DATA PRIVACY ADDENDUM

This Data Privacy Addendum ("Agreement") is incorporated by reference into that certain Master Software as a Service Agreement (the “MSA”) and all related orders for Services (defined below) between [CLIENT] (“**Client**”) and Teleskope, LLC ("**Vendor**"). This Agreement is entered into as of the later of the dates beneath the parties' signatures below or on the acceptance of the MSA.

BACKGROUND

Vendor and Client (each a “party” and together the “parties”) are, or are about to be, parties to one or more agreements whereunder Vendor processes data owned or controlled by Client. This Agreement shall address data protection issues required by law, such as the European General Data Protection Regulation 2016/679 (“**GDPR**”), the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100, *et seq.* (“**CCPA**”), and/or good business practices in all current and future contractual relationships between the parties. To the extent that any Data Protection Laws are applicable to the Processing of Personal Data, the applicable provisions of this Agreement shall determine the obligations of the parties.

1. DEFINITIONS

1.1. "**Client Data**" means any Personal Data in any form, collected, generated, Processed or used for or in relation to the Services.

1.2. “**Data Protection Laws**” means all data protection laws controlling the Processing of the Client Data and the provision of Services by Vendor, including but not limited to, as applicable: (a) the local law and regulation of the place(s) where all Processing by Vendor and its Personnel takes place; (b) the GDPR; and (c) the CCPA, in each case as amended, replaced or supplemented from time to time, and all subordinate legislation made under them, together with any codes of practice or other guidance issued by the governments, agencies, data protection regulators, or other relevant authorities.

1.3. “**Personal Data**” means any information relating to an identified or identifiable natural person or household and/or any information identified as such by Client.

1.4. “**Personnel**” means all officers, directors and employees (including of its affiliates), independent contractors or service providers of Vendor.

1.5. “**Processing**” means any operation or set of operations which is performed on Client Data or on subsets of Client Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, retention, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.6. “**Sell**” is defined in Section 1798.140(t) of the CCPA. “Sell” shall also mean “**Share**” when applicable under any Data Protection Laws, including any amendment to CCPA, such as the California Privacy Rights Act of 2020.

1.7. “**Services**” means any services performed by Vendor or its Personnel in any agreement between Vendor and Client.

1.8. “**Underlying Agreement**” means any written agreement between the parties, whether in existence at the time of execution of this Agreement or a future contractual relationship, under which Vendor provides Services to Client and Processes Client Data.

2. APPOINTMENT

2.1. If, at any time, Client requests that Vendor Process Client Data, the parties agree that for the purposes of the Data Protection Laws, Client is the data controller and business, and Vendor is the Service Provider and data processor of any Client Data.

2.2. Vendor and its Personnel shall Process the Client Data only to the extent, and in such a manner, as is necessary for the provision and improvement of the Services or Client’s written instructions from time to time and shall not process Client Data for any other purpose. The types of Client Data to be Processed by the Vendor will be limited to the data specified in this Agreement or in the Underlying Agreement between the parties.

2.3. Vendor acknowledges and confirms that it does not receive any Client Data as consideration for any Services or other items provided to Client. Vendor must not Sell any Client Data or disclose it for a commercial purpose. Also, Vendor must not collect, retain, share or use any Client Data except as necessary to perform services for Client. Vendor agrees to refrain from taking any action that would cause any transfers of Client Data to or from Vendor to qualify as "selling” or “sharing” personal information under the Data Protection Laws.

2.4. Vendor shall not retain, use, or disclose Client Data in the servicing of a different business or otherwise outside the direct business relationship between Vendor and Client.

2.5. Vendor shall logically keep separated Client Data received from or on behalf of Client from any other Personal Data, except as necessary to provide the Services.

2.6. Vendor shall immediately notify Client if, in its opinion, any instruction made pursuant to this Agreement does not conform with applicable Data Protection Laws.

2.7. Upon termination of the Underlying Agreement or Client's request, whichever is sooner, Vendor shall, and shall procure that the Personnel and any sub-processors shall, within thirty (30) days of termination of the Underlying Agreement or of Client's request (whichever comes soonest), cease using the Client Data and promptly deliver in a manner reasonably acceptable to Client or destroy all Client Data, unless applicable Data Protection Laws requires the continued storage of Client Data.

