DATA PROCESSING ADDENDUM – GDPR

1. DEFINITIONS AND INTERPRETATION

1.1 In this Addendum, the following terms shall have the meanings set out in this clause 1.1, unless expressly stated otherwise:

"**Addendum**" means this data processing addendum;

"**Adequate Country**" means a country or territory outside the EU/EEA that is recognized for the purposes of the Data Protection Laws (including by virtue of a decision of the European Commission) as providing an adequate level of protection for Personal Data;

"**Agreement**" means the Subscription Agreement to which this Addendum is attached;

"**Customer Personal Data**" means any Personal Data Processed by TRIBLIO on behalf of Customer pursuant to or in connection with the Agreement;

"**Data Protection Laws**" means, until 24 May 2018, EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and, with effect from 25 May 2018, the GDPR;

"**Data Subject Request**" means the exercise of rights by Data Subjects of Customer Personal Data under Chapter III of the GDPR;

"**Triblio Services**" means the Subscription services provided pursuant to the Agreement;

"**GDPR**" means the EU General Data Protection Regulation 2016/679 and to the extent the GDPR is no longer applicable in the United Kingdom, any implementing legislation or legislation having equivalent effect in the United Kingdom;

"**Personnel**" means employee, agent, consultant or contractor;

"**Third Country**" means a country or territory outside the EU/EEA that is not an Adequate Country;

"**Transfer**" means a transfer of Customer Personal Data to a Third Country that falls within the scope of Chapter V of the GDPR (including, where applicable, any 'onwards transfers' from that Third Country);

"**Sub-processor**" means any third party appointed by or on behalf of TRIBLIO to Process Customer Personal Data; and

1.2 In this Addendum:

(a) the terms, “**Data Controller**”, “**Data Processor**”, “**Data Subject**”, “**Personal Data**”, “**Personal Data Breach**”, “**Process/Processing/Processed**” and “**Supervisory**

Authority" shall have the meaning ascribed to the corresponding terms in the Data Protection Laws.

(b) unless otherwise defined herein, all capitalized terms shall have the meaning given to them in the Agreement;

(c) references to this Addendum include its Schedules;

(d) references to clauses and/or Schedules are to clauses of, and Schedules to, this Addendum;

(e) references to "laws" shall mean (a) any statute, regulation, by-law, or subordinate legislation; (b) the common law and the law of equity; (c) any binding court order, judgment or decree; or (d) any industry code, policy or standard enforceable by law; and

(f) any English legal term for any legal document, action, remedy, judicial proceeding, court, official, status, doctrine or any other legal concept shall, in relation to any jurisdiction other than England and Wales, be deemed to include the term which most nearly approximates in that jurisdiction to the English legal term.

1.3 This Addendum shall be incorporated into and form part of the Agreement and is subject to the limitations set forth therein. In the event of any conflict or inconsistency between this Addendum and the main body of the Agreement, this Addendum shall prevail.

2. PROCESSING OF CUSTOMER PERSONAL DATA

2.1 TRIBLIO shall:

(a) comply with all applicable Data Protection Laws in Processing Customer Personal Data; and

(b) not Process Customer Personal Data other than (i) on Customer's instructions (subject always to clause 2.7) and (ii) as required by applicable laws.

2.2 To the extent permitted by applicable laws, TRIBLIO shall inform Customer of:

(a) any Processing to be carried out under clause 2.1(b)(ii); and

(b) the relevant legal requirements that require it to carry out such Processing,

before the relevant Processing of that Customer Personal Data by TRIBLIO.

2.3 Customer instructs TRIBLIO to Process Customer Personal Data as necessary (i) to provide the TRIBLIO Services to Customer (including, without limitation, to improve and update the TRIBLIO Services and to carry out Processing initiated by Users (as defined in the Agreement) in their use of the TRIBLIO Services) and (ii) to perform TRIBLIO's obligations and exercise TRIBLIO's rights under the Agreement.

2.4 Schedule 1 to this Addendum sets out certain information regarding TRIBLIO's Processing of Customer Personal Data as required by Article 28(3) of the GDPR.

2.5 Customer may amend Schedule 1 on written notice to TRIBLIO from time to time as Customer reasonably considers necessary to meet any applicable requirements of Data Protection Laws. Nothing in Schedule 1 (including as amended pursuant to this clause 2.5) confers any right or imposes any obligation on any party to this Addendum.

2.6 Where TRIBLIO receives an instruction from Customer that, in its reasonable opinion, infringes or violates the GDPR, TRIBLIO shall inform Customer.

