Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name:SilkRoad Technology, Inc. Trading name (if different): Main address (if a company registered address): 100 South Wacker Drive, Suite 425, Chicago, IL 60606 Official registration number (if any) (company number or similar identifier):

Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Job Title: Contact details including email:
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1		Included	Decline to include	General Authorisation	Term of Service Contract and	Yes

					reasonable period afterward to perform obligations after termination of contract	
2						
3						
4						

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: 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): …

Annex 1B: 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 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.

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 (Modules 2 and 3 only):

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)
Fidelity	Non-disclosed Location	Payroll	Heartbeat (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

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: X Importer X Exporter neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix	As set out in Table 3.

Information	
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will

take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

        "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

        "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d. Clause 8.7(i) of Module 1 is replaced with:

        "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

    e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

        "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

    f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

    g. References to Regulation (EU) 2018/1725 are removed;

    h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with

the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information.

This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a its direct costs of performing its obligations under the Addendum; and/or

    b its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory Part 2: Mandatory Clauses of the Approved Addendum, **Clauses** being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.