

**CLARI, INC.**

**DATA PROCESSING ADDENDUM**

This Clari, Inc. Data Processing Addendum and its Annexes (“DPA”) forms part of the Master Subscription Agreement (the “Agreement”) between Clari, Inc. (“Clari” or “Processor”) and the party identified as “Customer” in the Agreement (“Customer” or “Controller”) and reflects the parties’ agreement with respect to the Processing of Personal Data by Clari on behalf of Customer in connection with the Services under the Agreement. In case of any conflict or inconsistency with the terms of the Agreement, the terms of this DPA will supersede and control. Any terms not defined in this DPA will have the meaning as set forth in the Agreement.

**1. Definitions**

“California Personal Information” means Personal Data that is subject to the protection of the CCPA.

“CCPA” means California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2018).

“Consumer”, “Business”, “Sell” and “Service Provider” will have the meanings given to them in the CCPA.

“Controller”, “Data Subject”, “Personal Data”, “Personal Data Breach”, “Processor”, and “Processing” will have the meanings given to them in the GDPR as it relates to Personal Data Processed by Clari and/or its Sub-Processors in connection with the provision of the Services.

“Data Protection Laws” means all applicable worldwide legislation relating to data protection and privacy which applies to the respective party in the role of Processing Personal Data under the Agreement, including European Data Protection Laws and the CCPA.

“European Data Protection Laws” means data protection laws applicable in Europe, including: (i) the General Data Protection Regulation (Regulation (EU) 2016/679) (“GDPR”) and all other laws relating to data protection and/or electronic communications in the EU or EEA; (ii) all laws relating to data protection and/or electronic communications in the UK, including the UK GDPR as it forms part of the law of the UK by virtue of section 3 of the European Union (Withdrawal) Act 2018 (“UK GDPR”), the Data Protection Act 2018 (c. 12) and any other law relating to data protection as a consequence of the UK leaving the EU (“UK Data Protection Laws”); and (iii) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance.

“Instructions” means a direction, either in writing or in electronic form (e.g. by e-mail or software), issued by Controller to Processor and directing Processor to Process Personal Data.

“Standard Contractual Clauses” (or “Clauses”) means the (i) the agreement executed by and between Controller and Processor and set out in Annex 4 pursuant to the European Commission’s decision (EU) 2021/914 of 4 June 2021 and (ii) the agreement and Addendum executed by and between Controller and Processor and set out in Annex 4 and Annex 5, respectively, pursuant to the UK Information Commissioner’s Office’s preliminary adoption of (EU)

2021/914 (“UK Standard Contractual Clauses”), as context requires; as may be amended, superseded or replaced. “Clause” means a specific clause within the Standard Contractual Clauses.

“Sub-Processor” means any Processor under the European Data Protection Laws or Service Provider under the CCPA, as applicable, engaged by Clari to assist in fulfilling its obligations with respect to the provision of the Services under the Agreement.

## **2. Customer Responsibilities**

a. Compliance with Laws. Customer will be responsible for complying with all requirements that apply to Customer under applicable Data Protection Laws with respect to its Processing of Personal Data and the Instructions Customer issues to Clari under the Agreement. Customer will be solely responsible for: (i) the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data; (ii) ensuring that Customer Instructions to Clari and Sub-Processors, as appropriate, regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws. Customer will inform Clari without undue delay if Customer is not able to comply with its responsibilities under this sub-section (a) or applicable Data Protection Laws. Customer shall not provide or make available to Clari any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Services and will indemnify Clari from all claims and losses in connection therewith.

b. Customer Instructions. The parties agree that the Agreement, together with Customer use of the Service in accordance with the Agreement, constitute Customer’s Instructions to Clari in relation to the Processing of Personal Data. The subject matter, nature, purpose, and duration of this Processing, as well as the types of Personal Data collected and categories of Data Subjects, are described in Annex 1 to this DPA.