2.7 Customer acknowledges and agrees that any instructions issued by Customer with regards to the Processing by TRIBLIO of Customer Personal Data pursuant to or in connection with the Agreement shall (i) be strictly required for the sole purpose of ensuring compliance with Data Protection Laws, and (ii) not relate to the scope of, or otherwise materially change the TRIBLIO Services. Notwithstanding anything to the contrary herein, TRIBLIO may terminate the Agreement in its entirety upon written notice to Customer with immediate effect if TRIBLIO considers (in its absolute discretion) that (a) it is unable to adhere to, perform or implement any instructions issued by Customer due to the technical limitations of its systems, equipment and/or facilities, and/or (b) to adhere to, perform or implement any such instructions would require disproportionate effort (whether in terms of time, cost, available technology, manpower or otherwise).

2.8 Customer represents and warrants on an ongoing basis that, (i) for the purposes of Article 6 of the GDPR, there is, and will be throughout the term of the Agreement, a legal basis for the Processing by TRIBLIO of Customer Personal Data in accordance with this Addendum and the Agreement (including, without limitation, any and all instructions issued by Customer from time to time in respect of such Processing); and (ii) it shall not provide or otherwise make available to TRIBLIO any special categories of Personal Data (as the term ‘special categories’ is defined in Article 9(1) of the GDPR) or any Personal Data relating to criminal convictions and/or offences (as those terms are defined in Article 10 of the GDPR).

3. TRIBLIO PERSONNEL

3.1 TRIBLIO shall take reasonable steps to ensure the reliability of any Personnel who may Process Customer Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know or access the relevant Customer Personal Data for the purposes described in this Addendum, and to comply with applicable laws, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. SECURITY

4.1 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, TRIBLIO shall in relation to the Customer Personal Data implement appropriate technical and organizational measures, as described in further detail in the Security Schedule, to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, TRIBLIO shall take into account the risks presented by Processing, in particular from a Personal Data Breach.

5. SUBPROCESSING

5.1 Customer authorizes TRIBLIO to appoint sub-processors in accordance with this clause 5 provided that TRIBLIO provides written notice of such sub-processors to Customer and ensures that all such sub-processors comply with the requirements of this Addendum. TRIBLIO will comply with the conditions referred to Article 28 of GDPR for engaging sub-processors and will inform the Customer of any intended changes (taking place after conclusion of the Agreement) concerning the sub-processors giving the Customer opportunity to object to such changes. Customer acknowledges that such objection may limit the Customer’s possibilities to use services provided by TRIBLIO.

5.2 TRIBLIO is responsible that its sub-processors Process the Personal Data in accordance with this Addendum. TRIBLIO must especially ensure that each sub-processor implements all the appropriate technical and organizational measures compliant with the Controls so that the Personal Data are Processed in accordance with this Addendum and the Data Protection Legislation.

5.3 TRIBLIO will, at Customer's written request, provide Customer with a written confirmation on how TRIBLIO has ensured that its sub-processors comply with the aforementioned obligations.

6. DATA SUBJECT RIGHTS

6.1 Taking into account the nature of the Processing, TRIBLIO shall, at Customer's cost, provide Customer with such assistance as may be reasonably necessary and technically possible in the circumstances, to assist Customer in fulfilling its obligation to respond to Data Subject Requests.

6.2 TRIBLIO shall:

(a) promptly notify Customer if TRIBLIO receives a Data Subject Request; and

(b) ensure that TRIBLIO does not respond to any Data Subject Request except on the documented instructions of Customer (and in such circumstances, at Customer's cost) or as required by applicable laws, in which case TRIBLIO shall to the extent permitted by applicable laws inform Customer of that legal requirement before TRIBLIO responds to the Data Subject Request.

7. PERSONAL DATA BREACH

7.1 TRIBLIO shall notify Customer without undue delay upon TRIBLIO becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information (insofar as such information is within TRIBLIO's possession) to allow Customer to meet any obligations to report or inform Data Subjects or Supervisory Authorities of the Personal Data Breach under Data Protection Laws.

7.2 TRIBLIO shall co-operate with Customer and take such reasonable commercial steps as may be directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

8.1 TRIBLIO shall provide reasonable assistance to Customer, at Customer's cost, with any data protection impact assessments, and prior consultations with Supervisory Authorities, which Customer reasonably considers to be required of Customer by Article 35 or 36 of the GDPR, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing by, and information available to, TRIBLIO.

