Global Data Privacy Addendum

This Global Data Privacy Addendum (this "**Privacy Addendum**") is attached and made part of the agreement (the **"Master Agreement**") between Customer (as identified on the Quote), including all affiliates, if any, and the Service Provider which processes Personal Data on behalf of Customer pursuant to the Master Agreement (as identified on the Quote).

The Privacy Addendum is divided into two separate addendums setting forth the privacy provisions applicable to the Master Agreement. Unless otherwise stated, the terms of this Privacy Addendum will apply to all processing of Personal Data in relation to the Services provided under the terms of the Master Agreement.

PART A: EU/UK GDPR and Swiss Addendum

1. DEFINITIONS

1.1 "**Adequate Country**" means a country or territory recognised as providing an adequate level of protection for Personal Data under an adequacy decision made, from time to time, by (as applicable) (i) the Information Commissioner's Office and/or under applicable UK law (including the UK GDPR), or (ii) the European Commission under the GDPR, or (iii) the Swiss Federal Data Protection Authority under Swiss Data Protection Law.

1.2 **"Data Subject Request**" means a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure, data portability, object to the processing, or its right not to be subject to an automated individual decision making**.**

1.3 "**EEA**" means the European Economic Area.

1.4 "**EU Clauses**" means the standard contractual clauses for international transfers of personal data to third countries set out in the European Commission's Decision 2021/914 of 4 June 2021 (at http://data.europa.eu/eli/dec_impl/2021/914/oj) incorporating Module Two for Controller to Processor transfers and Module Three for Processor to Processor transfers (as applicable), or its valid successor, and which form part of this DPA in accordance with Schedule 4.

1.5 **"EU/UK Rules"** means (a) in the European Union, the General Data Protection Regulation 2016/679 (the "**GDPR**"), (b) in the UK, the UK General Data Protection Regulation 2016/679, as implemented by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020 (the "**UK GDPR**") and the Data Protection Act 2018.

1.6 **"Personal Data**" means any information relating to an identified or identifiable natural person ('**Data Subject'**) located in the EEA, United Kingdom ("**UK**") or Switzerland; an identifiable natural person is one who can be identified, directly or indirectly in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; and is processed by Service Provider on behalf of the Customer within the scope of the Master Agreement.

1.7 **"Services"** means the services and other activities to be supplied to or carried out by or on behalf of Service Provider for the Customer pursuant to the Master Agreement.

1.8 **"Standard Contractual Clauses"** means the EU Clauses, the Swiss Addendum and/or the UK Approved Addendum.

1.9 "**Supervisory Authority**" means in the UK, the Information Commissioner's Office ("**ICO**") (and, where applicable, the Secretary of State or the government), and in the EEA, an independent public authority established pursuant to the GDPR.

1.10 "**Swiss Addendum**" means the addendum set out in Schedule 3.

1.11 "**Swiss Data Protection Law**" means the Swiss Federal Data Protection Act of 19 June 1992 and, when in force, the Swiss Federal Data Protection Act of 25 September 2020 and its corresponding ordinances as amended, superseded or replaced from time to time.

1.12 "**UK Approved Addendum**" means the template Addendum B.1.0 issued by the UK's Information Commissioner's Office and laid before Parliament in accordance with s119A of the Data Protection Act 2018 of the UK on 2 February 2022, and expected to be in force on 21 March 2022, or its valid successor.

1.13 **"UK Mandatory Clauses**" means the Mandatory Clauses of the UK Approved Addendum, as updated from time to time and/or replaced by any final version published by the Information Commissioner's Office.

2. APPLICABILITY; ROLES OF THE PARTIES

2.1 This Privacy Addendum amends and supplements the Master Agreement between the parties. This Privacy Addendum will not apply to the processing of Personal Data, where such processing is not regulated by the EU/UK Rules or Swiss Data Protection Law.

2.2 Capitalized terms used but not defined in this Privacy Addendum have the meanings assigned to them in the Master Agreement or the EU/UK Rules, including the terms "Data Protection Officer", "Member States", "Personal Data Breach", "Privacy Impact Assessment".

2.3 In the context of this Privacy Addendum, the Customer acts as a Data Controller or Data Processor (as applicable) and the Service Provider acts as a Data Processor with regard to the processing of Personal Data.