## **3. Clari Obligations**

a. Compliance with Instructions. Clari will Process Personal Data only (i) for the purposes described in the Agreement, (ii) in accordance with the terms under this DPA and any other Instructions provided by Customer, and (iii) in compliance with Data Protection Laws, unless otherwise required by applicable law.

b. Security. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Clari will implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of Processing Personal Data, as described under Annex 2 to this DPA.

c. Confidentiality. Clari will take commercially reasonable steps to (i) ensure the reliability and appropriate training of any personnel whom Clari authorizes to Process Personal Data on Clari’s behalf (“Authorized Personnel”); (ii) ensure that Authorized Personnel are subject to a confidentiality agreement that prevents the processing of Personal Data, both during and after their engagement by Clari, except in accordance with their obligations in connection with the Services; and (iii) limit access to Personal Data only to Authorized Personnel. Clari will be liable for any acts or omissions in violation of this DPA by Clari’s Authorized Personnel.

d. Personal Data Breaches. Clari will notify Customer without undue delay, and in accordance with all Data Protection Laws, after Clari becomes aware of any Personal Data Breach and take such steps as Clari in its sole discretion deems necessary and reasonable to remediate such Personal Data Breach. Any such data breach notification shall include all the information as required by Data Protection Laws.

e. Deletion or Return of Personal Data. Within ninety (90) days from completion of the Services, at Customer's choice, Clari will return or delete the Personal Data, except as required to be retained by applicable laws. After such period, Clari may delete all such data (except as otherwise required to be retained by applicable laws).

#### **4. Data Subject Requests**

a. Taking into account the nature of the Services, Clari offers Customer controls that Customer can use to comply with its obligations towards responding to requests from Data Subjects under Data Protection Laws ("Data Subject Requests"). Where a Data Subject Request is made directly to Clari, Clari will either advise the Data Subject to submit their request to Customer or forward that Data Subject Request to Customer. Customer will be responsible for responding to such Data Subject Request.

b. To the extent that Customer is unable to independently address a Data Subject Request through the Services, then upon Customer's written request Clari will provide reasonable assistance to Customer to respond to any Data Subject Requests relating to the Processing of Personal Data under the Agreement. Customer will be responsible to the extent legally permitted for any costs and expenses arising from this assistance by Clari and its Sub-Processors.

#### **5. Sub-Processors**

a. Clari engages the Sub-Processors listed in Annex 3 of this DPA (the "List") to Process Personal Data on Customer's behalf in connection with the Services. The Sub-Processors set on the List as of the Effective Date are approved by Customer. If Clari intends to add a new Sub-Processor to the List after the Effective Date, it will provide written notice Customer of such intention (via email). Customer will have thirty (30) days from such notice to object to the newly proposed Sub-Processor. Objection must be based on reasonable grounds. If no objection is provided within such period, the Sub-Processor is deemed approved by Customer. If Customer provides an objection within such period, the parties will, for a period of ten (10) days after such objection, discuss the issue diligently and in good faith. If they cannot agree on a workaround or alternative within such period, Customer's sole remedy is to terminate the Agreement on written notice to Clari and receive a pro rata refund of all pre-paid, unearned fees after the effective date of such termination.

b. Clari will ensure that it imposes data protection terms on the Sub-Processors that provide at least the same or an equivalent level of protection for Personal Data as those set out in this DPA. Clari will remain responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor to the same extent that Clari would itself be liable under this DPA had it conducted such acts or omissions.

c. If Customer has entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the above authorizations will constitute Customer's prior written consent to the sub-Processing by Clari of the Processing of Personal Data.

**6. Transfers of Personal Data**

a. Any transfer of Personal Data made subject to this DPA from Europe to the United States will be undertaken by Clari using the Standard Contractual Clauses set forth in Annex 4 of this DPA.

