Data Processing and Information Security Addendum ("Addendum")

THIS ADDENDUM is an addendum to Master Services Agreement between Customer (the “Company” in this Addendum) and Qubit. Each party is referred to as a “Party” and together the “Parties”.

WHEREAS

(A) Qubit has developed and operates certain web-based software applications and digital customer experience delivery platforms (the “Products”) that it makes available via the Internet.

(B) Company wishes to use the Products in its business operations for the purpose of delivering improvements to the online experience of customers of Company (the “Business Purpose”).

(C) Qubit has agreed, or may agree after the date of this Addendum, pursuant to a Services Agreement or otherwise, to supply the Products to Company, which may involve the processing of Customer Data by Qubit (including Personal Data). In so doing, the Parties intend that Company shall be the Controller and Qubit shall be the Processor.

(D) In compliance with the provisions of the General Data Protection Regulation and the applicable national Data Protection Laws, the Parties wish to agree this Addendum.

In consideration of the mutual covenants and undertakings stated herein, THE PARTIES AGREE AS FOLLOWS:

1. DEFINITIONS AND INTERPRETATION

1.1 Definitions:

“Additional Services” means those services undertaken by a Qubit employee or contractor, as may be more particularly described in the Services Agreement.

“Affiliate” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. “Control,” for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

“Authorized Users” means those employees, agents and independent contractors of Company or a Company Affiliate who have been Authorised by Company to use the Products in accordance with the Services Agreement.

“Customer Data” means (i) the Personal Data inputted by Company or any Authorised User, or Qubit on the Company's behalf, for the purpose of using the Products or facilitating Company’s use of the Products, and (ii) Personal Data inputted by and collected from End Users.

“Customer Site” means those properties (including domains and mobile applications) owned and operated by Company or one of its affiliates on which Qubit has agreed to provide the Products, as such properties are more particularly detailed in the Services Agreement.

“Data Protection Laws” means all applicable data protection laws and regulation in the jurisdiction where the Company is located, including Regulation (EU) 2016/679 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, and repealing Directive 95/46/EC (“General Data Protection Regulation”), Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) as the parties anticipate will be replaced by ePrivacy Regulation and applicable local data protection laws.

“**End User**” means an end user of the Customer Site(s).

“Instruction” means an instruction, issued by Company to Qubit, and directing the same to perform a specific action with regard to Personal Data as further set out in Section 3.2 of this Addendum.

“**Personal Data**” means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Customer Data.

“**Personnel**” means all persons authorized to process Personal Data under this Addendum.

“Products” means the products ordered by Company under the Services Agreement, but expressly excluding any third-party products or services.

"**Purposes**" means the purposes for which Qubit Processes Personal Data as listed in Section 2 of this Addendum.

“**Qubit Group**” means Qubit and its Affiliates engaged in the Processing of Personal Data.

"**Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

"**Services**" means Products and Additional Services.

"**Services Agreement**" means the agreement between Company and Qubit relating to the provision of Services, as amended in writing from time to time, and including all schedules, statements of work, addenda and exhibits appended thereto, if any.

"**Sub-Processor**" means any Processor engaged by Qubit or a member of the Qubit Group.

1.2 All capitalised terms used but not defined in this Addendum shall have the meaning ascribed to such terms in the Services Agreement. In the case of conflict or ambiguity between any provision in this Addendum and any provision contained in the Services Agreement, the provision in the Services Agreement shall prevail.

1.3 References to the terms "Processor", "Controller", "Processing", "Processed" and "Data Subject" in this Addendum shall be construed in accordance with the meanings attributed to them in the General Data Protection Regulation.

1.4 Where the words "include", "includes", "including" or "in particular" are used in an Addendum, they are deemed to have the words without limitation following them.

1.5 Unless the context otherwise requires, words in the singular shall include the plural and in the plural shall include the singular.

1.6 A reference to a statute or statutory provision is a reference to it as it is in force as at the date of this Addendum. Such reference shall include all subordinate legislation made as at the date of the Addendum under that statute or statutory provision.

