DATA PROCESSING ADDENDUM

SECTION A. GENERAL TERMS

1.1   This Data Processing Addendum ("**DPA**") is supplemental to and may also serve as an update to the Agreement (comprising the Order and Blue Triangle Terms of Use or other written service agreement) ("**Agreement**") between Blue Triangle Technologies and Customer (each, a "**Party,**" and collectively, the "**Parties**") for the provision of the Service and establishes additional responsibilities of the Parties for processing Customer personal information subject to CCPA and/or GDPR regulations.

1.2   This DPA supplements the current Agreement with Customer and will terminate automatically upon termination of the Agreement, unless earlier terminated pursuant to its terms.

1.3   The Customer will act as a single point of contact for its Affiliates with respect to compliance of applicable privacy laws in accordance with this DPA. If BLUE TRIANGLE provides information or notice to the Customer under this DPA, such information or notice will be deemed received by the Customer's Affiliates. The Parties acknowledge and agree that any claims, inquiries, or requests for support in connection with this DPA will be brought by the Customer, whether acting for itself or on behalf of an Affiliate.

1.4   In the event of any conflict between an Order, the DPA and/or the Agreement, the following order of precedence will apply (in descending order): (1) the DPA, (2) the Agreement, and (3) the Order. No other terms or contract relating to Customer personal information will be valid or enforceable.

1.4   Any provision of this DPA that is prohibited or unenforceable shall be ineffective to the extent of such prohibition or unenforceability without invaliding the remaining provisions. The parties will attempt to agree upon a valid and enforceable provision that is a reasonable substitute and then incorporate such substitute provision into this DPA.

SECTION B. CCPA PERSONAL INFORMATION PROCESSING

1. GENERAL

To the extent Blue Triangle is required to Process CCPA Personal Information on behalf of Customer, the following terms in this Section B shall apply.

1.1   Role of the Parties

For the purposes of the CCPA, the Parties acknowledge and agree that Blue Triangle will act as a "Service Provider" as such term is defined in the CCPA, in its performance of its obligations pursuant to this DPA or the Agreement. Blue Triangle shall be referred to as "Service Provider" throughout this Section B. The Customer will act as a single point of contact for its Affiliates and Consumers with respect to CCPA compliance. If Service

Provider gives notice to the Customer, such information or notice will be deemed received by the Customer's Affiliates and Consumers. The Parties acknowledge and agree that any claims in connection with the CCPA under this DPA will be brought by the Customer, whether acting for itself or on behalf of an Affiliate or Consumer.

1.2   Definitions

"**Affiliates**" means the current and future respective affiliated offices of Customer;

"**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code 1798.100 et seq., including any amendments and any implementing regulations thereto that become effective on or after the effective date of this DPA.

"**CCPA Consumer**" means a "consumer" as such term is defined in the CCPA.

"**CCPA Personal Information**" means the "personal information" (as defined in the CCPA) that the Service Provider Processes on behalf of the Customer and/or Customer's Affiliates in connection with the Service Provider's provision of the Service;

"**Data Processing Services**" means the Processing of CCPA Personal Information for any purpose permitted by the CCPA, such as for a permitted "business purpose," as such term is defined in the CCPA, or for any other purpose expressly permitted by the CCPA;

"**Processing**" has the meaning given in the CCPA, and "Process" will be interpreted accordingly;

"**Services**" means the assessment services and any other services provided by Service Provider to the Customer under the Agreement, including the Data Processing Services;

"**Subprocessor**" means any subcontractor engaged by Service Provider who Processes CCPA Personal Information on behalf of Service Provider.

2. CCPA PERSONAL INFORMATION PROCESSING

2.1   Instructions for CCPA Personal Information

Customer and Service Provider agree and acknowledge that Service Provider is authorized to use, retain and disclose CCPA Personal Information for the delivery of Services to Customer in accordance with the Agreement, including: (i) disclosures to Subprocessors; (ii) for Blue Triangle's business purposes and (iii) as authorized by the CCPA. Processing CCPA Personal Information outside the scope of this DPA or the Agreement will require prior written agreement between the Customer and the Service Provider on additional instructions for Processing.

