Q4 Data Protection Addendum
Controller to Processor Transfers of Personal Data

This Data Protection Addendum ("Addendum") forms part of the Master Subscription Agreement ("Agreement") between: (i) **Q4 Inc.** ("Processor") acting on its own behalf and as agent for each Processor's Affiliate; and (ii)_____ ("Controller") acting on its own behalf and as agent for each Controller Affiliate and is effective as of _____ ("Effective Date").

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Agreement. Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement as amended by, and including, this Addendum.

1. Definitions

1.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "**Applicable Laws**" means (a) European Union or Member State laws with respect to any Controller Personal Data in respect of which any Controller Group Member is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Controller Personal Data in respect of which any Controller Group Member is subject to any other Data Protection Laws;

1.1.2 "**Controller Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Controller, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.3 "**Controller Group Member**" means Controller and/or any Controller Affiliate;

1.1.4 "**Controller Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of a Controller Group Member pursuant to or in connection with the Agreement;

1.1.5 "**Contracted Processor**" means Processor, Affiliate Processor, Subprocessor, Subprocessor Affiliate, sub-subprocessor, sub-subprocessor affiliate, etc.;

1.1.6 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.7 "**EEA**" means the European Economic Area;

1.1.8 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or

superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.9 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.10 "**Processor**" means any person (including any third party and any Processor Affiliate, but excluding an employee of Processor or any of its sub-contractors) appointed by or on behalf of the Controller Process Personal Data on behalf of any Controller Group Member in connection with the Agreement;

1.1.11 "**Processor Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Processor, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.1.12 "**Processor Group Member**" means Processor and/or any Processor Affiliate;

1.1.13 "**Restricted Transfer**" means:

1.1.13.1 a transfer of Controller Personal Data from any Controller Group Member to a Contracted Processor; or

1.1.13.2 an onward transfer of Controller Personal Data from a Contracted Processor to another Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established under section 6.4.3 or 12 below;

For the avoidance of doubt: (a) without limiting the generality of the foregoing, the parties to this DPA intend that transfers of Personal Data from the UK to the EEA or from the EEA to the UK, following any exit by the UK from the European Union shall be a Restricted Transfers for such time and to such extent that such transfers would be prohibited by Data Protection Laws of the UK or EU Data Protection Laws (as the case may be) in the absence of the Standard Contractual Clauses to be established under section 6.4.3 or 12 or an adequacy ruling of the Commission at which time sub-section (b) shall apply to any UK transfer of Personal Data; and (b) where a transfer of Personal Data is of a type authorized by Data Protection Laws in the exporting country, for example in the case of transfers from within the EEA to a country (such as Switzerland and Canada which, as long as applicable, benefit from a ruling of adequacy pursuant to articles 45(9) and 45(3) of the GDPR) or scheme (such as the US Privacy Shield) which is approved by the Commission as ensuring an adequate level of protection or any transfer which falls within a permitted derogation, such transfer shall not be a Restricted Transfer

1.1.14 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Processor for Controller Group Members pursuant to the Agreement;

1.1.15 "**Standard Contractual Clauses**" means the contractual clauses set out in Annex 3, as amended or replaced from time to time by the Commission or such other competent authority as applicable and pursuant to section 13.4;

1.1.16 "**Subprocessor**" means any person (including any third party and any Subprocessor Affiliate, but excluding an employee of Subprocessor or any of its sub-contractors) appointed by or on behalf of the Processor or any Processor Affiliate to Process Personal Data on behalf of any Controller Group Member in connection with the Agreement;

1.1.17 "**Subprocessor Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Subprocessor, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise; and

1.1.18 "**Subprocessor Group Member**" means Subprocessor and/or any Subprocessor Affiliate.

1.2 The terms, "**Commission**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

1.3 The terms, "**Controller**" and "**Processor**" shall, in addition to the definition set out in this Addendum, be supplemented by the meanings as set out in the GDPR.