2.8. Notwithstanding anything to the contrary, the obligations in this Agreement will remain in effect until deletion of all Client Data by Vendor as described in this Agreement.

3. PERSONNEL

3.1. Vendor shall take all such steps as are necessary to ensure the reliability of Personnel who have access to Client Data.

3.2. Vendor shall ensure that access to the Client Data is limited to (a) Personnel who need access for the purpose of exercising Vendor's rights or performing Vendor's obligations under any Agreement between the Vendor and Client; and (b) any Personnel who need to access the specific part of Client Data strictly necessary for performance of such Personnel's duties.

3.3. Vendor shall ensure that Personnel with access to Client Data (a) do not process Client Data except in accordance with this Agreement; (b) are informed of and maintain the confidential nature of the Client Data and are subject to a duty of confidentiality with respect to such data and (c) are aware of Vendor's duties and obligations under the Data Protection Laws and this Agreement.

4. **SUB-PROCESSORS**

4.1. Client agrees that where necessary to perform the Services, Vendor may engage a "sub-processor," as that or a similar term may be defined under applicable Data Protection Laws, to process the Client Data from a list of sub-processors approved by Client.

4.2. Vendor shall provide Client with reasonable prior notice and in any event no less than thirty (30) calendar days if it intends to make any changes to its subprocessors. Client may object in writing to Vendor's appointment of a new sub-processor, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties will discuss their concerns in good faith with a view to achieving resolution. If a resolution does not occur, either party may suspend or terminate the Underlying Agreement.

4.3. Vendor shall ensure that each of its sub-processors are bound by written contractual obligations with respect to the Client Data which are the same as, or no lesser than, those contained in this Agreement, including with respect to limitations on use of Client Data and in compliance with the requirements of applicable Data Protection Laws.

5. DATA SUBJECT AND CONSUMER RIGHTS

5.1. To the extent that Client, in its use of the Services, does not have the ability to fulfil data subject requests required by applicable Data Protection Laws without assistance from Vendor, such as requests to report the content of, correct, amend, block, delete or limit the use of Client Data, Vendor shall, and shall ensure that its sub-processors shall, promptly comply with a request from Client to facilitate such actions at Client's sole expense. If Vendor receives any such requests regarding Personal Data that is Client Data, Vendor shall forward the request to Client within five (5) business days.

5.2. If Vendor processes Client Data that is considered "sensitive" Personal Data under applicable Data Protection Laws, Vendor shall provide assistance to Client, upon reasonable request, to limit the use of such "sensitive" Personal Data.

5.3. If Vendor receives any complaint, notice or communication which relates directly or indirectly to the Processing of Client Data, it shall immediately, and in any event within 5 calendar days, notify Client and shall provide full cooperation and assistance to enable Client to address the request.

6. SECURITY

6.1. Vendor shall implement appropriate technical and organisational measures which are at least as protective as those required of Client under the Data Protection Laws, and appropriate to the risk of unauthorised, accidental or unlawful Processing, access, loss, disclosure or destruction of Client Data (a "**Security Breach**").

6.2. Vendor shall promptly and in any event within 48 hours inform Client in writing of any actual or suspected Security Breach and any breach of or inability to comply with, its security obligations contained in Section 6.

6.3. To the extent that a Security Breach is caused, or is otherwise suffered, by Vendor or its sub-processor(s), Vendor shall, at its expense, investigate, identify and remediate the Security Breach as soon as possible, and within five (5) business days.

6.4. Vendor shall provide full cooperation and assistance and all information as may be reasonably requested by Client in relation to the Security Breach.

6.5. Vendor shall consult with Client in advance regarding any public statements to be made relating to the Security Breach which directly references Client. Unless required to do so by law, Vendor shall not make any public statement relating to the Security Breach which directly references Client without the prior written consent of Client.

6.6. In the event of a Security Breach, Client may, upon notice to Vendor, take reasonable and appropriate steps to remediate any unauthorized use of Client Data by Vendor or its subprocessors.