9. DELETION AND RETURN OF CUSTOMER PERSONAL DATA

9.1 TRIBLIO will Process Personal Data as long as it is necessary for TRIBLIO in order to provide Services to the Customer under the Agreement. TRIBLIO undertakes, in accordance with Customer's written request and without undue delay, to delete or return the Personal Data to Customer (or to a third party appointed by Customer) in agreed format.

9.2 TRIBLIO will return or delete the Personal Data upon termination of this Addendum, including all existing copies of the Personal Data in its possession, unless TRIBLIO is required to store the said Personal Data under mandatory law or regulation.

9.3 TRIBLIO undertakes not to Process Personal Data after it has been successfully transferred to Customer or a third party appointed by Customer, or after it has been successfully removed.

TRIBLIO may however continue to store and access Personal Data as provided by Section 9.2 above.

10. AUDIT RIGHTS

10.1 TRIBLIO will provide Customer with all information reasonably requested by the Customer to demonstrate TRIBLIO's compliance with the requirements of this Addendum (including implementation of the Controls).

10.2 During the term of this Addendum, Customer or an independent third-party auditor appointed by Customer will have the right to audit TRIBLIO's compliance with the obligations under this Addendum (including any implementation of the Controls).

10.3 The third-party auditor used by the Customer must have the necessary skills and qualifications required to carry out such audit, must be bound by appropriate confidentiality obligations and may not be TRIBLIO's competitor. The report of the auditor must be shared with both Parties.

10.4 Customer must notify TRIBLIO of the audit at least 14 days in advance. TRIBLIO will always allow the regulatory authority supervising Customer's business to conduct audits targeted at Customer's obligations as data controller. The relevant parts of this Section 11 will be applied to such audits.

10.5 The subject of the audit will be TRIBLIO's documentation related to information security and the Processing of Personal Data and other information necessary to evaluate TRIBLIO's compliance with this Addendum. TRIBLIO will participate in and contribute to the audit to the extent necessary. TRIBLIO will also, on Customer's request, participate in a supervisory authority's audit targeted at Customer and provide the supervisory authority with the required information to conduct such audit. Both the Customer and TRIBLIO agree to cooperate, on request, with the supervisory authority in the performance of its tasks.

10.6 Each Party will bear its own costs resulting from the audit and Customer will bear the costs for the use of third-party auditor.

11. TRANSFERS

11.1 TRIBLIO and its sub-processors may transfer personal data outside the EU/EEA area for processing in order to provide services to the Customer. When such transfer takes place, the European Commission Standard Contractual Clauses (2021/914/EU – MODULE TWO: Transfers Controller to Processor) for the Transfer of Personal Data to Processors Established in Third Countries ("Standard Contractual Clauses"), or other appropriate safeguards provided by the GDPR, will apply to such transfer. These Standard Contractual Clauses are incorporated here by reference. The required Options and Annexes are in Exhibit 1 of this DPA.

11.2 TRIBLIO and its sub-processors may transfer personal data outside of the UK for processing in order to provide services to the Customer. When such transfer takes place, TRIBLIO relies on the UK Addendum to the EU Standard Contractual Clauses. These are as laid out in Exhibit 2.

11.3 TRIBLIO will notify Customer upon request of the countries in which Personal Data will be Processed (including the countries from which the Personal Data can be accessed).

12. STATISTICAL DATA

12.1 Customer acknowledges and agrees that (i) TRIBLIO shall be freely able to use and disclose Statistical Data for TRIBLIO's own purposes without restriction; (ii) to the extent that Statistical

Data constitutes Personal Data for the purposes of the GDPR), each Party shall be an independent Data Controller in respect of such data, shall independently determine the purposes and means of its processing of such data and will comply with the obligations applicable to it under Data Protection Laws in respect of such data; (iii) Statistical Data does not constitute Customer Personal Data for the purposes of this Agreement; and (iv) except for this clause 12, the terms of this Addendum shall not apply to TRIBLIO's Processing of Statistical Data.

[Signature Page Follows]

SCHEDULE 1 TO THE DATA PROCESSING ADDENDUM DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

1. THE PURPOSE OF THE PROCESSING OF PERSONAL DATA

TRIBLIO will Process Personal Data only for the following purposes:

Providing Customer the Service under the Agreement (including the technical support and maintenance services specified in the Agreement) and other purposes provided by the Agreement.