1.4 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Authority

Processor warrants and represents that, before any Processor Affiliate Processes any Controller Personal Data on behalf of any Controller Group Member, Processor's entry into this Addendum as

agent for and on behalf of that Processor Affiliate will have been duly and effectively authorized (or subsequently ratified) by that Processor Affiliate.

3. Processing of Controller Personal Data

3.1 Processor and each Processor Affiliate shall:

3.1.1 comply with all applicable Data Protection Laws in the Processing of Controller Personal Data; and

3.1.2 not Process Controller Personal Data other than on the relevant Controller Group Member's written instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case Processor or the relevant Processor Affiliate shall to the extent permitted by Applicable Laws

inform the relevant Controller Group Member of that legal requirement before the relevant Processing of that Controller Personal Data.

3.2 Each Controller Group Member:

3.2.1 instructs Processor and each Processor Affiliate (and authorizes Processor and each Processor Affiliate to instruct each Subprocessor and each Subprocessor Affiliate) to:

3.2.1.1 Process Controller Personal Data; and

3.2.1.2 in particular, transfer Controller Personal Data to any country or territory,

as reasonably necessary for the provision of the Services and consistent with the Agreement, Applicable Laws, and this Addendum;

3.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorized to give the instruction set out in section 3.2.1 on behalf of each relevant Controller Affiliate;

3.2.3 warrants and represents that all of its instructions to any Contracted Processor will, at all times, comply with Data Protection Laws.

3.3 Annex 1 to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Controller Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). Controller may, upon 60 days prior written notice, make reasonable amendments to Annex 1 by written notice to Processor from time to time as Controller reasonably considers necessary to meet those requirements.

4. Processor and Processor Affiliate Personnel

Processor and each Processor Affiliate shall, in accordance with Applicable Laws, take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Controller Personal Data through any Processor Group Member, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Controller Personal Data, as strictly necessary for the purposes of the Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. Security

5.1 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, Processor and each Processor Affiliate shall in relation to the Controller Personal Data implement appropriate technical and organizational

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.

5.2 In assessing the appropriate level of security, Processor and each Processor Affiliate shall take into account the particular risks that are presented by Processing, in particular, from a Personal Data Breach.

5.3 The Controller has assessed any security measures specifically agreed in the Agreement and in this Addendum and the Controller confirms that it is satisfied with the security measures in place.

6. Subprocessing

6.1 Each Controller Group Member authorizes Processor and each Processor Affiliate to appoint (and permit each Subprocessor appointed in accordance with this section 6 to appoint) Subprocessors (and sub-subprocessors with regards to Subprocessors) in accordance with this section 6 and, if applicable, any restrictions in the Agreement.

6.2 Each Contracted Processor may continue to use those Contracted Processors already engaged and that are planned to be engaged by the engaging Contracted Processor as at the date of this Addendum, subject to Processor and each Processor Affiliate in each case meeting the obligations set out in section 6.4.

6.3 Processor shall give Controller prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within 30 days of receipt of that notice, Controller objects to the proposed appointment, neither Processor nor any Processor Affiliate shall appoint (or disclose any Controller Personal Data to) that proposed Subprocessor until reasonable steps have been taken to address the objections raised by any Controller Group Member and Controller has been provided with a reasonable written explanation of the steps taken. Processor will use reasonable efforts to make available to Controller a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Subprocessor without unreasonably burdening Customer. If, within 60 days of receipt of the notice, the Processor is unable to make available such change, the Controller may by written notice to Processor terminate the Agreement to the extent that it relates to the Services which require the use of the proposed Subprocessor. Processor will refund Customer any prepaid fees covering the remainder of the term of such terminated Agreement following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Controller. For the avoidance of doubt, Processor undertakes to fulfil the obligations as required by article 28(2) of the GDPR.