7. RECORDS

7.1. Vendor shall maintain a record of the Processing activities carried out on behalf of Client which shall, at a minimum, contain the following information:

7.1.1. a description of the Client Data processed by Vendor, including the types of Personal Data, the categories of data subjects and the Processing activities carried out on behalf of Client;

7.1.2. details of any transfers of Client Data to a third country and the legal basis for the legitimate transfer of the same under the Data Protection Laws;

7.1.3. a general description of the technical and organisation security measures used to protect Client Data in accordance with Section 6.1; and

7.1.4. the name and contact details of the Vendor's data protection officer, Chief Privacy Officer or similarly qualified Vendor Personnel.

7.2. Vendor shall promptly provide such records on request from Client.

8. TRANSFERS

8.1. If Client Data in the European Economic Area ("**EEA**"), Switzerland or the UK is transferred to, stored in, or otherwise processed in any country or territory outside the EEA, Switzerland or the UK the following shall apply to those instances of Client Data transfer only:

8.1.1. the Standard Contractual Clauses (2021/914) as available at http://data.europa.eu/eli/dec_impl/2021/914/oj (the "**New SCCs**") are incorporated into and form part of this Agreement subject to the following: the optional language at Clause 11(a) of the New SCCs shall not apply and the following of the New SCCs shall apply: Clause 7; Module Two: Transfer controller to processor; Clause 9(a) Option 2: General Written Authorisation and "*[Specify time period]*" shall be replaced with "thirty (30) calendar days"; Clause 17 Option 1; Clause 17 and Clause 18 shall reference the EU member state Ireland;

8.1.2. the information in Exhibit 1 of this Agreement shall be used as Annex I and II (and III if necessary) of the New SCCs and the findings of the Transfer Impact Assessment set out in Exhibit 2 of this Agreement shall be adopted;

8.1.3. for transfers of Client Data originating from Switzerland: (i) references in the New SCCs to a "Member State" shall not be read to prevent data subjects from Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e. Switzerland); (ii) until the revised Swiss Federal Act of 19 June 1992 on Data Protection ("**FADP**") enters into force the New SCCs shall also protect the data of legal entities in Switzerland; and

8.1.4. for transfers of Client Data originating from the UK the Addendum issued by the Information Commissioner's Office under s119A(1) of the UK's Data Protection Act 2018 ("**UK Addendum**") is appended to the New SCCs subject to the following (i) the New SCCs are considered amended as set out in the UK Addendum (ii) "Exporter" is selected for the purpose of Section 19 and Table 4 of the UK Addendum; and (iii) the parties recognise that the information required to populate the Tables of the UK Addendum is provided for in this Agreement including the Exhibits and that by entering into this Agreement and the New SCCs as provided for in this Section 8.1 then they have also entered into the UK Addendum and agree to be bound by its terms.

1.1. Vendor shall ensure sub-processors involved in Processing Personal Data are subject to the relevant commitments regarding access by public authorities as set out in Clause 15 of the New SCCs. Vendor warrants that it has assessed the laws and practices of any third country where Processing of Client Data occurs (including via sub-processors), including measures authorising access by a public authority or any requirements to disclose Personal Data, and that the outcome of the assessment does not prevent the Vendor (or it's sub-processors) from fulfilling its obligations under this Agreement and as set out in the New SCCs and UK Addendum as applicable. Vendor shall provide such results of the assessment to Client.

1.2. If either the New SCCs, UK Addendum or other legal instrument in relation to international transfers of personal data from the EEA, UK or Switzerland is invalidated, amended or replaced then the parties agree to work together in good faith to resolve any resulting non-compliance issue and enter into such other form of contract as necessary to ensure that processing of Client Data remains compliant with applicable Data Protection Laws and the parties will execute documentation to effectuate the legality of such.

1.3. Except as set out in Section 8.1, if any term or provision of the Agreement or Underlying Agreement is contradictory or inconsistent with any term or provision of the New SCCs or UK Addendum as applicable to such Client Data, then the terms and provisions of the applicable New SCCs or UK Addendum available shall control.

9. CERTIFICATIONS

9.1. Vendor shall notify Client of any third-party certification, seal or other mark obtained by Vendor demonstrating the compliance of its Services with the Data Protection Laws.