**7. Demonstration of Compliance; Audits**

a. Clari will maintain records sufficient to demonstrate its compliance with its obligations under this DPA and retain such records for a period of three (3) years after the termination of the Agreement (“Documentation”). Clari also uses external auditors to verify the adequacy of its security measures. This audit (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards or substantially equivalent standards; (c) will be performed by independent third party security professionals at Clari’s selection and expense; and (d) will result in the generation of a confidential audit report (“Audit Report”). Upon Customer’s request, no more than once per year, Clari will provide (on a confidential basis) Customer with a summary of the Documentation and Audit Reports so that Customer can verify Clari’s compliance with this DPA.

b. To the extent Customer’s audit requirements under the Standard Contractual Clauses or Data Protection Laws cannot reasonably be satisfied through Section 7(a) above, Customer may audit Clari’s systems and facilities to verify compliance with this DPA. Customer agrees to exercise any such right only through use of an independent, accredited third-party audit firm that is acceptable to Clari. The audit will occur during Clari’s regular business hours. The auditor’s may be required to execute reasonable confidentiality obligations with Clari. Before the commencement of the audit, Customer and Clari will mutually agree upon the scope, timing, duration, control and evidence requirements, and fees for the audit, provided that this requirement to agree will not permit Clari to unreasonably delay performance of the audit. To the extent needed to perform the audit, Clari will make the processing systems, facilities and supporting documentation relevant to the Processing of Personal Data by Clari and its Sub-Processors available. Customer will be responsible for the costs and fees of any such audits or inspections. If the audit report generated as a result of Customer’s audit includes any finding of material non-compliance with this DPA or applicable law, Customer will share such audit report with Clari and, after Clari’s verification of the issue, Clari will promptly cure the non-compliance.

**8. Additional Provisions for European Data**

a. Data Protection Impact Assessments and Consultation with Supervisory Authorities. To the extent required by European Data Protection Laws, Clari will provide reasonable assistance to Customer with any data protection impact assessments and prior consultations with supervisory authorities.

**9. Additional Provisions for California Personal Information**

a. Roles and Responsibilities. When Processing California Personal Information in accordance with Customer’s Instructions, the parties acknowledge and agree that Customer is a Business and Clari is a Service Provider for the purposes of the CCPA. The Parties agree that Clari will not (i) retain, use or disclose or otherwise process California Personal Information as a Service Provider for any other purpose, including a commercial purpose, other than to perform the Services under the Agreement or as otherwise permitted by the CCPA; (ii) sell California Personal

Information; or (iii) retain, use or disclose California Personal Information outside of the direct business relationship with Customer. The parties certify that they understand and will comply with the CCPA and restrictions contained herein.

**10. General Provisions**

- a. Limitation of Liability. The limitations on liability in the Agreement apply to any breach of this DPA.
- b. Governing Law. This DPA will be governed in accordance with the choice of jurisdiction stipulated in the Agreement, unless required otherwise by Data Protection Laws.

**ANNEX 1 – Details of Processing**

This Annex forms part of the DPA and Clauses and must be completed and signed by the parties.

**A. LIST OF PARTIES**

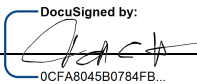
**Data exporter(s):** *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: Todd Hogan

Address: Alton House, 66 High Street, Northwood, Middlesex HA6 1BL

Contact person’s name, position and contact details: CRO, [todd.hogan@ziflow.com](mailto:todd.hogan@ziflow.com)

Activities relevant to the data transferred under these Clauses: \_\_\_\_\_

Signature and date:  7/29/2022

Role (controller/processor): Controller


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

Name: Jay Wedge

Address: 1154 Sonora Ct. Sunnyvale, CA 94086

Contact person’s name, position and contact details: Jay Wedge, Head of Legal, [jwedge@clari.com](mailto:jwedge@clari.com)

Activities relevant to the data transferred under these Clauses: \_\_\_\_\_

Signature and date:  7/29/2022

Role (controller/processor): Processor

**B. DESCRIPTION OF TRANSFER**

***Categories of data subjects whose personal data is transferred***

Customer may submit Personal Data in the course of using the Service, the extent of which is determined and controlled by Customer in Customer’s sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

Individuals including Customer’s end users, employees, agents, contractors, collaborators, prospects, suppliers and subcontractors.