6.4 With respect to each relevant Contracted Processor, Processor or the relevant Processor Affiliate shall (and shall procure that each Contracted Processor shall):

6.4.1 before the relevant Contracted Processor first processes Controller Personal Data (or, where relevant, in accordance with section 6.2), carry out adequate due diligence to ensure that the relevant Contracted Processor is capable of providing the level of protection for Controller Personal Data required by the Agreement;

6.4.2 in accordance with Data Protection Laws, take reasonable steps to ensure that the arrangement between the two relevant Contracted Processors, is governed by a written contract including terms which offer at least the same level of

protection for Controller Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR;

6.4.3 subject to section 12 and as reasonably determined by the Processor with respect to which approach the relevant Contracted Processor should take in the relevant circumstance, if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand and on behalf of the Controller and the Controller Affiliates, the Processor and the relevant Contracted Processor; and

6.4.4 upon written requests, provide to Controller for review such copies of the relevant Contracted Processors' relevant data protection agreements (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as Controller may request from time to time.

6.5 Processor and each Processor Affiliate shall, in accordance with Applicable Laws, take reasonable steps to ensure that each relevant Contracted Processor performs the obligations under sections 3.1, 4, 5, 7.1, 8.2, 9 and 11.1, as they apply to Processing of Controller Personal Data carried out by that relevant Contracted Processor, as if it were party to this Addendum in place of Processor.

6.6 The Data Processor will list the approved Subprocessors at https://www.q4inc.com/GDPR/Subprocessors-List. The Controller can, at any time, subscribe to be updated if and when the list is updated pursuant to and in accordance with this Addendum.

7. Data Subject Rights

7.1 Taking into account the nature of the Processing, Processor and each Processor Affiliate shall assist each Controller Group Member by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller Group Members' obligations, as reasonably understood by Controller, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

7.2 Processor shall:

7.2.1 as soon as possible, but in no event more than 5 days from receipt of an applicable Data Subject request, notify Controller if any Contracted Processor receives an applicable request from a Data Subject under any Data Protection Law in respect of Controller Personal Data; and

7.2.2 in accordance with Applicable Laws, take reasonable steps to ensure that the Contracted Processor does not respond to that request except on the documented instructions of Controller or the relevant Controller Affiliate or as required by Applicable Laws to which the Contracted Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Controller of that legal requirement before the Contracted Processor responds to the request.

8. Personal Data Breach

8.1 Processor shall notify Controller without undue delay upon any relevant Contracted Processor becoming aware of a Personal Data Breach affecting Controller Personal Data, providing Controller with sufficient information to allow each Controller Group Member to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

8.2 Processor shall (and shall procure that each relevant Contracted Processor) co-operate with Controller and each Controller Group Member and take such reasonable steps as are directed by Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation

Processor and each Processor Affiliate shall (and shall procure that each relevant Contracted Processor) provide reasonable assistance to each Controller Group Member with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Controller reasonably considers to be required of any Controller Group Member by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Controller Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

10. Deletion or return of Controller Personal Data

10.1 Subject to sections 10.2 and 10.3 Processor and each Processor Affiliate shall (and shall procure that each relevant Contracted Processor), after the date of cessation of any Services involving the Processing of Controller Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those Controller Personal Data without undue delay.

10.2 Subject to section 10.3 prior to the Cessation Date as set out in section 10.1, Controller may in its absolute discretion by written notice to Processor require Processor and each Processor Affiliate to (a) return a complete copy of all Controller Personal Data to Controller by secure file transfer in such format as is reasonably agreed upon between Processor and Controller and the Processor shall procure the return of all copies by any relevant Contracted Processor of those Controller Personal Data.

10.3 Each Contracted Processor may retain Controller 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 any relevant Contracted Processor shall ensure the confidentiality of all such Controller Personal Data and shall, in accordance with Applicable Laws, take reasonable steps to ensure that such Controller Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Law requiring its storage and for no other purpose.

10.4 After the Cessation Date, upon written request by Controller, Processor shall provide written certification to Controller that it and each relevant Contracted Processor has fully complied with this section 10 within 90 days of such written request.