2.4 Service Provider shall carry out the Services and process the Personal Data received from the Customer as set out in the Master Agreement or as otherwise notified in writing by the Customer to Service Provider during the term of the Master Agreement. In the event that in Service Provider's opinion a processing instruction given by the Customer may infringe EU/UK Rules or Swiss Data Protection Law, Service Provider shall immediately inform the Customer upon becoming aware of such a processing instruction.

2.5 Service Provider shall undertake at all times to comply with the EU/UK Rules and not to perform its obligations under the Master Agreement in such way as to cause the Customer to breach any of its applicable obligations under the EU/UK Rules and any existing regulations issued by the relevant data protection authorities.

3. DATA PROTECTION

3.1 All Personal Data provided to Service Provider by the Customer or obtained by Service Provider in the course of its work with the Customer should be protected and may not be copied, disclosed or processed in any way without the written authority of the Customer. To the extent that the provisions of the Master Agreement or the instructions of the Customer necessitate the copying, disclosure or processing of data, this will be deemed to constitute the required authority to do so.

3.2 Service Provider agrees to comply from time to time with any reasonable measures required by the Customer to ensure its obligations under this Privacy Addendum are satisfactorily performed in accordance with all applicable legislation. This includes any best practice guidance relevant to the Services that Customer directly brings to the attention of Service Provider.

4. PROCESSING PERSONAL DATA

4.1 Where Service Provider processes Personal Data (whether stored in the form of physical or electronic records) on behalf of the Customer it shall:

4.1.1 Process the Personal Data only to the extent, and in such manner, as is necessary in order to comply with its obligations under the Master Agreement or as is required by law including the EU/UK Rules, Swiss Data Protection Law and any existing laws, rules or regulations issued by the relevant data protection authorities;

4.1.2 Implement appropriate technical and organisational measures and take the steps necessary to protect the Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure, and promptly supply details of such measures as requested by the Customer; such security measures are set out in Section 6 of this Privacy Addendum (Part A); and

4.1.3 At the Customer's request, promptly supply the Customer with details of the technical and organisational systems in place to safeguard the security of the Personal Data held and to prevent unauthorised access.

4.2 Customer acknowledges and agrees that (a) Service Provider's affiliates may be retained as sub-processors; and (b) Service Provider and Service Provider's affiliates respectively may engage third-party sub-processors in connection with the provision of the Services. Service Provider will ensure that any third party to which it sub-contracts any processing has entered into a written contract with Service Provider containing similar provisions to those in this Privacy Addendum, to the extent applicable to the nature of the Services provided by such sub-processor. Upon Customer's request, Service Provider shall make available to Customer the current list of sub-processors with their country of location. If Service Provider provides hosting services under the Master

Agreement, the Customer agrees and acknowledges that Service Provider is allowed to host the Personal Data at a third-party data center provider. For the avoidance of doubt, Service Provider shall remain liable for the processing activities of each sub-processor as if those achieved were its own.

4.3 Unless applicable laws require retention of such Personal Data, Service Provider agrees that in the event that it is notified by the Customer that it is not required to provide any further services to the Customer under this Privacy Addendum, Service Provider shall transfer a copy of all information (including Personal Data) held by it in relation to this Privacy Addendum to the Customer in a format chosen by the Customer (provided that the Customer pays for the associated costs) and/or, at the Customer's request, destroy all such information using a secure method which ensures that it cannot be accessed by any third party and shall issue the Customer with a written confirmation of secure disposal.

4.4 All copyright, database right and other intellectual property rights in any Personal Data processed under this Privacy Addendum (including but not limited to any updates, amendments or adaptations to the Personal Data by either the Customer or Service Provider) will belong to the Customer. Service Provider is licensed to use such data only for the term of and in accordance with this Privacy Addendum.

5. RIGHTS OF DATA SUBJECTS

5.1 Service Provider shall, to the extent legally permitted, promptly notify Customer if it receives a Data Subject Request. Taking into account the nature of the processing, Service Provider shall assist Customer by appropriate technical and organizational measures, to the extent possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Chapter III of the GDPR. Except to the extent required by applicable law, Service Provider shall not respond to any such Data Subject Request without Customer's prior written consent except to confirm that the request relates to Customer.

5.2 Further, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Service Provider shall upon Customer's request provide reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Service Provider is legally permitted to do so and provided that such Data Subject Request is required under applicable EU/UK Rules. Any costs arising from such provision of assistance shall be the responsibility of Customer, to the extent legally permitted.

