SilkRoad Client Data Processing and GDPR Addendum

This Data Processing and GDPR Addendum ("DPA") provides a set of supplemental obligations that SilkRoad Technology, Inc. ("SilkRoad") hereby assumes as part of the agreement (the "Agreement") with each SilkRoad customer (the "Customer") who has purchased and maintains an active subscription to use SilkRoad's software as a service (SAAS) products (the "Hosted Services"). This DPA shall be effective on the later of (i) the effective date of the Agreement, and (ii) 25 May 2018 ("Effective Date"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement. In the event that SilkRoad and Customer have entered into a separate signed agreement document with regard to compliance with the Data Protection Laws (defined below), this DPA shall not apply; provided, however, that at a minimum, SilkRoad shall in any case be bound by its obligations set forth in this DPA.

1. Definitions

"**Affiliate**" has the meaning set forth in the Agreement.

"**Agreement**" means the agreement between Client and SilkRoad for the provision of the SilkRoad Hosted Service to Client.

"**California Privacy Statutes**" means the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et. seq. ("CCPA") and the California Privacy Rights Act of 2020 ("CPRA").

"**Client Data**" has the meaning set forth in the Agreement.

"**Client Personal Data**" means any Client Data that is Personal Data.

"**Data Protection Laws**" means all data protection and privacy laws applicable to the respective party in its role in the processing of Personal Data under the Agreement, including, where applicable, EU Data Protection Law , the data protection laws in the United Kingdom and Switzerland and the California Privacy Statutes.

"**Data Controller**" means an entity that determines the purposes and means of the processing of Personal Data.

"**Data Processor**" means an entity that processes Personal Data on behalf of a Data Controller.

"**EU Data Protection Law**" means (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data ("**Directive**") and (ii) on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**"), and repealing Directive 95/46/EC.

"Hosted Service" has the meaning set forth in the Agreement.

"Standard Contractual Clauses" means the then-current Standard Contractual Clauses for International Transfers of Personal Data as approved by the European Commission, the United Kingdom, and Switzerland, respectively**.**

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

"**Processing**" has the meaning given to it in the GDPR and "**process**", "**processes**" and "**processed**" will be interpreted accordingly.

"**Security Incident**" means any unauthorized or unlawful breach of security in the Hosted Service that leads to the unauthorized disclosure of or access to Client Personal Data.

"**Sub-processor**" means any Data Processor engaged by SilkRoad or its Affiliates to assist in fulfilling its obligations with respect to providing the SilkRoad Hosted Service pursuant to the Agreement or this DPA. Sub-processors may include third parties or SilkRoad's Affiliates.

The terms, "**Controller**", "**Member State**", "**Processor**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR. The terms "**Business**", "**Business Purpose**", "**Consumer**" and "**Service Provider**" shall have the same meaning as in the California Privacy Statutes.

For the purpose of clarity, within this DPA "**Controller**" shall also mean "**Business**", and "**Processor**" shall also mean "**Service Provider**", to the extent that the California Privacy Statutes applies. In the same manner, Processor's Sub-processor shall also refer to the concept of Service Provider.

2. Scope and Applicability of this DPA

3.1 This DPA applies where and only to the extent that SilkRoad Processes Client Personal Data on behalf of Client as Data Processor in the course of providing Hosted Service pursuant to the Agreement.

3.2 Notwithstanding expiry or termination of the Agreement, this DPA will remain in effect until, and will automatically expire upon, deletion of all Client Personal Data by SilkRoad as described in this DPA or termination of the Agreement.

3. Roles and Scope of Processing

4.1 **Role of the Parties**. As between SilkRoad and Client, Client is either the Data Controller of Client Personal Data, or in the case that Client is acting on behalf of a third party Data Controller, then a Data Processor, and SilkRoad shall process Client Personal Data only as a Data Processor acting on behalf of Client.