11. Audit rights

11.1 Subject to sections 11.2 to 11.3, Processor and each Processor Affiliate shall make available to each Controller Group Member on request all information reasonably necessary to

demonstrate compliance with this Addendum, and shall allow for and contribute to audits, at the sole cost of the Controller, including inspections, by any Controller Group Member or an auditor mandated by any Controller Group Member in relation to the Processing of the Controller Personal Data by the Processor and/or each Processor Affiliate.

11.2 Except if section 11.3.2 applies and/or in case of an emergency (at which time Controller shall give reasonable notice considering the circumstances and urgency), Controller or the relevant Controller Affiliate undertaking an audit, at the Controller's sole cost, shall give Processor or the relevant Processor Affiliate no less than 30 business days prior notice of any audit or inspection to be conducted under section 11.1 and shall ensure that each of its mandated auditors will not cause any material damage, injury, and/or disruption to the Processor's and/or each Processor Affiliate's premises, equipment, personnel and business while its auditing personnel are on those premises in the course of such an audit or inspection. A Processor and/or each Processor Affiliate need not give access to its premises for the purposes of such an audit or inspection:

11.2.1 to any individual unless he or she produces reasonable evidence of identity and authority;

11.2.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Controller or the relevant Controller Affiliate undertaking an audit has given notice to Processor and/or the relevant Processor Affiliate that this is the case before attendance outside those hours begins; or

11.2.3 for the purposes of more than one audit or inspection, in respect of the Processor and/or any Processor Affiliate, in any 12-month rolling basis, except for any additional audits or inspections which:

11.2.3.1 Controller or the relevant Controller Affiliate undertaking an audit reasonably considers necessary because of genuine concerns as to Processor's and/or the relevant Processor Affiliate's compliance with this Addendum; or

11.2.3.2 A Controller Group Member is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory,

where Controller or the relevant Controller Affiliate undertaking an audit has identified its concerns or the relevant requirement or request in its notice to Processor and/or the relevant Processor Affiliate of the audit or inspection.

12. Restricted Transfers

12.1 Subject to section 12.3, each Controller Group Member (as "data exporter") and each Contracted Processor, as appropriate, (as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from that Controller Group Member to that Contracted Processor.

12.2 The Standard Contractual Clauses shall come into effect under section 12.1 on the later of:

12.2.1 the data exporter becoming a party to them;

12.2.2 the data importer becoming a party to them; and

12.2.3 commencement of the relevant Restricted Transfer.

12.3 Section 12.1 shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from

Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

12.4 subject to section 6.4.3 and as reasonably determined by the Processor with respect to which approach it should take in the relevant circumstance, if it reasonably chooses the approach set out in this section 12.4 with respect to Restricted Transfers, before the commencement of any Restricted Transfer to a Contracted Processor which is not a Processor Affiliate, Processor or Processor Affiliates may enter into the Standard Contractual Clauses with the Controller on behalf of the Contracted Processor. If the Processor chooses to proceed pursuant to this section, Processor warrants and represents that Processor's or the relevant Processor Affiliate's entry into the Standard Contractual Clauses under section 12.1, and agreement to variations to those Standard Contractual Clauses made under section 13.4.1, for and on behalf of that Contracted Processor will have been duly and effectively authorized (or subsequently ratified) by that Contracted Processor.

13. General Terms

Governing law and jurisdiction

13.1 Without prejudice to sections 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses:

13.1.1 the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

13.1.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose, if applicable, in the Standard Contractual Clauses.

Order of precedence

13.2 Nothing in this Addendum reduces Processor's or any Processor Affiliate's obligations under the Agreement in relation to the protection of Personal Data or permits Processor or any Processor Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Agreement. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

13.3 Subject to section 13.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

Changes in Data Protection Laws, etc.