6. SECURITY

6.1 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, Service Provider shall ensure that in respect of all Personal Data it receives from or processes on behalf of the Customer it shall maintain security measures to a standard appropriate to the:
(a) harm that might result from unlawful or unauthorised processing or accidental loss, damage or destruction of the Personal Data; and (b) nature of the Personal Data.

6.2 Service Provider shall, with regard to Personal Data, implement and maintain appropriate technical and organizational security measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR, and particularly those related to possible Personal Data Breaches. Specifically, Service Provider shall:

6.2.1 have in place and comply with a security policy which: (a) defines security needs based on a regular Privacy Impact Assessment; (b) allocates responsibility for implementing the policy to a specific individual or members of a team, including having a Data Protection Officer in place where required under EU/UK Rules; (c) is disseminated to all relevant members, volunteers and staff; and (d) provides a mechanism for feedback and review;

6.2.2 ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in processing the Personal Data in accordance with best industry practice;

6.2.3 prevent unauthorised access to the Personal Data;

6.2.4 ensure its storage of Personal Data conforms with the industry practice such that the media on which Personal Data is recorded (including paper records and records stored electronically) are stored in secure locations and access by personnel to Personal Data is strictly monitored and controlled;

6.2.5 have secure methods in place for the transit of Personal Data within the customer support portal (for instance, by using encryption);

6.2.6 use password protection on computer systems on which Personal Data is stored and ensure that only authorised personnel are given details of the password;

6.2.7 take reasonable steps to ensure the reliability of any employee, agent, contractor or other individuals who have access to the Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know or access the relevant Personal Data, as strictly necessary for the purposes of the Master Agreement, and to comply with EU/UK Rules in the context of that individual's duties to the Service Provider;

6.2.8 ensure that any employees, agents, contractors or other individuals required to access the Personal Data are informed of the confidential nature of the Personal Data and comply with the obligations set out in this Privacy Addendum;

6.2.9 ensure that none of the employees, agents, contractors or other individuals who have access to the Personal Data publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Customer;

6.2.10 have in place methods for detecting and dealing with breaches of security (including loss, damage or destruction of Personal Data) including: (a) the ability to identify which individuals have worked with specific Personal Data; and (b) having a proper procedure in place for investigating and remedying breaches of the data protection principles contained in the EU/UK Rules, including written records.

6.2.11 have a secure procedure for backing up and storing back-ups separately from originals; and

6.2.12 have a secure method of disposal for unwanted Personal Data including back-ups, disks, print outs and redundant equipment.

6.3 Service Provider shall provide the Customer with relevant documentation, such as an audit report (upon a written request and subject to obligations of confidentiality), with regard to any data protection impact assessments, and prior consultations with supervising authorities or other competent data privacy authorities, when the Customer reasonably considers that such data protection impact assessments or prior consultations are required pursuant to Article 35 or 36 of the GDPR or pursuant to the equivalent provisions of any other EU/UK Rules, but in each such case solely with regard to processing of Personal Data by, and taking into account the nature of the Processing and information available to, the Service Provider. Such audit will be conducted at the Customer's cost and expense, to the extent legally permitted.

7. SECURITY BREACH MANAGEMENT AND NOTIFICATION

7.1 Service Provider shall, in accordance with the EU/UK Rules, notify the Customer and/or the supervisory authority as soon as any Personal Data Breach with respect to the Personal Data occurs, but no later than 48 hours from the discovery of such a Personal Data Breach. Service Provider's notification of or response to a Personal Data Breach under this Section 7.1 will not be construed as an acknowledgement by Service Provider of any fault or liability with respect to the Personal Data Breach.

7.2 Service Provider will use reasonable efforts to identity the cause of such Personal Data Breach and shall promptly and without undue delay: (a) investigate the Personal Data Breach and provide Customer with information about the Personal Data Breach, including if applicable, such information a Data Processor must provide to a Data Controller under Article 33(3) of the GDPR to the extent such information is reasonably available; and (b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Personal Data Breach to the extent the remediation is within Service Provider's reasonable control The obligations herein shall not apply to any breach that is caused by Customer or authorized users. Notification will be delivered to Customer in accordance with Section 7.3 below.

7.3 Notification(s) of Personal Data Breaches, if any, will be delivered to one or more of Customer's business, technical or administrative contacts by any means Service Provider selects, including via email. It is Customer's sole responsibility to ensure it maintains accurate contact information on Service Provider's support systems at all times.