2. SUBJECT-MATTER OF THE PROCESSING

The following Personal Data are Processed by Qubit on behalf of Company under the Addendum:

Type of Personal Data	Nature and Purpose of Processing	Categories of Data Subjects
● Personal Data inputted by Company, Authorised User, or Qubit on Company's behalf	● Use of Products	● Employees of Company or Authorised User
● Data about End Users or mobile application collected by Company and sent to Qubit via a pre-determined data layer implemented by Company, or otherwise transferred to Qubit. Such data may include: o email address o exit feedback o CRM ID o purchase history	● Improvements to the online experience of customers of Company	● End User
● Data on the connection of End User to the website (timestamp, number of pages viewed, IP address)	● Improvements to the online experience of customers of Company	● End User
● Information about the End User's device (e.g OS and version, browser and version, browser settings, IP address)	● Improvements to the online experience of customers of Company	● End User
● Geolocation data inferred from IP address	● Improvements to the online experience of customers of Company	● End User

3. RIGHTS AND OBLIGATIONS OF COMPANY

3.1 Company acknowledges and agrees that:

(a) it is Company's responsibility as Controller to ensure that its use of the Products complies with all Data Protection Laws applicable to Company (including, in particular, in respect of the placing and use of cookies upon which the Products rely and the capturing of any consents required to be obtained from the relevant End User);

(b) if Company requests Qubit to transfer Customer Data (including Personal Data) to a third party, Company is solely responsible and liable for this transfer and in any event, Company shall not act or omit to act in a way which places Qubit in breach of any applicable Data Protection Laws;

(c) Company shall have sole responsibility for the accuracy, quality, integrity, legality, reliability and copyright of all Customer Data. Qubit is under no duty to investigate the completeness, accuracy or sufficiency of the Customer Data, including Personal Data.

(d) Company undertakes not to use the Services to process or request Qubit to process any sensitive personal data or any payment card information.

3.2 Qubit shall Process Customer Data only on Instructions from Company. Company instructs Qubit to Process the types of Personal Data listed in Section 2 of this Addendum and in the Services Agreement for the Purposes. This is the final Instruction of Company to Qubit with regard to the Processing of Customer Data. If Company requests Qubit to Process Customer Data outside the scope of this Addendum, it is Company's obligation to enter into an additional agreement with Qubit and Company will have to bear the costs (if any) for such additional Processing.

3.3 In case of a claim of a Data Subject against Qubit, Company undertakes to assist Qubit with regard to the verification of the active legitimation and subject matter in the defense of the claim.

3.4 Company grants to Qubit the non-exclusive, worldwide right to copy, adapt, transmit, communicate, display, distribute and create compilations and derivative works of the Customer Data for the purpose of providing the Services pursuant to the Services Agreement and to improve or enhance such Services. This licence includes use of Customer Data to compile, use and disclose anonymous, aggregated statistics that include Customer Data, provided that no such information will directly identify and cannot reasonably be used to identify Company or Company's End Users. Company shall be solely responsible for ensuring that Company has obtained all necessary third party consents and made all required disclosures in connection with the foregoing grant.

4. RIGHTS AND OBLIGATIONS OF QUBIT

4.1 Qubit shall Process Personal Data only to the extent, and in such a manner, as is reasonably necessary for the Purposes, and in accordance with the Service Agreement and Company's written Instructions from time to time, unless the exception in Article 28 (3) (a) of the General Data Protection Regulation applies.

4.2 Qubit shall keep a record of any Processing of Personal Data it carries out on behalf of Company and shall only disclose such records to third parties with the prior written consent of Company, unless provided otherwise by applicable law.

4.3 At Company's request and sole expense, Qubit shall provide to Company a copy of all Personal Data held by it under the Addendum in a commonly used and machine-readable format.

4.4 Qubit shall notify Company promptly in writing (and in any event within five (5) working days of receipt) of any communication received from a Data Subject relating to its rights to access, modify, correct, erase or block his or her Personal Data.

4.5 To the extent not prohibited by applicable Data Protection Laws and applicable national laws, Qubit shall notify Company as soon as reasonably practicable in writing of any subpoena or other judicial or administrative order or proceeding seeking access to, or disclosure of, Personal Data. Qubit acknowledges that Company may, at its sole expense, seek to defend against or contest such action in lieu of and on behalf of Qubit.