13.4 Controller may:

13.4.1 by at least 90 days' written notice or such other time as the relevant change in or decision of a competent authority under relevant EU Data Protection Law requires for implementation of these legal changes, whichever is greater, from time to time, make any legally required variations to the Standard Contractual Clauses (including any Standard Contractual Clauses entered into under section 12.1 or 6.4.3), as they apply to Restricted Transfers which are subject to a particular EU Data Protection Law, which are required, as a result of any change in, or decision of a competent authority under, that relevant EU Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that relevant EU Data Protection Law; and

13.4.2 propose any other variations to this Addendum which are legally necessary to address the requirements of any EU Data Protection Law.

13.5 If Controller gives notice under section 13.4.1:

13.5.1 Processor and each Processor Affiliate shall promptly co-operate (and in accordance with Applicable Laws, take reasonable steps to ensure that any affected Contracted Processors promptly co-operate) in accordance with applicable EU Data Protection Laws, to take

reasonable steps to ensure that equivalent variations are made to any agreement put in place under section 6.4.3 and 12.1; and

13.5.2 Controller shall not withhold or delay agreement to any reasonably required consequential variations to this Addendum proposed by Processor to protect the Contracted Processors against additional risks associated with the variations made under section 13.4.1 and/or 13.5.1.

13.6 If Controller gives notice under section 13.4.2, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Controller's notice as soon as is reasonably practicable.

13.7 Neither Controller nor Processor shall require the consent or approval of any Controller Affiliate or Processor Affiliate to amend this Addendum pursuant to this section 13.5 or otherwise.

Severance

13.8 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

Liability

13.9 FOR THE PURPOSES OF THIS ADDENDUM ONLY, THE Q4'S LIABILITY UNDER, SECTION 11 OF THE MASTER SERVICE AGREEMENT (https://www.q4inc.com/mca-euro/) SHALL BE INCREASED TO 3X THE AGGREGATE AMOUNT CLIENT HAS PAID TO Q4 HEREUNDER FOR THE SERVICE, THE APPLICATIONS, THE DELIVERABLES AND/OR THE INTELLECTUAL PROPERTY WITH RESPECT TO WHICH THE CLAIM IS MADE DURING THE TWENTY-FOUR (24) MONTH PERIOD PRECEDING THE DATE ON WHICH THE EVENT GIVING RISE TO THE CLAIM OCCURRED. FOR THE AVOIDANCE OF DOUBT, THIS INCREASE SHALL NOT APPLY FOR ANY LIABILITY UNDER THE MCA.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Agreement with effect from the date first set out above.

Company		Company	
Signature		Signature	
Name		Name	Kenneth Szeto
Title		Title	General Counsel
Date		Date	

ANNEX 1: DETAILS OF PROCESSING OF CONTROLLER PERSONAL DATA

This Annex 1 includes certain details of the Processing of Controller Personal Data as required by Article 28(3) GDPR.

Duration of the Processing of Controller Personal Data

Processor will process the Controller Personal Data for as long as it provides services to Controller and/or Controller Affiliates and will hold the Controller Personal Data after that date only as set out in the Agreement and this Addendum, and then only as necessary for its legitimate business purposes.

The subject matter, nature, and purpose of the Processing of Controller Personal Data

All processing activities (including the collection, organization and analysis of Personal Data) as are reasonably required to facilitate or support the provision of the Services described under the Agreement and for the purposes as set out in the Agreement and for no other purposes.

The types of Controller Personal Data to be Processed

The Services under the Agreement may involve the processing of the following types of personal data: First Name, Last Name, Email Address, Company Information, Country, Language, Email Type, Investor Type, Occupation, Position/Title

The categories of Data Subject to whom the Controller Personal Data relates

The data subjects may include individuals named in respect of which Controller or Controller Affiliates has engaged for Processor to provide any services and/or individuals that are beneficiaries of, or have made claims under, or are otherwise involved in the provision of receipt of any such services.

The obligations and rights of Controller and Controller Affiliates

The obligations and rights of Controller and Controller Affiliates are set out in the Agreement and this Annex 1.