8. OBLIGATIONS OF THE CUSTOMER

The Customer is solely responsible for:

8.1 Complying, at all times with the EU/UK Rules with respect to the processing of Personal Data in connection with the Master Agreement and the Services;

8.2 Ensuring the processing of the Personal Data by Service Provider is lawful;

8.3 Where applicable, ensuring that legally binding consents to the collection, access, use, maintenance, and/or disclosure of the Personal Data in accordance with the EU/UK Rules and Customer policies and procedures have been obtained from each individual and entity (including without limitation consumers, business customers, and/or Customer employees and contractors) to whom the Personal Data relates;

8.4 Rendering any Personal Data on its systems unusable, unreadable, or indecipherable to unauthorized individuals in accordance with industry standards, applicable law, and any relevant Codes of Conduct;

8.5 Establishing the applicable information security safeguards and associated policies for protecting Personal Data in its facilities. Customer must communicate the relevant safeguards and policies to Service Provider with reasonable advance notice and in writing when Service Provider provides Services at a Customer facility or accesses Customer's systems;

8.6 Promptly informing Service Provider of any policies it implements with respect to the processing and protection of Personal Data with express instructions as to how these policies should be implemented by Service Provider;

8.7 Promptly informing Service Provider of any request for erasure with respect to Data Subject's Personal Data with detailed instructions as to how Service Provider should address the request; and

8.8 Providing to Service Provider and also promptly updating, when necessary, the information indicated below (where applicable): (a) identity and contact information of the Data Protection Officer of the Customer; (b) identity and contact information of the EU representative of the Customer; (c) description of the categories of processing carried out by Customer with respect to the Services; (d) types of Personal Data to be processed; and (e) categories of Data Subjects to whom the Personal Data relates.

9. INTERNATIONAL DATA TRANSFERS

9.1 Customer agrees that its use of the Services will involve the transfer of Personal Data to, and processing of Personal Data in, locations outside of the UK, Switzerland and/or EEA from time to time, such as for purposes of providing support to Customer, including but not limited to processing in the United States.

9.2 **Transfers Pursuant to the Standard Contractual Clauses**

9.2.1 *UK transfers:*

9.2.1.1 To the extent Personal Data is transferred to Service Provider and processed by or on behalf of Service Provider outside the UK (except if in an Adequate Country) in circumstances where such transfer would be prohibited by UK GDPR in the absence of a transfer mechanism, the parties agree that the EU Clauses subject to the UK Approved Addendum will apply. The UK Approved Addendum is incorporated into this Privacy Addendum.

9.2.1.2 Schedule 2 references the information required by Tables 1 to 4 inclusive of the UK Approved Addendum.

9.2.2 *EU transfers:*

9.2.2.1 To the extent Personal Data is transferred to Service Provider and processed by or on behalf of Service Provider outside the EEA (except if in an Adequate Country) in circumstances where such transfer would be prohibited by EU GDPR in the absence of a transfer mechanism, the parties agree that the EU Clauses will apply in respect of that processing and are incorporated into this Privacy Addendum in accordance with Schedule 4.

9.2.2.2 Schedule 4 contains the information required by the EU Clauses.

9.2.3 *Swiss transfers:*

9.2.3.1 To the extent Personal Data is transferred to Service Provider and processed by or on behalf of Service Provider outside Switzerland (except if in an Adequate Country) in circumstances where such transfer would be prohibited by Swiss Data Protection Laws in the absence of a transfer mechanism, the parties agree that the EU Clauses subject to the Swiss Addendum will apply in respect of that processing. The Swiss Addendum is incorporated into this Privacy Addendum.

9.2.3.2 Schedule 3 and Schedule 4 contains the information required for the Swiss Addendum, including for the purposes of transfers to which this clause 9.2.3 applies.

9.2.4 Service Provider may (i) replace the EU Clauses, the Swiss Addendum and/or the UK Approved Addendum generally or in respect of the EEA, Switzerland and/or the UK (as appropriate) with any alternative or replacement transfer mechanism in compliance with applicable EU/UK Rules or applicable Swiss Data Protection Law, including any further or alternative standard contractual clauses approved from time to time and (ii) make reasonably necessary changes to this Privacy Addendum by notifying Customer of the new transfer mechanism or content of the new standard contractual clauses (provided their content is in compliance with the relevant decision or approval), as applicable.