4.6 Qubit shall assist Company within the scope of its ability to fulfil the requests and claims of Data Subjects laid down in Chapter III of the General Data Protection Regulation and to comply with the obligations pursuant to Articles 32 to 36 of the General Data Protection Regulation. To the extent Company has notification or communication obligations in case of a Security Incident, Qubit undertakes to provide cooperation and support to Company at Company's sole expense.

4.7 Qubit is not obliged to actively monitor Instructions for infringements of Data Protection Laws. Without prejudice to the foregoing, Qubit shall notify the Company immediately upon becoming aware that an Instruction infringes Data Protection Laws.

4.8 Qubit shall comply with its obligation to implement a process for regularly testing, assessing and evaluating

the effectiveness of technical and organizational measures for ensuring the security of the Processing pursuant to Article 32 (1) (d) of the General Data Protection Regulation.

5. SECURITY OBLIGATIONS OF QUBIT

5.1 Qubit shall implement appropriate technical and organizational measures to protect the Customer Data, which shall be designed to meet the requirements of the General Data Protection Regulation (Article 32). In particular, Qubit shall implement technical and organizational measures to provide the on-going confidentiality, integrity, availability and resilience of processing systems and services. The technical and organizational measures are described in Annex 1 to this Addendum. Company has knowledge of these technical and organizational measures and is responsible for ensuring that they provide an appropriate level of protection for the risks of the Customer Data to be Processed. Qubit may update or modify the measures listed in Annex 1 from time to time provided that such updates or modifications do not result in any material degradation of the security of the Customer Data.

5.2 Qubit shall notify Company without undue delay after becoming aware of a Security Incident and assist Company with its third party notification and communication obligations, taking into account the nature of Processing and the information available to Qubit. However, Company is solely responsible for fulfilling any third party notification and communication obligations. Qubit will take, where appropriate, measures to mitigate the possible adverse effects of the Security Incident.

5.3 In the event of any loss or damage to Customer Data, Qubit shall use commercially reasonable endeavors to restore the lost or damaged Customer Data from the latest back-up of such Customer Data maintained by Qubit in accordance with its standard archiving procedures.

5.4 Qubit shall not be responsible for any destruction, loss, alteration or disclosure of Customer Data caused by any third party (except any third parties sub-contracted by Qubit to perform services related to Customer Data maintenance and back-up).

6. PERSONNEL

6.1 Qubit shall provide that access to Customer Data is limited to those Personnel who need access to the Customer Data to meet Qubit's obligations under this Addendum and/or the Services Agreement.

6.2 Qubit shall provide that all Personnel authorized to Process Customer Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7. INFORMATION TO DEMONSTRATE COMPLIANCE

7.1 Qubit shall make available to Company such information as is requested by Company to demonstrate its compliance with applicable statutory obligations, in a commonly used and machine-readable format.

7.2 As of the date of this Addendum, Qubit is certified under ISO 27001. If Company requests to conduct audits, including inspections, Qubit will use external auditors to demonstrate compliance with the obligations laid down in this Addendum. This audit will be performed by a third party auditor annually according to ISO 27001 standards or other standards that are substantially equivalent to ISO 27001 at the selection and expense of Qubit. Qubit will provide the audit report to Company at Company's written request.

7.3 In cases of official requests of data protection authorities with jurisdiction over the Processing hereunder, or, in case Company has reasonable grounds to assume that a Security Incident has taken place, Company may upon at least fourteen days prior written notice to Qubit conduct a site visit of the applicable Qubit operations center at Company's expense by a representative of Company or its independent third party auditor. Such audits shall be carried out at normal business hours without disrupting the on-going business operations of Qubit. Qubit may make the audits dependant on the signing of a nondisclosure agreement with Qubit. If the auditor commissioned by Company is in a competitive relationship with Qubit, Qubit shall have the right to object to Company.

8. SUB-CONTRACTORS

8.1 Company consents that (i) Qubit's Affiliates can be retained as Sub-processors; and (b) Qubit and Qubit's Affiliates shall be entitled to subcontract Qubit's obligations specified in this Addendum to third-party Sub-processors. Qubit or a Qubit Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations no less protective than those contained in this Addendum with respect to the protection of Customer Data to the extent applicable to the nature of the Services provided by such Sub-processor.