10. VENDOR ASSISTANCE

1. Vendor shall provide full cooperation and assistance to Client relating to: (a) an assessment by Client of the impact of the Services on the protection of Personal Data; (b) where necessary, meeting its obligations to comply with applicable Data Protection Laws; and (c) where necessary, a consultation with a supervisory authority prior to any Processing activity.

11. AUDITS

11.1. Vendor shall allow Client and any auditors of or other advisers to Client to access (on reasonable notice) any Vendor premises and Personnel as may be reasonably required in order to undertake verifications of compliance with the provisions of this Agreement and the Data Protection Laws (an "**Audit**"). Any Audit performed pursuant to this Section 11 may be limited in scope by Vendor to the extent necessary to prevent the violation of its reasonable confidentiality obligations related to the information of Vendor's other clients. Where an Audit requires access to Vendor's systems, networks, or premise, it may be supervised by and performed in the presence of Vendor's appropriate security Personnel and performed in accordance with Vendor's security policy and procedures. The results of an Audit will be shared with Vendor, upon Vendor's written request, and any information collected or documentation prepared as a result of an Audit shall be deemed the confidential information of both Vendor and Client.

11.2. Vendor shall provide Client (and its auditors and other advisers) with all reasonable cooperation, access and assistance in relation to each audit.

11.3. In the event of a Security Breach, Client may, upon notice to Vendor, take reasonable and appropriate steps to remediate any unauthorized use of Client Data by Vendor or its sub-processors.

1.5. Vendor shall notify Client immediately and, in any event, within 5 days, in writing in the event that Vendor is unable to comply with its security obligations under the Agreement.

12. APPLICABLE LAW; CHANGES

11.4. Vendor shall process the Client Data in compliance with, and shall not cause itself or Client to be in breach of, the Data Protection Laws and will notify Client immediately and, in any event within 5 business days in writing, in the event it can no longer meet its obligations under applicable Data Protection Laws. Where necessary, Vendor shall assist Client in meeting its obligations to comply with applicable Data Protection Laws.

11.5. Any Data Protection Law applicable to Client Data or the Services that is amended or newly enacted will automatically apply to Vendor's provision of Services and the terms of this Agreement shall be interpreted in a manner consistent with the current Data Protection Laws.

12. ENTIRE AGREEMENT

12.1. This Agreement constitutes the entire agreement between the parties regarding its subject matter and supersedes and extinguishes all agreements, promises, assurances, warranties, representations and understandings between them, whether written or oral, relating to its subject matter. In the event of a conflict between one or more terms in this Agreement and anything in any other agreement between the parties, including, but not limited to, any Underlying Agreement, the language in this Agreement shall prevail, unless expressly agreed in writing with specific reference to this Agreement.

1. BREACH LIABILITY

1.1. Any breach of the obligations of this Agreement shall be deemed a breach of the Underlying Agreement that governs the applicable Processing Services and shall be subject to the obligations (including any indemnification obligations), remedies, cure periods, termination rights and limitations of liability contained in the Underlying Agreement.

13. JURISDICTION AND GOVERNING LAW

13.1. This Agreement shall be governed by and interpreted in accordance with the substantive laws of the jurisdiction controlling Underlying Agreement(s) between the parties. Any dispute arising under this Agreement shall be resolved in accordance with the venue and/or dispute resolution provisions of that/those same Underlying Agreement(s). In the event no such provisions exist, this Agreement shall be interpreted in accordance with the law of the State of Delaware and the venue shall be the state or

federal courts in Kent County, Delaware. Vendor expressly consents to exclusive jurisdiction as set forth in this Section 15.1.

1. NOTICE

1.1. All notice to Client under this Agreement (except the Security Breach notice described in Section 4.2, Section 5.3 and Section 6.2) shall be made in accordance with the Underlying Agreement(s) between the parties.

ACCEPTED AND AGREED TO:

Client	**Teleskope, LLC**
By:_____	By: _____
Name:_____	Name:_____
Title:_____	Title: _____
Date:_____	Date: _____

2.