9.3 **Transfers Pursuant to the Privacy Shield**

9.3.1 In the event that after the CJEU Schrems II decision, the EU-US Privacy Shield (including but not limited to its successor and any similar programs for other countries) (collectively, "**Privacy Shield**") constitutes a valid transfer mechanism under EU/UK Rules, and Service Provider self-certifies to, or otherwise participates in, the Privacy Shield, to the extent permitted by EU/UK Rules, Service Provider shall transfer Personal Data in accordance with the Privacy Shield in lieu of the applicable EU Clauses, UK Approved Addendum, and Swiss Addendum.

10. GENERAL TERMS

10.1 Each party's and all of its affiliates' liability, taken together in the aggregate, arising out of or related to this Privacy Addendum whether in contract, tort or under any other theory of liability, is subject to the limitation of liability section of the Master Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its affiliates under the Master Agreement and this Privacy Addendum.

10.2 No alteration, amendment, or modification of this Privacy Addendum will be valid unless in writing and signed by an authorized representative of both parties.

10.3 Any ambiguity in the terms of this Privacy Addendum will be resolved to permit Service Provider or Customer to comply with the EU/UK Rules .

10.4 This Privacy Addendum is the entire and complete agreement between the parties with respect to the privacy and security of Personal Data and supersedes any other agreements, representations, or understandings whether oral or written. All clauses of the Master Agreement, that are not explicitly amended or supplemented by the clauses of this Privacy Addendum, and as long as this does not contradict with compulsory requirements of EU/UK Rules or other applicable laws, under this Privacy Addendum, remain in full force and effect and shall apply, including, but not limited to: Governing Law and Dispute Resolution, Jurisdiction, Limitation of Liability (to the maximum extent permitted by the EU/UK Rules and EU Clauses). If the Master Agreement does not contain a venue or jurisdiction for disputes and claims, Service Provider and Customer agree that, notwithstanding any language to the contrary, disputes between the Parties under the Standard Contractual Clauses may also be adjudicated in the United States to the extent not expressly prohibited by applicable laws.

10.5 Should any provision of this Privacy Addendum be found invalid or unenforceable pursuant to any applicable law, then the invalid or unenforceable provision will be deemed superseded by a valid, enforceable provision that most closely matches the intent of the original provision and the remainder of the Privacy Addendum will continue in effect.

10.6 If Service Provider makes a determination that it can no longer meet its obligations in accordance with this Privacy Addendum, it shall promptly notify the Customer of that determination, and cease the processing or take other reasonable and appropriate steps to remediate.

10.7 Notices required under this Privacy Addendum shall be sent according to the Master Agreement with a copy (which shall not constitute notice) to both the usual point of contact or support at Service Provider and via e-mail to: privacy@trilogy.com.

SCHEDULE 1

Data Processing Details

For the purposes of the Privacy Addendum and Schedules 2. 3 and 4, the parties set out below a description of the Personal Data being processed under the Master Agreement and further details required pursuant to the EU/UK Rules.

Subject Matter of the Processing	Service Provider's provision of the Services to Customer.
Nature and purpose of Processing	The collection and storage of Personal Data pursuant to providing the Services to Customer.
Types of Personal Data	Personal Data that Customer in its discretion uploads into the Services or Service Provider is directed to collect.
Sensitive Personal Data and applied restrictions	None
Categories of Data Subject	Data Subjects may include any end users or others (including without limitation employees, customers, or suppliers) about whom Personal Data is provided to Service Provider via the Services by, or at the direction of, Customer.
Duration of Processing	For the duration of the Agreement, or until the processing is no longer necessary for the purposes.

SCHEDULE 2

UK transfers

For the purposes of the UK Approved Addendum,

1. the information required for Table 1 is contained in Schedule 1 of this Privacy Addendum and the start date shall be deemed dated the same date as the EU Clauses;
2. in relation to Table 2, the version of the EU Clauses to which the UK Approved Addendum applies is Module Two for Controller to Processor and Module Three for Processor to Processor transfers (as applicable);
3. in relation to Table 3, the list of parties and description of the transfer are as set out in Annex I of Schedule 4 of this Privacy Addendum, Service Provider's technical and organisational measures are set in section 6.2 of this Privacy Addendum, and the list of Service Provider's sub-processors shall be provided pursuant to section 4.2 of this Privacy Addendum; and
4. in relation to Table 4, neither party will be entitled to terminate the UK Approved Addendum in accordance with clause 19 of the UK Mandatory Clauses.