8.2 Company approves the Sub-processors identified on the Qubit Infrastructure and Sub-processors list available at: www.qubit.com/infrastructure-and-subprocessors. On the website is a mechanism to subscribe to notifications of new Sub-processors for Services, to which Company shall subscribe, and if Company subscribes, Qubit shall provide notification of a new Sub-processor(s) before authorizing any new

Sub-processor(s) to Process Personal Data in connection with the provision of the Services.

8.3 Company may object to Qubit's use of a new Sub-processor by notifying Qubit promptly in writing within ten (10) business days after receipt of Qubit's notice in accordance with the mechanism set out in Section 8.2. hereof. If Company does not object within the deadline, the consent to the change of Sub-processor shall be deemed to be given. In the event Company objects to a new Sub-processor, as permitted in the preceding sentence, Qubit will use reasonable efforts to make available to Company a change in the Services or recommend a commercially reasonable change to Company's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Company. If Qubit is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Company may terminate the applicable Services Agreement with respect only to those Services which cannot be provided by Qubit without the use of the objected-to new Sub-processor by providing written notice to Qubit. Qubit will refund Company any prepaid fees covering the remainder of the term of such Services Agreement following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Company.

9. LIMITATION OF LIABILITY

The limitation of liability agreed between the Parties in the Services Agreement shall also apply to this Addendum, unless otherwise expressly agreed.

10. TRANSFER MECHANISMS

10.1 Subject to the additional terms in Annex 2 hereof, Qubit makes available the transfer mechanisms listed below which shall apply, in the order of precedence as set out in Section 11.2 hereof, to any transfers of Personal Data under this Addendum from the European Union, the European Economic Area and/or their member states and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations of the foregoing territories, to the extent such transfers are subject to such Data Protection Laws and Regulations:

1. Qubit Group's EU-U.S. Privacy Shield Framework self-certification, subject to the additional terms in Section 1 of Annex 2;

2. The Standard Contractual Clauses set forth in Annex 3 to this Addendum, subject to the additional terms in Section 2 of Annex 2.

10.2 In the event that Services are covered by more than one transfer mechanism, the transfer of Personal Data will be subject to a single transfer mechanism in accordance with the following order of precedence: (1) Qubit's EU-U.S. Privacy Shield Framework self-certification and, (2) the Standard Contractual Clauses.

11. GENERAL

11.1 Upon expiry or termination of the Services Agreement or this Addendum, or upon earlier request by Company, Qubit shall – at the choice of Company - return to Company or securely delete or destroy all Customer Data and existing copies (including Personal Data) in a manner appropriate to the sensitivity thereof, unless applicable Data Protection Laws require storage of the Customer Data. Qubit shall provide written confirmation to Company that the deletion process has been completed.

11.2 The Addendum is an attachment to and integral part of the Services Agreement. This Addendum is the entire agreement between Qubit and Company regarding data protection and privacy issues regarding the Company's use of the Services and supersedes all prior and contemporaneous agreements, proposals or representations, written or oral, concerning its subject matter. Accordingly, any Qubit representations, warranties and covenants in the Services Agreement regarding the privacy, security or disaster recovery measures with respect to the Services or any data submitted to or accessed via the Services, are superseded and replaced hereby.

This Addendum has been entered into on the date first written above.

Annex 1:
Description of the Technical and Organizational Security Measures taken by Qubit

Qubit has implemented the following technical and organizational security measures to provide the ongoing confidentiality, integrity, availability and resilience of processing systems and services:

1. Confidentiality

Qubit has implemented the following technical and organizational security measures to protect the confidentiality of processing systems and services, in particular:

- Qubit processes all customer data on remote server sites owned and operated by industry leading cloud service providers that offer highly sophisticated measures to protect against unauthorized persons gaining access to data processing equipment (namely telephones, database and application servers and related hardware). Such measures include:
  - a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics, and the data center floor features laser beam intrusion detection;
  - data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders;
  - access logs, activity records, and camera footage are available in case an incident occurs;
  - data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training;
  - access to the data center floor is only possible via a security corridor which implements multi-factor access control using security badges and biometrics;
  - only approved employees with specific roles may enter.