4.2 **Client Processing of Personal Data**. Client agrees that (i) it will comply with its obligations under Data Protection Laws in respect of its processing of Personal Data, including any obligations specific to its role as a Data Controller and/or Data Processor (as applicable), and any processing instructions it issues to SilkRoad; and (ii) it has provided notice and obtained (or will obtain) all consents and rights necessary under Data Protection Laws for SilkRoad to process Personal Data and provide the SilkRoad Hosted Service pursuant to the Agreement and this DPA. If Client is itself a Data Processor, Client warrants to SilkRoad that Client's instructions and actions with respect to that Client Personal Data, including its appointment of SilkRoad as another Data Processor, have been authorized by the relevant Data Controller to the extent required under applicable law.

4.3 **Client Instructions**. SilkRoad will process Client Personal Data only for the purposes described in this DPA and only in accordance with Client's lawful instructions documented in this DPA, the Agreement, and via Client's use of the Hosted Service, and in order for SilkRoad to fulfil its obligations to provide Hosted Service under the Agreement ("Client Instructions"). The parties agree that this DPA and the Agreement set out the Client's complete and final instructions to SilkRoad in relation to the processing of Client Personal Data. Additional processing outside the scope of these Client Instructions (if any) will require prior written agreement between Client and SilkRoad.

4.4 **Details of Data Processing.**

(a) Subject matter: The subject matter of the data processing under this DPA is the Client Personal Data.

(b) Purpose: The purpose of the data processing under this DPA is the provision of the SilkRoad Hosted Service to the Client and the performance of SilkRoad's obligations under the Agreement (including this DPA) or as otherwise agreed by the parties in mutually executed written form.

(c) Duration: As between SilkRoad and Client, the duration of the data processing under this DPA is until the termination of the Agreement in accordance with its terms.

(d) Nature of the processing: SilkRoad provides the Hosted Service, which may process Client Personal Data upon the instruction of the Client in accordance with the terms of this DPA, the Agreement, and Client Instructions.

4.5 **Access or Use**. SilkRoad will not access or use Client Personal Data, except as necessary to maintain or provide the SilkRoad Hosted Service and its obligations under the Agreement, this DPA, or as necessary to comply with the law or binding order of a governmental body.

4. Subprocessing

5.1 **Authorized Sub-processors**. Client agrees that SilkRoad may engage Sub-processors, to provide data centers to host Client Data and the Hosted Services application software, disaster recovery, and backup related services and to otherwise Process Personal Data on its behalf. Client hereby consents to SilkRoad's use to the Sub-processors currently utilized by SilkRoad to Process Client Personal Data. SilkRoad will provide a then-current list of the Sub-processors engaged by it on Client's written request. SilkRoad shall inform the Client (via an email or other electronic communication) of any intended addition of any new Sub-processor (whether to replace an existing Sub-processor or otherwise). If Client does not object to such new Sub-processor for a period of 10 days thereafter, Client shall be deemed to have consented to such new Sub-processor. If Client reasonably objects in writing within such 10-day period to SilkRoad's proposed use of such new Sub-processor, SilkRoad will either (i) refrain from permitting such objected-to new Sub-processor from Processing Client Personal Data within 30 days thereafter; or (ii) notify the Client within 30 days thereafter that it is not able to refrain from using such objected-to new Sub-Processor without adversely impacting the applicable Hosted Services product ("Non-Feasibility Notice"). Upon receipt of such Non-Feasibility Notice, Client shall have the option for a period of 30 days thereafter, terminate upon written notice its subscription to use only those Hosted Services products which cannot be provided by SilkRoad without the use of the objected-to new Sub-processor. Such termination shall be without penalty or liability (other than for fees due and owing to SilkRoad for any services performed prior to such termination) effective immediately upon written notice of such termination to SilkRoad.

5.2 **Sub-processor Obligations**. SilkRoad will: (i) enter into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Client Personal Data to the standard required by Data Protection Laws; and (ii) remain responsible for its compliance with the obligations of this DPA and for any breach of this DPA caused by acts or omissions of the Sub-processor to the same extent that SilkRoad would be liable if such breach was committed by SilkRoad.