Exhibit 1

ANNEX I

A. LIST OF PARTIES

Data exporter(s): 1:

Name	[TBC]
Address	[TBC]
Contact person's name, position and contact details:	[TBC]
Activities relevant to the data transferred under these Clauses:	[TBC]
Signature and date:	
Role (controller/processor)	Exporter

Data importer(s): 1:

Name	Teleskope LLC
Address	10411 Motor City Drive Suite 500, Bethesda MD 20817
Contact person's name, position and contact details:	Aman Brar, CEO / policy@teleskope.io
Activities relevant to the data transferred under these Clauses:	[TBC]
Signature and date:	
Role (controller/processor)	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:	Data subjects relevant for the performance of the Services as set out in the Underlying Agreement including Employee Profile Data
Categories of personal data transferred:	Personal data for the performance of the Services as set out in the Underlying Agreement including Basic Employee Profile (First name, Last name, Name Suffix, Job Title, Job Department, Job Location, Email, Employee Id, Company Name), Employee Resource Group membership details.

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:	[[TBC – if sensitive data is transferred, provide details and specify all data categories] OR [Not applicable]
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous basis as needed for providing the services.
Nature of the processing:	The performance of the Services pursuant to the Underlying Agreement.
Purpose(s) of the data transfer and further processing:	Data Importer shall process the Personal Data as necessary to perform the Services pursuant to the Underlying Agreement.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	Subject to Clause 2.5 of this Agreement and unless otherwise agreed in writing, Data Importer shall process the Personal Data for the duration of the Underlying Agreement.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	[Sub-processor's shall process Personal Data as necessary to perform the Services pursuant to the Underlying Agreement.] [OR] [Not applicable]

The identities of the sub-processors used in the provision of the Services and the subject matter which they process are listed here:	Teleskope uses the following cloud services providers to store Personal Data and use their compute, network and other infrastructure to process and deliver Teleskope Services. These are secure environments that are controlled by the Teleskope team and are protected by vendors standard Data Processing Agreements: **Entity Name - Purpose - Entity Country** Amazon Web Services, Inc. - Cloud Service Provider - United States Microsoft Corporation (Microsoft Azure) - Cloud Service Provider - United States Google Inc. - Cloud Service Provider | United States Teleskope works with other third-parties to provide specific functions or features within the Teleskope Service. These providers will have access to relevant personal information (both in an identifiable and anonymous manner) in order to provide their relevant functions. The use of information is limited to the specific purposes we've detailed below and are protected by vendors standard Data Processing Agreements: **Entity Name - Purpose - Entity Country** Atlassian, Inc. - Cloud-based Customer Support Services for managing customer support tickets - Australia; data in the US Intuit, Inc (QuickBooks) - Cloud-based Accounting Services for generating invoices - United States

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13:
Ireland - Data Protection Commission, 21 Fitzwilliam Square South, Dublin 2
D02 Rd28, Ireland in parallel with the Swiss Federal Data Protection Information Commissioner insofar as data transfer(s) are governed by the FADP.

ANNEX II -

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Exhibit 2
Transfer Impact Assessment
[please complete all sections as indicated]

Step 1: Nature of Transfer

Data Exporter & country:	
Data Importer:	See DPA Exhibit 1
Country(ies) of Data Importer for the purpose of the transfer:	☐USA
Data Importer Sector :	☐Other. Please specify_ENTERPRISE HR SOFTWARE_____
Professional or other rules which apply in addition to the general legal regime of the destination country e.g. professional secrecy obligations:	☐None. ☐Yes. Please specify_____ If yes, what impact will this have on the transfer? Please specify _____
Transfer Features:	Context and purpose of transfer, duration of processing, categories of data subjects, categories of personal data, technical and organisational measures to protect the security of the data and frequency of the export - see Information Security Agreement between the parties where applicable and DPA Exhibit 1. Special categories of personal data: ☐are transferred. ☐are not transferred.
Format of data to be transferred:	Please select all that apply: ☐Encrypted in transit ☐Encrypted at rest ☐Data is pseudonymised or encrypted ☐Other. Please specify_____ See DPA Exhibit 1 for further detail and Information Security Agreement where applicable.
Transfer Implementation:	Please select all that apply: ☐Data will be stored outside of the EEA, UK and Switzerland ☐Web interface ☐Data Importer API ☐Cloud storage situated outside of the EEA ☐Email ☐Remote online access with the ability to download data ☐Other. Please specify_____
Onward Transfer(s) & Recipient(s):	☐Not applicable - controller to controller relationship.
Starting date of transfer(s) and review period:	The transfer(s) will begin on the effective date of the DPA. This assessment will be reviewed should there be a substantial change to the processing or overarching legal regime or if the Importer can no longer honour its commitments in respect of the personal data being processed.