2.2   Required Consents and Notices

The Customer is responsible for complying with the CCPA in connection with the collection, use and storage of CCPA Personal Information and will ensure that it obtains

all necessary consents, and provides all necessary notices, for the lawful Processing of CCPA Personal Information by the Service Provider in accordance with the Agreement.

3. TRANSFER OF CCPA PERSONAL INFORMATION

3.1   No Disclosure of CCPA Personal Information

Except for permitted disclosures to Subprocessors pursuant to similar terms as this DPA, the Service Provider shall not disclose, release, transfer, make available or otherwise communicate any CCPA Personal Information to another business or third party without the prior written consent of the Customer. Notwithstanding the foregoing, nothing in this Agreement shall restrict the Service Provider's ability to disclose CCPA Personal Information to comply with applicable laws or as otherwise permitted by the CCPA.

3.2   No Sale of CCPA Personal Information

The Service Provider shall not Sell any Customer Personal Data to another business or third party without the prior written consent of the Customer.

4. CONSUMER RIGHTS REQUESTS

4.1   CCPA Consumer Rights Requests

On and after the effective date of the CCPA, Service Provider shall comply with all applicable requirements of the CCPA. Subject to a detailed written request by Customer and where possible, Service Provider shall assist Customer with responding to CCPA Consumer Rights Requests as required by applicable CCPA requirements.

4.2   Notice of Requests

The Service Provider shall promptly notify the Customer of any verified request received by the Service Provider from a CCPA Consumer or authorized representative enforcing available rights in respect of the CCPA Personal Information of the CCPA Consumer. Service Provider shall direct such CCPA Consumer or authorized representative to contact the Customer.

SECTION C. GDPR PERSONAL DATA PROCESSING

1. GENERAL

To the extent Blue Triangle is required to Process GDPR Personal Data on behalf of Customer, the following terms in this Section C shall apply.

1.1   Role of the Parties

For the purposes of the EU Data Protection Laws, the Parties acknowledge and agree that Blue Triangle acts as a "Processor" and the Customer and/or Customer's Affiliates act as "Controllers." Blue Triangle shall be referred to as "Processor" throughout this Section C.

2   DEFINITIONS

2.1   Unless otherwise set out below, each capitalized term in this Section C shall have the meaning set out in the Agreement and the following capitalized terms used in this DPA shall be defined as follows:

1. "**GDPR Personal Data**" means the "personal data" (as defined in the GDPR) described in ANNEX 1 and any other personal data that Processor Processes on behalf of Customer or Customer's Affiliate in connection with Processor's provision of the Services;
2. "**EU Data Protection Laws**" means the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council ("GDPR") and all applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the Processing of GDPR Personal Data;
3. "**European Economic Area**" or "EEA" means the Member States of the European Union together with Iceland, Norway, and Liechtenstein;
4. "**Security Incident**" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any GDPR Personal Data;
5. "**Subprocessor**" means any person or legal entity engaged by Processor who agrees to receive from Processor any Customer Personal Data; and
6. the terms "**personal data**", "**Controller**", "**Processor**", "**Data Subject**", "**Process**" and "**Supervisory Authority**" shall have the same meaning as set out in the GDPR.

3   DATA PROCESSING

3.1   Instructions for Data Processing. Processor will only Process Customer Personal Data in accordance with (a) the Agreement, to the extent necessary to provide the Service to the Customer, and (b) the Customer's written instructions, unless Processing is required by European Union or Member State law to which Processor is subject, in which case Processor shall, to the extent permitted by applicable law, inform the Customer of that legal requirement before Processing that GDPR Personal Data. The Agreement (subject to any changes to the Service agreed between the Parties) and this DPA shall be the Customer's complete and final instructions to Processor in relation to the processing of GDPR Personal Data.

3.2   Processing outside the scope of this DPA or the Agreement will require prior written agreement between the Customer and Processor on additional instructions for Processing.

3.3   Required consents. Where required by applicable EU Data Protection Laws, Customer will be responsible for ensuring that all Data Subjects have given/will give all

necessary consents for the lawful Processing of GDPR Personal Data by the Processor in accordance with the Agreement.