ANNEX 2: DETAILS OF TECHNICAL SECURITY MEASURES

As of the Effective Date of this Agreement, Q4, as Data Processor processing Personal Data on behalf of the Data Controller in connection with the Services, shall implement and maintain the following technical and organizational security measures for processing of such Personal Data ("Security Standards"):

1. Physical Access Control: Q4 Inc., as a Data Processor, shall take reasonable measures to restrict physical access, such as security personnel and secured buildings and factory premises, to prevent unauthorized persons from gaining access to Personal Data, or ensure third parties operating data centers on its behalf are adhering to such controls.

2. System Access Controls: Q4, as a Data Processor, shall take reasonable measures to prevent Personal Data from being used without authorization. These controls shall vary based on the nature of the Processing undertaken and may include, among other controls, authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes, and/or logging of access on several levels.

3. Data Access Controls: Q4, as a Data processor, shall take reasonable measures to provide that Personal Data is accessible and manageable only by properly authorized staff, direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the Personal Data to which they have privilege of access.

4. Data Backup: Backups of the databases in the Service are taken on a regular basis are secured and encrypted to ensure that Personal Data is protected against accidental destruction or loss when hosted by Data Processor.

5. Logical Separation: Data from different Processor's subscriber environments is logically segregated on Data Processor's systems to ensure that Personal Data that is collected for different purposes may be processed separately.

6. Transmission Controls: Q4 shall take reasonable measures to ensure that it is possible to check and establish as to which entities the transfer of Personal Data by means of data transmission facilities is envisaged, so that data cannot be read, copied or removed without the authorization during electronic transmission or transport.

7. Input Controls: Data Processor shall take reasonable measures to provide that it is possible to check and establish whether and by whom service data has been entered into data processing systems, modified or removed. Data Processor shall take reasonable measures to ensure that (i) the Personal Data source is under the control of Data Controller; and (ii) Personal Data integrated into the Services is managed by secured transmission from Data Controller.

8. Availability Control: Q4 implements suitable measures designed to ensure that Personal Data are protected from accidental destruction or loss, and that Q4 Inc. can restore the availability and access to Personal Data in a timely manner in the event of a security incident. This is accomplished by (i) Infrastructure redundancy (ii) Scalable architecture design to support large traffic

9. Deletion & Return: Upon Customer's request, or upon termination or expiration of this agreement, Q4 Inc. shall destroy or return to Customer all Personal Data (including copies) in its possession or control (including any Personal Data processed by its Subprocessors). This requirement shall not apply to the extent that Q4 Inc. is required by any applicable law to retain some or all the Personal Data, in which event Q4 Inc. shall isolate and protect the Personal Data from any further processing except to the extent required by such law.

10. Security Measures: Q4 shall ensure that any authorized person is subject to a strict duty of confidentiality (whether a contractual or statutory duty) and that they process the Personal Data only for delivering the Services under the Contract(s) to Customer. Q4 utilizes third party hosting providers that are ISO27001, SOC2 and Privacy Shield certified.

ANNEX 3: STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([1]) for the transfer of personal data to a third country.

(b) The Parties:

the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

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

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 –Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 –Module Two Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 –Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to

mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([4]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account

relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) GENERAL WRITTEN AUTHORISATION: The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 DAYS in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [Where the data exporter 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 the data exporter 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.

[Where the data exporter 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.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([12]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

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

(The data importer agrees to document its legal assessment and any challenge to the request for disclosure

(b) and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of EU Member State in which the data exporter is established.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

ANNEX I to the Standard Contractual Clauses

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s):

_____ with primary offices located at _____. Activities shall be as set forth in the Agreement thereof (controller).

Data importer(s):

Q4, Inc., with address and contact information as set forth in the Agreement. Activities shall be as set forth in the Agreement (processor).

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred shall be as set forth in the Agreement.

Categories of personal data transferred shall be as set forth in the Agreement.

The frequency of the transfer is continuous.

Nature of the processing shall be as set forth in the Agreement.

Purpose(s) of the data transfer and further processing shall be for provision of the Services as set forth in the Agreement.