2. CONTENTS OF THE PROCESSING

TRIBLIO will perform the following Personal Data Processing operations:

- TRIBLIO will store the Personal Data on servers hosted by TRIBLIO or a service provider engaged by TRIBLIO.
- TRIBLIO will have access to the Personal Data and use the data for providing services to the Customer under the Agreement and carrying out other acts provided by the Agreement.

3. CATEGORIES OF DATA SUBJECTS AND PERSONAL DATA

TRIBLIO will Process the following categories of data subjects and Personal Data:

- Information related to the users of the Services provided by TRIBLIO to Customer under the Agreement, such as:
  - Username and other user credentials,
  - e-mail addresses,
  - IP addresses,
  - other contact details of the users, such as phone numbers,
  - log data relating to the use of the services and
  - other Personal Data that may be provided by the users under the Agreement (for example data provided in the service requests sent by the users).

Exhibit 1

For the sake of clarity, the parties hereby agree:

1. Not to include *Clause 7 (optional) – Docking Clause*, as part of these SCC's.
2. Regarding *Clause 9 – Use of sub-processors, MODULE TWO: Transfer controller to processor*. (a) Option 2 will apply with a 30 day time period.
3. Not to include the optional paragraph under *Clause 11 (a) – Redress*, as part of these SCC's.
4. Regarding *Clause 17 – Governing Law*, that the following Clauses shall be governed by the law of Ireland.
5. Regarding *Clause 18 – Choice of forum and jurisdiction*, that any dispute arising from these Clauses shall be resolved by the courts of Ireland.

ANNEX I

A. **LIST OF PARTIES**

MODULE TWO: Transfer controller to processor

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

1 Details as per page two of order form.

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]*

1. Name: Triblio, Inc.

Address: 11600 Sunrise Valley Drive, Suite #100, Reston, VA 20191, USA

Contact person's name, position and contact details: Dawn Orr, CFO/COO, dawn@triblio.com

Activities relevant to the data transferred under these Clauses: Services provided by Triblio, Inc. as specified in the Service Agreement.

Signature and date:

Role (controller/processor): Processor

2. DPO

   John McGill

   c/o IDG Direct, Millennium House, Great Strand Street, Dublin 1, Ireland

   gdpr@idgcommunications.com

3. EU Representative
   IDG Communications Media AG
   Lyonel-Feininger-Strasse 26
   Munich 80807
   Germany

   GDPRrepresentative@idgcommunications.com

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Users of the Services provided by TRIBLIO to CUSTOMER.

Categories of personal data transferred

Information related to the users of the services provided by TRIBLIO to CUSTOMER under the Customer Contract, such as:

- username and other user credentials,
- e-mail addresses,
- IP addresses,
- other contact details of the users, such as phone numbers,
- log data relating to the use of the services and
- other Personal Data that may be provided by the users under the Customer Contract (for example data provided in the service requests sent by the users).

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.

There is no sensitive or special category data processed or transferred

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

Whenever a user of the Services provided by TRIBLIO to CUSTOMER arrives at the CUSTOMER website and consents.

Nature of the processing

Performance of the services described above (activities relevant to the transfer).

Purpose(s) of the data transfer and further processing

TRIBLIO may receive Personal Data from Customer related to the provision of services by TRIBLIO under the Customer Contract (including the technical support and maintenance services specified in the Customer Contract) and other purposes provided by the Customer Contract.

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

Until the Data Subject withdraws their consent or the purpose for which the data was collected no longer exists or the contract with the Customer terminates.

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

Transfers to sub-processors will where required be covered by separate Standard Contractual Clauses for Controller to Processor or Processor to Processor transfers.

C. COMPETENT SUPERVISORY AUTHORITY

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

Bavarian Supervisory Authority (Germany)

ANNEX II

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

MODULE TWO: Transfer controller to processor

EXPLANATORY NOTE:

The technical and organizational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Triblio has implemented technical and organisational security measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and its internal controls are regularly audited by independent third party auditors and reported via the SOC II, Type 2 Report, a summary of which is is available to Customer upon request.