***Categories of personal data transferred***

Customer may submit Personal Data to the Service, the extent of which is determined and controlled by Customer in Customer's sole discretion, and which may include but is not limited to the following categories of Personal Data:

- First and last name
- Business email address
- Business title
- Employer
- Business phone number
- Physical business address
- IP address of devices used to access the Service
- Any other Personal Data submitted by, sent to, or received by Customer, or Customer's end users, via the Service.

***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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.***

The parties do not anticipate the transfer of special categories of data.

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

Personal Data will be Processed on a continuous basis.

***Nature of the processing***

Personal Data will be Processed in accordance with the Agreement (including this DPA) and may be subject to the following Processing activities:

- a. Storage and other Processing necessary to provide, maintain and improve the Services provided to Customer; and/or
- b. Disclosure in accordance with the Agreement (including this DPA) and/or as compelled by applicable laws.

***Purpose(s) of the data transfer and further processing***

Clari will Process Personal Data as necessary to provide the Services pursuant to the Agreement, as further specified in the Order Agreement, and as further instructed by Customer in Customer's use of the Services.

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

Subject to the 'Deletion or Return of Personal Data' section of the DPA, Clari will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

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

---

**C. COMPETENT SUPERVISORY AUTHORITY**

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

---



## **ANNEX 2 – Security Measures**

This Annex forms part of the DPA and Clauses.

Description of the technical and organizational security measures implemented by the Clari in accordance with Clause 8 (or document/legislation attached):

### **1. SECURITY**

a. Controls for the Protection of Personal Data. Clari shall maintain administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Personal Data as set forth in Clari's 'Security, Privacy and Architecture Documentation' (available on request). Clari regularly monitors compliance with these safeguards. Clari will not materially decrease the overall such security of the Services during a subscription term.

b. Third-Party Certifications and Audits. Clari has obtained the third-party certifications and audits set forth in its Security, Privacy and Architecture Documentation. These include certifications by ISO 27001-2013, SOC 2 type II, and other applicable certifications as deemed appropriate by the Clari. Upon Customer's written request at reasonable intervals, Clari shall make available to Customer a copy of Clari's then most recent, relevant third-party audits or certifications, as applicable, or summaries thereof, that Clari generally makes available to its customers at the time of such request.

### **2. SECURITY BREACH MANAGEMENT AND NOTIFICATION**

Clari maintains security incident management policies and procedures specified in its Security, Privacy and Architecture Documentation and shall, to the extent permitted by law, promptly notify Customer of any unauthorized disclosure of Personal Data by Clari or its Sub-Processors of which Clari becomes aware (a "Security Breach"). To the extent such Security Breach is caused by a violation of the requirements of this Appendix by Clari, Clari shall make reasonable efforts to identify and remediate the cause of such Security Breach. Clari shall specify via its standard 'Service Level Agreement' document specifics on service uptime, breach notification and remediation consistent with the generally accepted industry guidelines for similar services.

**ANNEX 3 – List of Sub-Processors**

Customer acknowledges and agrees that the third parties listed at the web page URL: [www.clari.com/gdpr](http://www.clari.com/gdpr) shall be deemed Sub-Processors that may Process Personal Data pursuant to this DPA. If new Sub-Processors are added, Clari will notify the Customer, and get Customer consent, as set forth in the DPA.

## ANNEX 4 – Standard Contractual Clauses

### STANDARD CONTRACTUAL CLAUSES

#### SECTION I

##### *Clause 1*

##### **Purpose and scope**

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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) for the transfer of personal data to a third country.
- (b) The Parties:
  - (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter ‘entity/ies’) transferring the personal data, as listed in Annex 1.A (hereinafter each ‘data exporter’), and
  - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex 1.A (hereinafter each ‘data importer’)have agreed to these standard contractual clauses (hereinafter: ‘Clauses’).
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex 1.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

##### *Clause 2*

##### **Effect and invariability of the Clauses**

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 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, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

##### *Clause 3*

##### **Third-party beneficiaries**

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

- (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - (ii) Clause 8 – Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e);
  - (iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e);
  - (iv) Clause 12 – Modules Two: Clause 12(a), (d) and (f);
  - (v) Clause 13;
  - (vi) Clause 15.1(c), (d) and (e);
  - (vii) Clause 16(e);
  - (viii) Clause 18 – Modules Two: Clause 18(a) and (b).
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

*Clause 4*

**Interpretation**

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

*Clause 5*

**Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

*Clause 6*

**Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex 1.B.

*Clause 7 – Optional*

**Docking clause**

- (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex 1.A.
- (b) Once it has completed the Appendix and signed Annex 1.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex 1.A.