- Qubit implements suitable measures to prevent its data processing systems from being used by unauthorized persons. This is accomplished by:
  - automatic time-out of user terminal if left idle, identification and password required to reopen;
  - issuing and safeguarding identification codes, requiring two-factor authentication for all Authorized Users;
  - letting customers define individual user accounts with permissions across Qubit resources;
  - industry standard encryption and requirements for passwords (minimum length, use of special characters, etc.); and
  - all access to data content is logged, monitored, and tracked.

- Qubit's employees entitled to use its data processing systems are only able to access personal data within the scope of and to the extent covered by their respective access permission (authorization). In particular, access rights and levels are based on employee job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities. This is accomplished by:
  - employee policies and training;
  - effective and measured disciplinary action against individuals who access personal data without authorization;
  - limited access to personal data to only authorized persons;
  - industry standard encryption; and
  - policies controlling the retention of back-up copies.

2. Integrity

Qubit has implemented the following technical and organizational security measures to protect the integrity of processing systems and services, in particular:

- Qubit implements suitable measures to prevent personal data from being read, copied, altered or

deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by:

- use of state-of-the-art firewall and encryption technologies to protect the gateways and pipelines through which the data travels;
- industry standard encryption; and
- avoiding the storage of personal data on portable storage media for transportation purposes and on company issued laptops or other mobile devices.

- Qubit does not access any customer content except as necessary to provide that customer with the Qubit products and professional services it has selected. Qubit does not access customers' content for any other purposes. Accordingly, Qubit does not know what content customers choose to store on its systems and cannot distinguish between personal data and other content, so Qubit treats all customer content the same. In this way, all customer content benefits from the same robust Qubit security measures, whether this content includes personal data or not.

3. Availability

Qubit has implemented the following technical and organizational security measures to protect the availability of processing systems and services, in particular:

- Qubit implements suitable measures to provide that personal data is protected from accidental destruction or loss. This is accomplished by:
  - infrastructure redundancy;
  - policies prohibiting permanent local (work station) storage of personal data; and
  - performing regular data back-ups.

4. Resilience

Qubit has implemented the following technical and organizational security measures to protect the resilience of processing systems and services, in particular:

- Qubit designs the components of its platform to be highly resilient. This is accomplished by:
  - selection of best-in-class infrastructure providers with data centers that have daily backups with an assured uptime and availability of 99.9999% by the service providers;
  - geographically distributed data centers to minimize the effects of regional disruptions on global products such as natural disasters and local outages; and
  - in the event of hardware, software, or network failure, platform services and control planes are automatically and instantly shifted from one facility to another so that platform services can continue without interruption.

Annex 2

1. ADDITIONAL TERMS FOR EU-U.S. PRIVACY SHIELD CERTIFICATION

1.1 Qubit Inc. self-certifies to and complies with the EU-U.S. Privacy Shield Framework, as administered by the US Department of Commerce, and shall maintain its self-certification to and compliance with the EU-U.S. Privacy Shield Frameworks with respect to the Processing of Personal Data that is transferred from the European Economic Area to the United States.

2. ADDITIONAL TERMS FOR STANDARD CONTRACTUAL CLAUSES

2.1 The Standard Contractual Clauses and the additional terms specified in this Section 2 of this Annex 2 apply to (i) the legal entity that has executed the Standard Contractual Clauses as a data exporter and, (ii) all Affiliates of Company established within the European Economic Area, Switzerland and the United Kingdom, which have signed Sales Order Forms with Qubit. For the purpose of the Standard Contractual Clauses and this Section 2, the aforementioned entities shall be deemed "data exporters".

2.2 This Addendum and the Services Agreement are Company's complete and final documented instructions at the time of signature of the Service Agreement to Qubit for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed an instruction by the Company to process Personal Data: (a) Processing in accordance with the Services Agreement, applicable Sales Order Form(s) and this Addendum; (b) Processing initiated by Authorized Users in their use of the Services and (c) Processing to comply with other reasonable documented instructions provided by Company (e.g., via email) where such instructions are consistent with the terms of the Services Agreement and this Addendum.

2.3 Pursuant to Clause 5(h) of the Standard Contractual Clauses, Company acknowledges and expressly agrees that (a) Qubit Affiliates may be retained as Sub-processors; and (b) Qubit and Qubit's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services as described in Sections 8 of this Addendum. Qubit shall make available to Company the current list of Sub-processors in accordance with Section 8 of this Addendum. Pursuant to Clause 5(h) of the Standard Contractual Clauses, Company acknowledges and expressly agrees that Qubit may engage new Sub-processors as described in Sections 8 of this Addendum.