SCHEDULE 3

Swiss Addendum

In respect of transfers otherwise prohibited by Swiss Personal Data:

1. The FDPIC will be the competent supervisory authority;

2. Data subjects in Switzerland may enforce their rights in Switzerland under Clause 18c of the EU Clauses, and

3. References in the EU Clauses to the GDPR should be understood as references to Swiss Data Protection Law insofar as the data transfers are subject to Swiss Data Protection Law.

SCHEDULE 4

EU Clauses

1. For the purposes of this Schedule 4, the EU Clauses (Module II and Module III as applicable), available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN, shall be incorporated by reference to this Schedule and the Privacy Addendum and shall be considered an integral part thereof, and the Parties' signatures in the Privacy Addendum, or Master Agreement (as applicable) shall be construed as the Parties' signature to the EU Clauses. In the event of an inconsistency between the Privacy Addendum and the EU Clauses, the latter will prevail.

2. For the purposes of the EU Clauses, the following shall apply:

   - Customer shall be the data exporter and Service Provider shall be the data importer. Each Party agrees to be bound by and comply with its obligations in its role as exporter and importer respectively as set out in the EU Clauses.

   - Clause 7 (Docking clause) shall be deemed as included.

   - Clause 9 (Use of sub-processors): OPTION 2 – GENERAL WRITTEN AUTHORISATION shall apply. 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 as set out in clause 4 of the Privacy Addendum.

   - Clause 11 (Redress): optional clause (optional redress mechanism before an independent dispute resolution body) shall be deemed as not included.

   - Clause 13 (a) (Supervision):

     - *[Where Customer is established in an EU Member State*:] 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 I.C, shall act as competent supervisory authority.

     - [*Where Customer is not established in an EU Member State but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679*:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority. [OR]

     - [*Where Customer is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679*:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

   - 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 (b) (Choice of forum and jurisdiction): The Parties agree that any dispute between them arising from the EU Clauses shall be resolved by the courts of Ireland.

3. To the extent not prohibited by applicable law, any provision in the EU Clauses relating to liability of the parties with respect to each other shall be subject to the limitations and exclusions of the Master Agreement.

4. Any provision in the EU Clauses relating to the right to audit shall be interpreted in accordance with Clause 6.3 of the Privacy Addendum and the Master Agreement.

ANNEX I to Schedule 4

A. LIST OF PARTIES

Data exporter(s):
Name: Customer as specified on the Quote
Address: As specified on the Quote
Contact person's name, position and contact details: As specified on the Quote or available on Customer's Privacy Policy
Activities relevant to the data transferred under these Clauses: data exporter will transfer Personal Data to the data importer as required for the provision of Services by the data importer under the Master Agreement and as set out in the Privacy Addendum.
Signature and date: please refer to signature and date in the Privacy Addendum or Master Agreement.
Role (controller/processor): Controller or Processor, as appropriate

Data importer(s):
Name: Service Provider as specified on the Quote
Address: As specified on the Quote
Contact person's name, position and contact details: Available on Privacy Policy.
Activities relevant to the data transferred under these Clauses: data importer will process personal data as required for the provision of Services under the Master Agreement and as set out in the Master Agreement.
Signature and date: signature and date in the Privacy Addendum or Master Agreement.
Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred
See Schedule I to the Privacy Addendum

Categories of personal data transferred
See Schedule I to the Privacy Addendum

Sensitive data transferred (if applicable) and applied restrictions or safeguards
See Schedule I to the Privacy Addendum

Frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
Transfers will occur from time to time as required during the course of the performance of the Services under the Agreement.

Nature of the processing
See Schedule 1 to the Privacy Addendum

Purpose(s) of the data transfer and further processing
See Schedule 1 to the Privacy Addendum

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
See Schedule 1 to the Privacy Addendum

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
Available on request in accordance with section 4.2 of the Privacy Addendum

C. COMPETENT SUPERVISORY AUTHORITY
Identify the competent supervisory authority/ies in accordance with Clause 13

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL
See section 6 of the Privacy Addendum

ANNEX III – LIST OF SUB-PROCESSORS
Available on request in accordance with section 4.2 of the Privacy Addendum

Non-GDPR Addendum

The following specific terms apply to all processing of Personal Information (as defined below) for the Customer as part of the services provided under the Master Agreement where the EU/UK GDPR and Swiss Addendum does not apply.

Whereas the parties have entered into a Master Agreement;

Whereas the parties would like to further specify the data privacy principles that apply to the Master Agreement;

Now, therefore, in consideration of the rights and obligations set forth in the Master Agreement, which they acknowledge, the parties agree as follows:

1. Definitions

1.1. Capitalized terms used but not defined in this Privacy Addendum will have the meanings assigned to them in the Master Agreement.