5. Security

6.1 **Security Measures**. SilkRoad shall implement and maintain appropriate technical and organizational security measures to preserve the security and confidentiality of the Client Personal Data processed by the Hosted Service.

6.2 **Security Incident Response**. Upon confirming a Security Incident, SilkRoad shall: (i) notify Client without undue delay, and in any event such notification shall, where feasible, occur no later than 72 hours from SilkRoad confirming the Security Incident; (ii) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Client; and (iii) SilkRoad shall promptly take reasonable steps to contain, investigate, and mitigate any Security Incident. SilkRoad's notification of or response to a Security Incident under this Section 5.2 (Security Incident Response) will not be construed as an acknowledgment by SilkRoad of any fault or liability with respect to the Security Incident.

6. Client Responsibilities.

Client agrees that SilkRoad has no obligation to protect Client Personal Data that Client elects to store or transfer outside of SilkRoad's systems (for example, offline or on-premise storage on Client's computers).

7. International Transfers

SilkRoad hosts Client Personal Data in the United States unless otherwise specified in the Agreement or the applicable Order Form), provided, however, that Client's Users may access and use the Hosted Service via the Internet from any international location where they connect to the Internet, and international transfers of Client Personal Data may take place in the ordinary course of providing Support and Maintenance for the Hosted Services. International transfers of Client Personal Data which are required under applicable privacy laws to be covered by the terms and principle set forth the Standard Contractual Clauses shall be governed by the Standard Contractual Clauses, as applicable. In connection therewith, Annexes 1, 2 and 3 to this DPA shall be deemed to be appendixes to the applicable Standard Contractual Clauses.

8. Return or Deletion of Client Data

9.1 **Deletion by Client**. SilkRoad will cooperate with Client to enable deletion of Client Personal Data in accordance with the procedures set forth in 9.1 below.

9.2 **Deletion on Termination.** For 90 days following termination or expiration of the Agreement, Client may retrieve any remaining Client Personal Data in accordance with the Agreement. Thereafter, Client hereby instructs SilkRoad to automatically delete all remaining Client Personal Data . SilkRoad shall not be required to delete Client Personal Data to the extent (i) SilkRoad is required by applicable law or order of a governmental or regulatory body to retain some or all of the Client Personal Data; and/or (ii), Client Personal Data it has archived on back-up systems, which Client Personal Data SilkRoad shall securely isolate and protect from any further processing, except to the extent required by applicable law.

9. Cooperation

10.1 The SilkRoad Hosted Service provides Client with a number of controls that Client may use to retrieve, correct, or delete Client Personal Data, which Client may use to assist it in connection with its obligations under the GDPR, including its obligations relating to responding to requests from data subjects or applicable data protection authorities. To the extent that Client is unable to access the relevant Client Personal Data within the SilkRoad Hosted Service using existing controls or otherwise, SilkRoad shall offer consulting services to Client at time and materials rates to reasonably assist Client in responding to any requests from individuals or applicable data protection authorities relating to the processing of Client Personal Data under the Agreement. In the event that any request from individuals or applicable data protection authorities is made directly to SilkRoad, SilkRoad shall not respond to such communication directly without Client's prior authorization, unless legally compelled to do so, and instead, after being notified by SilkRoad, Client shall respond. If SilkRoad is required to respond to such a request, SilkRoad will promptly notify Client and provide it with a copy of the request unless legally prohibited from doing so.

10.2 Client acknowledges that SilkRoad is required under the GDPR to: (a) collect and maintain records of certain information, including the name and contact details of each Data Processor and/or Data Controller on behalf of which SilkRoad is acting and, where applicable, of such Data Processor's or Data Controller's local representative and data protection officer; and (b) make such information available to the supervisory authorities. Accordingly, Client will, where requested, provide such information to SilkRoad.

