LOOM DATA PROCESSING ADDENDUM

This Data Processing Agreement ("DPA") is entered into between Loom, Inc., located at 140 2nd Street, Floor 3, San Francisco, California 94105, USA ("Processor") and _____, located at _____ ("Controller"). This DPA is effective on the date that it has been duly executed by both parties.

1 Scope of this DPA

1.1 This DPA forms part of the Terms between Controller and Processor with regard to the processing of personal data that is subject to the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"). Terms used herein that are not otherwise defined have the meanings given in the Terms.

1.2 The parties agree that Processor acts as a data processor for Controller in providing the Service.

1.3 "Personal data" has the meaning given in the GDPR.

1.4 "Standard Contractual Clauses" means the clauses annexed to EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ L 39, 12.2.2010, p. 5-18).

1.5 "International Data Transfer" means any transfer of Controller Personal Data from the EEA, Switzerland or the United Kingdom to an international organization or to a country outside of the EEA, Switzerland and the United Kingdom.

2 Processing of personal data

2.1 The parties agree that Processor will process the personal data only for the purposes of providing the Service. The types of personal data and the specific uses of the personal data are specified in Exhibit A attached hereto.

2.2 Controller hereby authorizes Processor to perform International Data Transfers to any country deemed adequate by the EU Commission; or pursuant to the Standard Contractual Clauses. By signing this DPA, Controller and Processor conclude the Standard Contractual Clauses, which are hereby incorporated into this DPA and completed as follows: the "data exporter" is Controller; the "data importer" is Processor; the governing law in Clause 9 and Clause 11.3 of the Standard Contractual Clauses is the law of the country in which Controller is established; Appendix 1 and Appendix 2 to the Standard Contractual Clauses, are **Exhibit 1** and **2** to this DPA respectively; and the optional indemnification clause is struck. If Processor's compliance with the Standard Contractual Clauses is affected by circumstances outside of Processor's control, including if the Standard Contractual Clauses are invalidated, amended, or replaced, then Controller and Processor will work together in good faith to reasonably resolve such non-compliance.

3 Processor's general obligations

3.1 Processor must ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.2 Processor shall implement appropriate technical and organizational measures to prevent the personal data from being:

(i) accidentally or unlawfully destroyed, lost or altered,

(ii) disclosed or made available without authorization, or

(iii) otherwise processed in violation of applicable laws.

3.3 The appropriate technical and organizational security measures must be determined with due regard for:

(i) the current state of the art,

(ii) the cost of their implementation, and

(iii) 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.

3.4 Processor shall upon request provide Controller with sufficient information to enable Controller to ensure that Processor complies with its obligations under this DPA, including ensuring that the appropriate technical and organizational security measures have been implemented.

3.5 Controller is entitled at Controller's own cost to appoint an independent expert who shall have access to Processor's premises and receive the necessary information in order to be able to audit whether Processor complies with its obligations under this DPA, including ensuring that the appropriate technical and organizational security measures have been implemented. Controller shall provide Processor with 14 days prior written notice, and Controller is obligated to ensure that the expert signs a customary non-disclosure agreement, treats all information obtained or received from Processor confidentially, and may only share the information with Controller. Any findings or reports created on the basis of such an inspection must be shared with Processor and shall be regarded as confidential information.

3.6 Processor must without undue delay after becoming aware of the facts in writing notify Controller about:

(i) any request for disclosure of personal data processed under this DPA by authorities, unless expressly prohibited under European Union or member state law,

(ii) any finding of (a) breach of security that results in accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed by Processor in connection with the Service, or (b) other failure to comply with Processor's obligations under this DPA, or

(iii) any request for access to the personal data received directly from the data subjects or from third parties relating to the processing of personal data on Controller's behalf.

3.7 Processor must promptly assist Controller with the handling of any requests from data subjects under Chapter III of the GDPR, including requests for access, rectification, blocking or deletion, which relates to the processing of personal data in connection with the Service.

3.8 Processor must assist Controller with meeting the other obligations that may be incumbent on Controller according to European Union or member state law related to data processing where the assistance of Processor is implied, and where the assistance of Processor is necessary for Controller to comply with Controller's data protection obligations.