3.4   Privacy notices. Customer warrants and represents that:

a. it has provided all applicable notices to Data Subjects required for the lawful Processing of GDPR Personal Data by the Processor in accordance with the Agreement; or

b. in respect of any GDPR Personal Data collected by the Processor on behalf of the Customer, it has reviewed and confirmed the notices provided by the Processor to Data Subjects as accurate and sufficient for the lawful Processing of GDPR Personal Data by the Processor in accordance with the Agreement.

3.5   Indemnity. Customer agrees to indemnify the Processor and its officers, directors, employees, agents, affiliates, successors and permitted assigns (each an "Indemnified Party", and collectively the "Indemnified Parties") against any and all losses, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs, or expenses of whatever kind, including legal fees and court fees, that are incurred by the Indemnified Parties (collectively, "Losses") arising out of any third party claim brought against the Processor relating to or arising out any instructions given by the Customer to the Processor under paragraph 3.1, any failure to obtain the consents under paragraph 3.3, any breach by the Customer of the warranty in paragraph 3.4 or any other breach by the Customer of any EU Data Protection Laws.

4   TRANSFER PERSONAL DATA

4.1   Authorized Subprocessors. The Customer agrees that Processor may use third party infrastructure and support services including Amazon Web Services, Inc, Snowflake Computing and Google Cloud as Subprocessors to Process GDPR Personal Data.

4.2   The Customer agrees that the Processor may use subcontractors to fulfill its contractual obligations under the Agreement. The Processor shall notify the Customer upon Customer request of the identity of any Subprocessors it engages. If the Customer (acting reasonably) does not approve of a new Subprocessor, then without prejudice to any right to terminate the Agreement, the Customer may request that the Provider moves the GDPR Personal Data to another Subprocessor and Processor shall, within a reasonable time following receipt of such request, use all reasonable endeavors to ensure that the Subprocessor does not Process any of the GDPR Personal Data.

4.3   Save as set out in clauses 4.1 and 4.2, the Provider shall not permit, allow or otherwise facilitate Subprocessors to Process GDPR Personal Data without the prior written consent of Customer and unless Processor enters into a written agreement with the Subprocessor which imposes the same obligations on the Subprocessor with regard to their Processing of GDPR Personal Data, as are imposed on the Processor under this DPA.

4.4   Liability of Subprocessors. The Processor shall at all times remain responsible for compliance with its obligations under the DPA and will be liable to the Customer (but only to the Customer) for the acts and omissions of any Subprocessor approved by the Customer as if they were the acts and omissions of Processor.

4.5   Prohibition on Transfers of Personal Data. The Customer acknowledges that the Processor and its Subprocessors will process and host GDPR Personal Data only inside the EEA or Switzerland, and that Processor complies with EU and US data regulations for cross-border data movement.

5   DATA SECURITY, AUDITS AND SECURITY NOTIFICATIONS

5.1   Provider Security Obligations. 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, Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including the measures set out in ANNEX 2.

5.2   Upon request by the Customer, Processor shall make available all information reasonably necessary to demonstrate compliance with this DPA. Contact info for any such requests is to be sent to privacy@bluetriangle.com

5.3   Security Incident Notification. If Processor or any Subprocessor becomes aware of a Security Incident, Processor will (a) notify the Customer of the Security Incident within 72 hours, (b) investigate the Security Incident and provide such reasonable assistance to the Customer (and any law enforcement or regulatory official) as required to investigate the Security Incident, and (c) take steps to remedy any non-compliance with this DPA.

5.4   Processor Employees and Personnel. Processor shall treat the GDPR Personal Data as the Confidential Information of the Customer, and shall ensure that any employees or other personnel have agreed in writing to protect the confidentiality and security of GDPR Personal Data.

6   ACCESS REQUESTS AND DATA SUBJECT RIGHTS

6.1   Data Subject Requests. Save as required (or where prohibited) under applicable law, Processor shall notify Customer of any request received by Processor or any Subprocessor from a Data Subject in respect of their personal data included in the GDPR Personal Data, and shall not respond to the Data Subject.

