
- Keeping an updated list with system administrators' identification details (e.g., name, surname, function, or organizational area) and responsibilities.

Definitions

"Wish Collaboration" means Wish Collaboration and all of its direct and indirect subsidiaries.

"Customer" means any purchaser of any Wish Collaboration offering.

"Customer" has the same meaning as in the Addendum to which this Appendix is attached.

"Personal Data" means any information directly or indirectly relating to an identified or identifiable natural person.

"Sensitive Personal Data" means Personal Data (1) consisting of an individual's first name and last name, or first initial and last name, in combination with some other data element that could lead to identity theft or financial fraud, such as a government-issued identification number, financial account number, payment card number, date of birth, mother's maiden name, biometric data, electronic signature, health information, or (2) consisting of login credentials, such as a username and password or answer to a security question, that would permit access to an online account or an information system; or (3) revealing the personal health information (PHI) of a natural person.

"Security Framework" refers to the collection of Wish Collaboration's policies and procedures governing information security, including, but not limited to, policies, training, education, monitoring, investigation, and enforcement of its data management and security efforts.