The period for which the personal data will be retained will be 90 days, or as otherwise agreed between the Parties.

For transfers to (sub-) processors, subject matter, nature and duration of the processing shall also be as set forth in the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, shall be the supervisory authority of an EU member state.

ANNEX II to the Standard Contractual Clauses

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

Description of the technical and organisational 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 shall be as stated in the Agreement.

For transfers to (sub-) processors, description of the technical and organisational 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 shall also be as stated in Agreement.

---

1. Physical Access Control: Q4 Inc., as a Data Processor, shall take reasonable measures to restrict physical access, such as security personnel and secured buildings and factory premises, to prevent unauthorized persons from gaining access to Personal Data, or ensure third parties operating data centers on its behalf are adhering to such controls.

2. System Access Controls: Q4, as a Data Processor, shall take reasonable measures to prevent Personal Data from being used without authorization. These controls shall vary based on the nature of the Processing undertaken and may include, among other controls, authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes, and/or logging of access on several levels.

3. Data Access Controls: Q4, as a Data processor, shall take reasonable measures to provide that Personal Data is accessible and manageable only by properly authorized staff, direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the Personal Data to which they have privilege of access.

4. Data Backup: Backups of the databases in the Service are taken on a regular basis are secured and encrypted to ensure that Personal Data is protected against accidental destruction or loss when hosted by Data Processor.

5. Logical Separation: Data from different Processor's subscriber environments is logically segregated on Data Processor's systems to ensure that Personal Data that is collected for different purposes may be processed separately.

6. Transmission Controls: Q4 shall take reasonable measures to ensure that it is possible to check and establish as to which entities the transfer of Personal Data by means of data transmission facilities is envisaged, so that data cannot be read, copied or removed without the authorization during electronic transmission or transport.

7. Input Controls: Data Processor shall take reasonable measures to provide that it is possible to check and establish whether and by whom service data has been entered into data processing systems, modified or removed. Data Processor shall take reasonable measures to ensure that (i) the Personal Data source is under the control of Data Controller; and (ii) Personal Data integrated into the Services is managed by secured transmission from Data Controller.

8. Availability Control: Q4 implements suitable measures designed to ensure that Personal Data are protected from accidental destruction or loss, and that Q4 Inc. can restore the availability and access to Personal Data in a timely manner in the event of a security incident. This is accomplished by (i) Infrastructure redundancy (ii) Scalable architecture design to support large traffic

9. Deletion & Return: Upon Customer's request, or upon termination or expiration of this agreement, Q4 Inc. shall destroy or return to Customer all Personal Data (including copies) in its possession or

control (including any Personal Data processed by its Subprocessors). This requirement shall not apply to the extent that Q4 Inc. is required by any applicable law to retain some or all the Personal Data, in which event Q4 Inc. shall isolate and protect the Personal Data from any further processing except to the extent required by such law.

10. Security Measures: Q4 shall ensure that any authorized person is subject to a strict duty of confidentiality (whether a contractual or statutory duty) and that they process the Personal Data only for delivering the Services

under the Contract(s) to Customer. Q4 utilizes third party hosting providers that are ISO27001, SOC2 and Privacy Shield certified.

ANNEX III to the Standard Contractual Clauses

LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

The controller has authorised the use of sub-processors as listed below.

As part of Q4's ongoing commitment to the privacy and protection of our customers' personal data, this page lists the subprocessors that we work with currently.

Amazon Web Services, Inc.: Cloud computing and storage

SendGrid, Inc.: Email deployment

MailChimp: Email deployment

Salesforce.com, Inc.: Storage of client agreements & service order forms

The Streaming Network (O24): Webcasting and Conference Calling

Chorus Call: Webcasting and Conference Calling

Macropod Software Pty Ltd (BugHerd): Website Bug Tracking

FullStory, Inc.: Customer Data Experience Logging

Jotform, Inc.: Online form builder

Zendesk, Inc: Online Support Helpdesk platform

Dropbox: File Hosting and Cloud Storage