6.2   Processor shall provide Customer with the ability to correct, delete, block, access or copy the GDPR Personal Data in accordance with the functionality of the Service.

6.3   Government Disclosure. Processor shall notify Customer of any request for the disclosure of GDPR Personal Data by a governmental or regulatory body or law enforcement authority (including any data protection supervisory authority) unless otherwise prohibited by law or a legally binding order of such body or agency.

7   ASSISTANCE

7.1   Where applicable, taking into account the nature of the Processing, and to the extent required under applicable EU Data Protection Laws, the Processor shall provide the Customer with any information or assistance reasonably requested by the Customer for the purpose of complying with any of the Customer's obligations under applicable EU Data Protection Laws, including:

a. reasonable endeavors to assist Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to requests for exercising Data Subject rights laid down in the GDPR; and

b. providing reasonable assistance to the Customer with any data protection impact assessments and with any prior consultations to any Supervisory Authority of the Customer, in each case solely in relation to Processing of GDPR Personal Data and taking into account the information available to Processor.

8   DURATION AND TERMINATION

8.1   Deletion of data. Subject to 8.2 and 8.3 below, Processor shall, within 60 (sixty) days of the date of termination of the Agreement or of the parties' service relationship:

1. make available to Customer a complete copy of all GDPR Personal Data by secure transfer in such a format as notified by Customer to Provider; and
2. delete and use all reasonable efforts to procure the deletion of all other copies of GDPR Personal Data Processed by Processor or any Subprocessors, according to instructions under section 8.2.

8.2   Subject to section 8.3 below, Customer may in its absolute discretion notify Processor in writing within 30 (thirty) days of the date of termination of the Agreement to require Processor to delete and procure the deletion of all copies of GDPR Personal Data Processed by Processor. Processor shall, within 60 (sixty) days of the date of termination of the Agreement:

1. comply with any such written request; and
2. use all reasonable endeavors to procure that its Subprocessors delete all GDPR Personal Data Processed by such Subprocessors, and, where this section 8.2 applies, Processor shall not be required to provide a copy of the GDPR Personal Data to Customer.

8.3   Processor and its Subprocessors may retain GDPR Personal Data to the extent required by applicable laws and only to the extent and for such period as required by applicable laws and always provided that Provider shall ensure the confidentiality of all such GDPR Personal Data and shall ensure that such GDPR Personal Data is only

Processed as necessary for the purpose(s) specified in the applicable laws requiring its storage and for no other purpose.

ANNEX 1

DETAILS OF THE PROCESSING OF GDPR PERSONAL DATA

This ANNEX 1 includes certain details of the processing of GDPR Personal Data as required by Article 28(3) of the GDPR.

Subject matter and duration of the Processing of GDPR Personal Data

The subject matter of the Processing of GDPR Personal Data is the use of and access to the Service by the Customer in accordance with the Agreement.

The duration of the Processing of GDPR Personal Data is the Term, subject to paragraphs 8.2 and 8.3 of this DPA

The nature and purpose of the Processing of GDPR Personal Data

The Processing of GDPR Personal Data provided by Customer to the Processor, or collected by Processor on behalf of the Customer, for the purposes of providing the Service to the Customer.

The types of GDPR Personal Data to be Processed

IP Address, which is also used to determine device geographical information to a city or regional level.

The categories of data subjects to whom the GDPR Personal Data relates

Data collected on behalf of our Customers for analytics information.

The obligations and rights of the Customer

The obligations and rights of the Customer are as set out in this DPA.

ANNEX 2

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

1.   Processor maintains internal policies and procedures, or procures that its Subprocessors do so, which are designed to:

   a. secure any personal data Processed by Processor against accidental or unlawful loss, access or disclosure;

   b. identify reasonably foreseeable and internal risks to security and unauthorized access to the personal data Processed by Processor;

   c. minimize security risks, including through risk assessment and regular testing.

2.   Processor will, and will use reasonable efforts to procure that its Subprocessors conduct periodic reviews of the security of their network and the adequacy of their information security program as measured against industry security standards and its policies and procedures.

3.   Processor will, and will use reasonable efforts to procure that its Subprocessors periodically evaluate the security of their network and associated services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.