10.3 Security Reports and Audits. SilkRoad shall provide written responses on a confidential basis to reasonable requests for information made by Client related to its Processing of Client Personal Data related to information security and audit questionnaires necessary to confirm SilkRoad's compliance with this DPA and the Data Protection Laws, provided that Client shall not exercise this right more than once per year, and any such request shall not be made in a manner so as to interfere with SilkRoad business.

10.4 In the event the Client is required to carry out data protection impact assessments under EU Data Protection Law, SilkRoad will (at Client's request and expense) no more than once annually, provide reasonably requested information regarding the SilkRoad Hosted Service to enable the Client to carry out such data protection impact assessments.

10. California Privacy Statutes Standard of Care; No Sale or Sharing of Personal Information**.**

SilkRoad acknowledges and confirms that it does not receive or process any Personal Information as consideration for any services or other items that SilkRoad provides to Client under the Agreement. SilkRoad shall not have, derive, or exercise any rights or benefits regarding Personal Information Processed on Client's behalf, and may use and disclose Personal Information solely for the purposes for which such Personal Information was provided to it, as contemplated under the Agreement and this DPA. SilkRoad certifies that it understands the rules, requirements and definitions of the California Privacy Statutes and agrees to refrain from "selling" or "sharing" (as such terms are defined in the California Privacy Statutes) any Personal Information Processed hereunder without Client's prior written consent, nor take any action that would cause any transfer of Personal Information to or from SilkRoad under the Agreement or this DPA to qualify as "selling" or "sharing" such Personal Information under the California Privacy Statutes. SilkRoad shall comply with the California Privacy Statures and implement the privacy protections required under the California Privacy Statutes. SilkRoad shall not combine Personal Information received from Client and its Users with Personal Information collected through other means from third parties outside the context of the Agreement or this DPA. SilkRoad shall notify Client if it determines that it can no longer meet its obligations under the California Privacy Statutes.

11. Relationship with the Agreement

11. 1 Precedence. The parties agree that DPA shall replace any existing DPA the parties may have previously entered into in connection with the SilkRoad Hosted Service. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict in connection with its subject matter.

11.2 Liability. The liability of each party and each party's Affiliates under this DPA shall be subject to the exclusions and limitations of liability set out in the Agreement.

11.3 Applicable Law. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

11.4 Termination. This DPA will continue for so long as SilkRoad is hosting, storing and/or processing Client Personal Data in connection with the Agreement.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: …

Address: …

Contact person's name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): …

2. …

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: SilkRoad Technology, Inc.

Address: 100 South Wacker Drive, Suite 425, Chicago, IL 60606

Contact person's name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): …

2. …

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Employees and contractors of the controller or one or more affiliates of controller

Categories of personal data transferred.

Human resources related data. Data may include, but is not limited to, name, address, identifying numbers (Social Security Number), pay rate and other personal information required to manage an employee.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, log files which track activity, encryption, all items listed in security annex

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous

Nature of the processing

The Services that the Data Importer provides consists of a suite of standardized software as a service (SAAS) applications for various human resources functions within an organization (e.g., employee onboarding). A Data Exporter's SAAS subscription includes a database account which is used to store human resources related data that is uploaded to the database account by Data Exporter's users or generated through use of the SAAS application by the Data Exporter's users. Data Importer does not access the data residing within the Data Exporter's SAAS database account in the ordinary course. Data Exporter's users directly and independently access, upload, download, modify, delete, manage and manipulate such data using the SAAS application. The range of functions available for processing the data are limited to the features and functionality of the standard SAAS application.

Purpose(s) of the data transfer and further processing

Human resources operations.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Term of the services contract and for an amount of time thereafter that is reasonable and appropriate to fulfill the processor's obligations under the contract.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Data centers in the cloud and co-location data centers to host the application and process data. Disaster recovery and data backup services. Third party application functionality.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

……..