4 Subprocessors

4.1 Controller hereby grant Processor a general authorization to engage subprocessors. At the time of this DPA, Processor uses the subprocessors listed here to provide the Service. Processor undertakes to inform Controller of any intended changes concerning the addition or replacement of a subprocessor by providing prior written notice via Controller's account. If Controller can document objective and valid reasons not to accept suggested new subprocessors, Controller may object to the use of these suggested new subprocessors. If Processor chooses not to suggest alternative subprocessors, or if Controller has valid and objective reasons to object to all suggested alternatives, Controller is entitled to terminate the Terms with Processor within 30 days after receiving notice hereof.

4.2 Prior to the engagement of a subprocessor, Processor shall conclude a written agreement with the subprocessor, in which at least the same data protection obligations as set out in this DPA shall be imposed on the subprocessor, including an obligation to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR.

5 Term and consequences of the termination of this DPA

5.1 The term of this DPA shall correspond to the term of the Terms.

5.2 On Controller's request, Processor shall immediately transfer or delete (including anonymize) personal data which Processor is processing for Controller, unless European Union or member state law requires storage of the personal data.

6 Priority

6.1 If any of the provisions of this DPA conflict with the provisions of the Terms, the provisions of this DPA shall prevail.

Exhibit A

Subject Matter of Processing	The subject matter of the processing is the Service pursuant to the Terms.
Duration of Processing	The processing will continue until the expiration or termination of the Terms.
Categories of Data Subjects	Employees and other authorized users of Controller.
Nature and Purpose of Processing	Nature: Processing as part of the Service provided to Controller by Processor under the Terms. Purpose: The purpose of the processing is to provide the Service pursuant to the Terms.
Types of Personal Data	Includes the following: ● Name, email address, payment information and related personal data required to register for the Service; ● Transaction logs for transactions conducted by Controller using the Service; ● Information about the Controller hardware and software used to access the Service; ● Information collected by tracking Controller's posting and usage of content on the Service; ● Employee authentication information, including user IDs such as user email addresses and organization group and department information to allow Controller to create access control policies; ● Other data provided by Controller to facilitate Processor's provision of the Service to Controller.

Exhibit B

Security Measures

Processor will implement the following types of security measures:

1. **Physical access control**

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware):

- Establishing security areas, restriction of access paths;
- Establishing access authorizations for employees and third parties;
- Access control system (ID reader, magnetic card, chip card);
- Key management, card-keys procedures;
- Door locking (electric door openers etc.);
- Security staff, janitors;
- Surveillance facilities, video/CCTV monitor, alarm system; and
- Securing decentralized data processing equipment and personal computers.

2. **Virtual access control**

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include:

- User identification and authentication procedures;
- ID/password security procedures (special characters, minimum length, change of password);
- Automatic blocking (e.g. password or timeout);
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts;
- Creation of *one* master record per user, user-master data procedures per data processing environment; and
- Encryption of archived data media.

3. **Data access control**

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to Personal Data in accordance with their access rights, include:

- Internal policies and procedures;
- Control authorization schemes;
- Differentiated access rights (profiles, roles, transactions and objects);
- Monitoring and logging of accesses;
- Disciplinary action against employees who access Customer Personal Data without authorization;
- Reports of access;
- Access procedure;
- Change procedure;
- Deletion procedure; and
- Encryption.

4. **Disclosure control**

Technical and organizational measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, include:

- Encryption/tunneling;
- Logging; and
- Transport security.

5. **Entry control**

Technical and organizational measures to monitor whether Personal Data have been entered, changed or removed (deleted), and by whom, from data processing systems, include:

- Logging and reporting systems; and
- Audit trails and documentation.

6. **Control of instructions**

Technical and organizational measures to ensure that Personal Data are Processed solely in accordance with the instructions of the Controller include:

- Unambiguous wording of the contract;
- Formal commissioning (request form); and
- Criteria for selecting the Processor.

7. **Availability control**

Technical and organizational measures to ensure that Personal Data are protected against accidental destruction or loss (physical/logical) include:

- Backup procedures;
- Uninterruptible power supply (UPS);
- Remote storage;
- Anti-virus/firewall systems; and

8. **Separation control**

Technical and organizational measures to ensure that Personal Data collected for different purposes can be Processed separately include:

- Separation of databases;
- Segregation of functions (production/testing); and
- Procedures for storage, amendment, deletion, transmission of data for different purposes.