1.2. "**Business Contact Information**" is defined as name, job title, department name, company name, business telephone, mobile phone number (if used for business purposes between Service Provider and Customer), business fax number, and business e-mail address.

1.3. "**CCPA**" is the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq.

1.4. **"Personal Information**" means information that is accessed, received, maintained, processed, stored, or transmitted by Service Provider on behalf of Customer within the scope of the Master Agreement, and includes an individual's first name or first initial and last name in combination with any one or more of the following items: (i) social security number; (ii) driver's license number or government-issued identification number; or (iii) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account. For clarity, Personal Information excludes Business Contact Information. For information covered by the CCPA, the above definition shall not apply and instead Personal Information shall use the applicable definition of Personal Information from the CCPA, subject to any applicable qualifications or exclusions contained in the CCPA.

1.5. "**Personal Information Request**" means a request from a consumer under the CCPA to exercise the right to know or right to delete.

1.6. "**Security Breach**" means an unauthorized acquisition or use of unsecured Personal Information that creates a substantial risk of identity theft or fraud against an individual. For clarity, a good faith acquisition of Personal Information by an employee or agent of Service Provider is not a Security Breach unless such employee or agent uses or discloses the Personal Information in an unauthorized manner.

2. General

2.1. This Privacy Addendum amends and supplements the Master Agreement between the parties. The terms of this Privacy Addendum will apply to all processing of Personal Information that is not covered by the terms of the GDPR Addendum in relation to the services provided under the terms of the Master Agreement.

2.2. Notices required under this Privacy Addendum shall be sent according to the Master Agreement with a copy (which shall not constitute notice) to both the usual point of contact or support at Service Provider and via e-mail to: privacy@trilogy.com.

2.3. The Service Provider shall carry out the services and process Personal Information received from the Customer as set out in the Master Agreement or as otherwise notified in writing by the Customer to the Service Provider during the term of the Master Agreement.

2.4. With respect to a Personal Information Request, Service Provider shall:

2.4.1. To the extent legally permitted, promptly notify Customer if it receives a Personal Information Request. Taking into account the nature of the processing, Service Provider shall assist Customer by appropriate technical and organizational measures, to the extent possible, for the fulfillment of Customer's obligation to respond to a Personal Information Request. Except to the extent required by applicable law, Service Provider shall not respond to any such Personal Information Request without Customer's prior written consent except to confirm that the request relates to Customer.

2.4.2. Upon Customer's request, to the extent Customer, in its use of the Services, does not have the ability to address a Personal Information Request, provide reasonable efforts to assist Customer in responding to such Personal Information Request, to the extent Service Provider is legally permitted to do so and provided that such Personal Information Request is required. Any costs arising from such provision of assistance shall be the responsibility of Customer, to the extent legally permitted.

3. Permitted Uses and Disclosures

3.1. Service Provider shall use, disclose, and retain all Personal Information:

3.1.1. As specifically authorized in the Master Agreement and this Privacy Addendum;

3.1.2. Solely for the purpose of performing the services described in the Master Agreement; and

3.1.3. In accordance with applicable laws.

3.2. Service Provider shall not sell, rent, transfer, distribute, or otherwise disclose or make available any Personal Information to any third party without prior written permission from Customer, unless and to the extent required by law. Notwithstanding the foregoing, Service Provider has the right to use third parties, including offshore entities who employ foreign nationals, as well as employees and contractors of Service Provider's affiliates and subsidiaries, who may also be foreign nationals, in performance of its obligations described in the Master Agreement, and Service Provider has the right to disclose Personal Information to such third parties provided that such third parties are subject to confidentiality obligations similar to those between Service Provider and Customer.

4. Data Security Obligations.

4.1. Service Provider shall:

4.1.1. Implement a comprehensive information security program which includes commercially reasonable technical, and administrative safeguards to protect the confidentiality of Personal Information that are no less rigorous than accepted security industry practices;

4.1.2. Keep all Personal Information contained in any format (e.g., paper, computer system, and removable media) in a secure facility where access of unauthorized personnel is restricted;

4.1.3. Install reasonably up-to-date firewall protection and operating system patches for files containing Personal Information on a system that is connected to the Internet;

4.1.4. Install reasonably up-to-date versions of system security agent software which includes malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis, on systems vulnerable to malware and containing or channeling access to systems containing Personal Information;