2.4 The parties agree that the copies of the Sub-processor agreements that must be provided by Qubit to Company pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by Qubit beforehand; and, that such copies will be provided by Qubit, in a manner to be determined in its discretion, only upon request by Company.

2.5 The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the following specifications:

Upon Company's request, and subject to the confidentiality obligations set forth in the Services Agreement and this Addendum, Qubit shall make available to Company that is not a competitor of Qubit (or Company's independent, third-party auditor that is not a competitor of Qubit) information regarding the Qubit Group's compliance with the obligations set forth in this Addendum in the form of the third-party certifications and audits set forth in the Section 6.2 of this Addendum to the extent Qubit makes them generally available to its customers. Company may contact Qubit in accordance with the "Notices" Section of the Services Agreement to request an on-site audit of the procedures relevant to the protection of Personal Data. Company shall reimburse Qubit for any time expended for any such on-site audit at the Qubit Group's then-current professional services rates, which shall be made available to Company upon request. Before the commencement of any such on-site audit, Company and Qubit shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Company shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Qubit. Company shall promptly notify Qubit with information regarding any non-compliance discovered during the course of an audit.

2.6 The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Qubit to Company only upon Company's request.

2.7 In the event that the Standard Contractual Clauses apply as per Section 11 of the body of this Addendum and there is any conflict or inconsistency between the body of this Addendum and any of its Annexes (not including the Standard Contractual Clauses) and the Standard Contractual Clauses in Annex 3, the Standard Contractual Clauses shall prevail.

ANNEX 3

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organisation:

Address:

Tel.: ; fax: ; e-mail:

Other information needed to identify the organisation:

……

(the data **exporter**)

And

Name of the data importing organisation: Qubit Inc.

Address: 55 West 21st Street, 6th Floor, New York, 10010, United States

Tel.: + 1 415-604-8163; fax: Not applicable; e-mail: legal@qubit.com

Other information needed to identify the organisation: Not applicable

(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the

data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a

summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

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

Signature…….

(stamp of organisation)

On behalf of the data importer:

Name (written out in full):

Position:

Address:

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

Signature…….

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

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

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Data Exporter is (i) the legal entity that has executed the Standard Contractual Clauses as a Data Exporter and, (ii) all Affiliates (as defined in the Addendum) of Company established within the European Economic Area (EEA) and Switzerland that have purchased Services on the basis of one or more Sales Order Form(s).

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Qubit, Inc. is a provider of web-based software applications and digital customer experience delivery platforms (the "Products") which processes personal data upon the instruction of the data exporter in accordance with the terms of the Services Agreement and the Addendum.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Employees of Company or Authorised User
- End Users of data exporter's website

Categories of data

The personal data transferred concern the following categories of data (please specify):

Data exporter may submit Personal Data to the SCC Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- Personal Data inputted by Company, Authorised User, or Qubit on Company's behalf
- Data about End Users of the Company website or mobile application collected by Company and sent to Qubit via a pre-determined data layer implemented by Company, or otherwise transferred to Qubit. Such data may include: email address, exit feedback, CRM ID and purchase history
- Data on the connection of an End User to the website (timestamp, number of pages viewed, IP address)
- Information about the End User's device (e.g OS and version, browser and version, browser settings, IP address)
- Geolocation data inferred from IP address

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Data exporter may submit special categories of data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The objective of Processing of Personal Data by data importer is the performance of the Services pursuant to the

Services Agreement.

DATA EXPORTER

Name:……..…

Authorised Signature ……

DATA IMPORTER

Name:……..…

Authorised Signature ……

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties
Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Data importer will maintain administrative, physical, and technical safeguards for the protection of the security, confidentiality and integrity of Personal Data uploaded to the Services, as described in Annex 1 of this Addendum. Data Importer will not materially decrease the overall security of the Services during a subscription term.

DATA EXPORTER

Name:……..…

Authorised Signature ……

DATA IMPORTER

Name:……..…

Authorised Signature ……