- (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

## SECTION II – OBLIGATIONS OF THE PARTIES

### *Clause 8*

#### **Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

#### **8.1 Instructions**

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

#### **8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex 1.B, unless on further instructions from the data exporter.

#### **8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex 2 and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

#### **8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

#### **8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex 1.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

## 8.6 Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex 2. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

## 8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex 1.B.

## 8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

## **8.9 Documentation and compliance**

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

### *Clause 9*

#### **Use of sub-processors**

- (a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [30 days] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

*Clause 10*

**Data subject rights**

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex 2 the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

*Clause 11*

**Redress**

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.



- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

*Clause 12*

**Liability**

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

*Clause 13*

**Supervision**

- (a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex 1.C, shall act as competent supervisory authority.
- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS  
IN CASE OF ACCESS BY PUBLIC AUTHORITIES

*Clause 14*

**Local laws and practices affecting compliance with the Clauses**

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
  - (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
  - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

*Clause 15*

**Obligations of the data importer in case of access by public authorities**

**15.1 Notification**

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
  - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

**15.2 Review of legality and data minimisation**

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

#### SECTION IV – FINAL PROVISIONS

##### *Clause 16*

##### **Non-compliance with the Clauses and termination**

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
  - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  - (ii) the data importer is in substantial or persistent breach of these Clauses; or
  - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

##### *Clause 17*

##### **Governing law**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

##### *Clause 18*

**Choice of forum and jurisdiction**

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of Ireland.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

**Where applicable, by signing we agree to be bound by the UK Addendum to the EU Commission Standard Contractual Clauses.**

**On behalf of the data exporter:**

Name (written out in full): Todd Hogan

Position: Chief Revenue Officer

Address: Alton House, 66 High Street, Northwood, Middlesex HA6 1BL

Other information necessary in order for the contract to be binding (if any):

Signature:  OCFA8045B0784FB...

**On behalf of the data importer:**

Name (written out in full):

Jay Wedge


Position:

Head of Legal

Address:

1154 Sonora Ct., Sunnyvale, CA 94086

Other information necessary in order for the contract to be binding (if any):

Signature:  5580E83DFBF1435...



## ANNEX 5 – UK ADDENDUM

### UK Addendum to the EU Commission Standard Contractual Clauses

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**

<b>Start date</b>	8/1/2022	
<b>The Parties</b>	<b>Exporter (who sends the Restricted Transfer)</b>	<b>Importer (who receives the Restricted Transfer)</b>
<b>Parties' details</b>	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: Clari Inc. Trading name (if different): Main address (if a company registered address): 1154 Sonora Court, Sunnyvale, CA 94086 Official registration number (if any) (company number or similar identifier):
<b>Key Contact</b>	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Jay Wedge Job Title: Head of Legal Contact details including email: jwedge@clari.com

**Table 2: Selected SCCs, Modules and Selected Clauses**

The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:

Date: June 4, 2021

Reference: 2021/914

**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

Annex 1B: Description of Transfer

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data

Annex III: List of Sub processors

**Table 4: Ending this Addendum when the Approved Addendum Changes**

Which Parties may end this Addendum as set out in Section 19:

- Importer
- Exporter
- neither Party

**Part 2: Mandatory Clauses****Entering into this Addendum**

- 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.
- 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**

- 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 Information	As set out in Table 3.



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:**

Part 2: Mandatory Clauses of the Approved Addendum, 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.