4.1.5. Implement secure user authentication protocols including:

4.1.5.1. Control of user IDs and other identifiers;

4.1.5.2. A reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;

4.1.5.3. Control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;

4.1.5.4. Restricting access to active users and active user accounts only; and

4.1.5.5. Blocking access to user identification after multiple unsuccessful attempts to gain access or exceeding the limitation placed on access for the particular system;

4.1.6. Implement secure access control measures that:

4.1.6.1. Restrict access to records and files containing Personal Information to those who need such information to perform their job's duties; and

4.1.6.2. Assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access that are reasonably designed to maintain the integrity of the security of the access controls;

4.1.7. Use strong encryption in the following situations:

4.1.7.1. When Personal Information is transmitted over a public network;

4.1.7.2. When Personal Information is stored on portable devices; and

4.1.7.3. When Personal Information is stored on removable media and that media is in transit between physical locations;

4.1.8. Provide ongoing employee training with respect to its information security program, the proper use of the computer security system, and the importance of Personal Information security;

4.1.9. Designate responsibility for maintaining Service Provider's comprehensive information security program;

4.1.10. Oversee its third-party service providers by taking reasonable steps to select and retain third-party service providers that are capable of maintaining security measures to protect Personal Information consistent with applicable laws;

4.1.11. Review the scope of its comprehensive security program at least once a year; and

4.1.12. Document responsive actions taken in connection with any incident involving a Security Breach, and mandatory post-incident reviews of events and actions taken, if any, in order to make changes in business practices relating to the protection of Personal Information.

5. Security Breach

5.1. Service Provider will notify Customer of a Security Breach in the most expedient time possible and without unreasonable delay, subject to any law enforcement delay and taking into account any measures necessary to determine the scope of the Security Breach and restore the reasonable integrity of the data system.

5.2. Service Provider will reasonably cooperate with Customer in any resulting investigation, reporting, or other obligations required by applicable law.

6. Obligations of Customer

6.1. Customer is solely responsible for:

6.1.1. Ensuring that the processing of the Personal Information is in compliance with all applicable laws;

6.1.2. Ensuring that any consents required by law and/or Customer policies and procedures for the collection, access, use, maintenance, and/or disclosure of the Personal Information have been obtained from each individual and entity (including without limitation consumers, business customers, and/or Customer employees and contractors) to whom the Personal Information relates.

6.1.3. Rendering any Personal Information on its systems unusable, unreadable, or indecipherable to unauthorized individuals in accordance with industry standards. Customer acknowledges that it is Customer's responsibility to encrypt all data on Customer's systems and media components prior to providing such Personal Information to Service Provider for any reason.

6.1.4. Establishing the applicable information security safeguards and associated policies for protecting Personal Information in its facilities. Customer must communicate the relevant safeguards and policies to Service Provider with reasonable advance notice and in writing when Service Provider provides services at a Customer facility or accesses Customer's systems.

6.1.5. Promptly informing the Service Provider of any policies that it implements with respect to the processing and protection of Personal Information with express instructions as to how these policies should be implemented by the Service Provider;

6.1.6. Promptly informing the Service Provider of any security breaches with detailed instructions as to how the Service Provider should address the breach.

6.2. Customers located outside the EEA, United Kingdom or Switzerland shall inform the Service Provider before providing it with Personal Information relating to individuals located in the EEA, United Kingdom or Switzerland to ensure that the appropriate privacy protections are applied to that data. For purposes of this Privacy Addendum, the Customer is considered to be located in the country specified in the Quote.

7. Miscellaneous

7.1. No alteration, amendment, or modification of this Privacy Addendum will be valid unless in writing and signed by an authorized representative of both parties.

7.2. Any ambiguity in the terms of this Privacy Addendum will be resolved to permit Service Provider or Customer to comply with applicable laws.

7.3. This Privacy Addendum is the entire and complete agreement between the parties with respect to the privacy and security of Personal Information that is not covered by the GDPR Addendum and supersedes any other agreements, representations, or understandings whether oral or written. To the extent there are any inconsistencies between the terms of this Privacy Addendum and the terms of the Master Agreement, this Privacy Addendum will prevail. Notwithstanding the foregoing, for the sake of clarity, the limitation of liability set forth in the Master Agreement remains in full force and effect and applies to this Privacy Addendum.

7.4. For the sake of clarity, this Privacy Addendum will be subject to the choice of law and dispute resolution procedure set forth in the Master Agreement.