Technical and Organizational Security Measures

Triblio is Soc II Type 2 certified

1. Confidentiality (Article 32 Paragraph 1 Point b GDPR)

- Physical Access Control
  No unauthorized access to Data Processing Facilities, e.g.: magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV Systems
- Electronic Access Control
  No unauthorized use of the Data Processing and Data Storage Systems, e.g.: (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media
- Internal Access Control (permissions for user rights of access to and amendment of data)
  No unauthorized Reading, Copying, Changes or Deletions of Data within the system, e.g. rights authorization concept, need-based rights of access, logging of system access events
- Isolation Control
  The isolated Processing of Data, which is collected for differing purposes, e.g. multiple Client support, sandboxing;
- Pseudonymization (Article 32 Paragraph 1 Point a GDPR; Article 25 Paragraph 1 GDPR)
  The processing of personal data in such a method/way, that the data cannot be associated with a specific Data Subject without the assistance of additional Information, provided that this additional information is stored separately, and is subject to appropriate technical and organizational measures.

2. Integrity (Article 32 Paragraph 1 Point b GDPR)

- Data Transfer Control
  No unauthorized Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature.
- Data Entry Control
  Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, e.g.: Logging, Document Management

3. Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)

- Availability Control
  Prevention of accidental or willful destruction or loss, e.g.: Backup Strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, IDS, reporting procedures and contingency planning
- Rapid Recovery (Article 32 Paragraph 1 Point c GDPR) ;

4. Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)

- Data Protection Management;
- Incident Response Management;
- Data Protection by Design and Default (Article 25 Paragraph 2 GDPR);
- Order or Contract Control
  No third-party data processing as per Article 28 GDPR without corresponding instructions from CLIENT, e.g.: clear and unambiguous contractual arrangements, formalized Order Management, strict controls on the selection of the Service Provider, duty of pre-evaluation, supervisory follow-up checks.

For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

Technical and Organizational Security Measures

1. Confidentiality (Article 32 Paragraph 1 Point b GDPR)

- Physical Access Control
  No unauthorized access to Data Processing Facilities, e.g.: magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV Systems
- Electronic Access Control
  No unauthorized use of the Data Processing and Data Storage Systems, e.g.: (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media
- Internal Access Control (permissions for user rights of access to and amendment of data)
  No unauthorized Reading, Copying, Changes or Deletions of Data within the system, e.g. rights authorization concept, need-based rights of access, logging of system access events
- Isolation Control
  The isolated Processing of Data, which is collected for differing purposes, e.g. multiple Client support, sandboxing;
- Pseudonymization (Article 32 Paragraph 1 Point a GDPR; Article 25 Paragraph 1 GDPR)
  The processing of personal data in such a method/way, that the data cannot be associated with a specific Data Subject without the assistance of additional Information, provided that this additional information is stored separately, and is subject to appropriate technical and organizational measures.

2. Integrity (Article 32 Paragraph 1 Point b GDPR)

- Data Transfer Control
  No unauthorized Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature.
- Data Entry Control
  Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, e.g.: Logging, Document Management

3. Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)

- Availability Control
  Prevention of accidental or willful destruction or loss, e.g.: Backup Strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, IDS, reporting procedures and contingency planning
- Rapid Recovery (Article 32 Paragraph 1 Point c GDPR) ;

4. Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)

- Data Protection Management;
- Incident Response Management;
- Data Protection by Design and Default (Article 25 Paragraph 2 GDPR);
- Order or Contract Control
  No third-party data processing as per Article 28 GDPR without corresponding instructions from CLIENT, e.g.: clear and unambiguous contractual arrangements, formalized Order Management, strict controls on the selection of the Service Provider, duty of pre-evaluation, supervisory follow-up checks.

ANNEX III

LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorization of sub-processors (Clause 9(a), Option 1).

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

1. Name: Amazon Web Services (AWS)

   Address: 410 Terry Avenue North Seattle, WA 98109-5210, USA

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorized): Platform/Cloud Storage, Hosting in US-West (California), US-East (Virginia) and EU-West (Ireland)

Exhibit 2 – UK International Data Transfers Addendum – UK SCCs

Information Commissioner's Office

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

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

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

Part 1: Tables

Table 1: Parties

Start date		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: Triblio, Inc. Trading name (if different): Main address (if a company registered address): 11600 Sunrise Valley Drive Suite #100, Reston, VA 20191, USA Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Dawn Orr Job Title: CFO/COO

		Contact details including email: dawn@triblio.com
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

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

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	NO	NO	NO			
2	YES	NO	NO	Prior	30 days	
3	NO					
4	NO					

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 A of this DPA
Annex 1B: Description of Transfer: Annex A of this DPA
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: ANNEX B of this DPA
Annex III: List of Sub processors (Modules 2 and 3 only): ANNEX C of this DPA

Table 4: Ending this Addendum when the Approved Addendum Changes

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

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

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

Interpretation of this Addendum

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

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

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.