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

- Measures of encryption of personal data
- Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing
- Measures for user identification and authorisation
- Measures for the protection of data during transmission
- Measures for the protection of data during storage
- Measures for ensuring physical security of locations at which personal data are processed
- Measures for ensuring events logging
- Measures for ensuring system configuration, including default configuration
- Measures for internal IT and IT security governance and management
- Measures for certification/assurance of processes and products
- Measures for ensuring data quality

- Measures for ensuring accountability

- Measures for ensuring erasure

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter. As per standard contractual clauses with sub-processors

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

Sub-Processor List for SilkRoad SAAS Products

Sub-Processor Name	Location	Sub-Processor Product	SilkRoad Product
US Government - DHS/USCIS	Washington, DC	E-Verify	Onboarding
Iron Mountain	U.S.	off-site back up tape storage	All
Iron Mountain	Canada	off-site back up tape storage	All
Rogers Data Centre	Canada	hosting facility Canadian datacenter	All
Rogers Data Centre	Canada	Canadian DR site	All
North State (formerly Data Chambers)	Winston-Salem, NC	Co-location Data Center	All
North State (formerly Data Chambers)	Kannapolis NC	Warm Site/ DR Site	All
Microsoft	U.S.	Azure (PaaS) hosting	Onboarding
Microsoft	U.S.	Text Analysis	Performance

Microsoft	U.S.	Azure (PaaS) Hosting Service	Onboarding, Analytics
Microsoft	U.S.	Logicapps	Onboarding, Recruiting
Microsoft	U.S.	PowerBI	Analytics
Microsoft-Services	Seattle, WA	Logicapps	Full Service Integration (if Client orders FSI project)
HelloSign	AWS US East (N. Virginia and Ohio).	E-signature Service	All
Joynd (formerly Cloudmills)	AWS – distributed US	SR/HRIS data integration middleware	Full Service Integration (if Client orders FSI project)
ADP	Non-disclosed Location	WorkforceNow	HRMS via Connect (if Client requests integration to ADP)
CWS Software	Florham Park, NJ	TimeOut (PTO processing)	HRMS (if Client requests integration to TimeOut)
HCR Software	Jacksonville, FL	Compensation XL	HRMS (if Client requests integration to Compensation XL)
	Non-disclosed		Heartbeat

Fidelity	Location	Payroll	(if Client requests integration to Fidelity)

Sub-Processors for SilkRoad Recruiting Utilized Only Upon Client's Specific Request

(Data Sharing with these Vendors can be discontinued if requested by Client)

Sub-Processor Name	Location	Sub-Processor Product	SilkRoad Product
SterlingBackcheck	AWS: undisclosed US locations	Screening Direct and SterlingONE Background Check Platforms	Recruiting
Vertical Screen	Undisclosed Location	Background Check	Recruiting
HireRight	US: Las Vegas, NV & Reno, NV EMEA: East London & Woking	Background Check	Recruiting
LexisNexis	Undisclosed Location	Background Check	Recruiting
OrangeTree	Minnetonka, MN (US) AWS: undisclosed US location	Background Check	Recruiting
Accurate	Elk Grove Village, IL. Ashburn, VA.	Background Check	Recruiting
Cisive	Holtsville, NY	Background Check	Recruiting
Private Eyes	Walnut Creek, CA	Background Check	Recruiting
Risk Assessment Group	Phoenix, AZ	Background Check	Recruiting

Talent+	AWS: undisclosed US location	Assessment	Recruiting
JOYND (formerly HRNX)	Chicago, IL	Background Check & Assessment	Recruiting
Broadbean	Undisclosed	Job Posting	Recruiting
JobTarget	Marlborough, MA	Job Posting	Recruiting
EmployeeReferrals.com	AWS: undisclosed US location	Employee Referrals	Recruiting
Indeed (Apply with Indeed)	Undisclosed	Candidate Apply Option	Recruiting
LinkedIn (Apply with LinkedIn)	All Client and personal data stored in data centers in US and Singapore.	Candidate Apply Option	Recruiting
Twilio		SMS communication	Recruiting Conversations
Nylas		Client scheduling	Recruiting Scheduling