Transfer Mechanism:	All transfers, including onward transfers if relevant, will be conducted pursuant to standard contractual clauses as set out in the DPA.

Step 2: Country Assessments

An analysis of the laws / regulatory environment and practices applicable to the protection of personal data in the Country(ies) of Data Importer and the Country(ies) of Onward Transfer(s) which are not covered by UK "adequacy regulations" and/or do not have an EC adequacy decision and supplementary measures[1] deemed necessary for the transfer.

Note: If a country is not listed below, please add it. Please remove any inapplicable countries.

USA
Overall Assessment: Whilst there is no federal, overarching data protection law in place, a combination of other laws offers reasonable protection for individual rights, personal data and privacy. Laws relating to access and assistance allow authorities fairly wide discretion to conduct surveillance, subject to certain statutory and Constitutional limitations. The rights granted to US citizens / restrictions in place in relation to surveillance in the US are different to those applicable to people / activity outside the US in certain instances. As a result, data access and surveillance measures may not be limited in the same proportionate and necessary way as in the EU / UK.
Supplementary Measures: The Data Importer will encrypt the data during transfer, the transfer will be subject to the standard contractual clauses and the Data Importer has stated that the history and likelihood of governmental access is limited / low. Therefore, additional supplementary measures are considered to be unnecessary however, the Data Importer will also employ the technical and organisational measures set out in DPA Exhibit 1 and in the Information Security Agreement where applicable.
Further Comment (optional):

Step 3: Assessment Conclusion

☐ **Not permitted:** Based upon our assessment of the data protection and privacy laws and practices in the country(ies) where data is being transferred, together with the nature of the transfer(s), our conclusion is that the transfer(s) would not be subject to adequate safeguards and are therefore not permitted.

☐ **Permitted:** Based upon our assessment of the data protection and privacy laws and practices in the country(ies) where data is being transferred, together with the nature of the transfer(s), our conclusion is that the transfer(s) would be subject to adequate safeguards. In summary, this is on the following basis:

- the format of the data to be transferred;
- considering the technical and organisational measures that will be put in place to protect the data as set out in DPA Exhibit 1, the Information Security Agreement where applicable and that supplementary measures as set out in Step 2 will be adopted;
- the transfer(s) will be subject to the standard contractual clause as set out in the DPA such that data subject will have contractual redress against the Data Importer for any breach of their rights under the GDPR (or UK GDPR as applicable), and, the New SCCs contractually oblige the Data Importer/Recipient to defend the personal data against unlawful access attempts; and
- the history & likelihood of governmental access as disclosed by the Data Importer.

[1] Supplementary measures must be adopted where necessary to ensure that the personal data transferred out of the UK, Switzerland or EEA has an essential equivalent level of protection as it would benefit from within those geographies. Supplementary measures may be contractual, technical or organisational – a combination is likely required. The adoption of supplementary measures will have to be considered on a case-by-case basis including consideration of whether any proposed supplementary measures are lawful in the relevant importing country. For example, the use of certain encryption technology or informing the data exporter about orders to disclose or grant access to personal data may be unlawful in the relevant importing country. The EDPB sets out potential supplementary measures and further details regarding their implementation in Annex 2 of its recommendations.

Final Note: Adoption and Preparation of this TIA

This TIA is to be adopted by both the Data Exporter and Data Importer as set out in the standard contractual clauses and the DPA.

This TIA has been prepared collaboratively between the Data Importer and Data Exporter in respect of Clause 14 of the New SCCs which requires both parties to carry out a transfer impact assessment and "warrant" that they have "no reason to believe" that the laws and practices applicable to the Data Importer, including any requirements around disclosure to, or access by, public authorities, prevent the Data Importer from complying with the New SCCs.