Data Processing Addendum ("Addendum")

THIS ADDENDUM is an addendum to Master Services Agreement between Customer and Qubit entity that is party to the Agreement. If this entity is not Qubit Digital Limited, then Qubit Digital Limited (the "Qubit") is also a party to this Addendum. The signing of the Agreement shall be deemed signing of this Addendum as well. 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) Customer wishes to use the Products in its business operations for the purpose of delivering improvements to the online experience of customers of Customer.

(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 Customer, which may involve the processing of Customer Data by Qubit (including Personal Data). In so doing, the Parties intend that Customer 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 Customer or a Customer Affiliate who have been Authorised by Customer to use the Products in accordance with the Services Agreement.

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Customer Data" means (i) the Personal Data inputted by Customer or any Authorised User, or Qubit on the Customer's behalf, for the purpose of using the Products or facilitating Customer'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 Customer 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 laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom and the United States and its states, applicable to the Processing of Personal Data under the Agreement as amended from time to time.

"**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

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

"Instruction" means an instruction, issued by Customer 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.

"**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Processor**" means the entity which Processes Personal Data on behalf of the Controller., including as applicable any "service provider" as that term is defined by the CCPA.

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

"**Public Authority**" means a government agency or law enforcement authority, including judicial authorities.

"**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 Customer 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 this Addendum shall prevail.

1.3 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.

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

1.5 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 Customer under the Addendum including Processing as reasonably necessary, proportionate, and consistent with business purpose of providing the Services to the extent permitted by applicable Data Protection Laws:

:

Type of Personal Data	**Nature and Purpose of Processing**	**Categories of Data Subjects**
● Personal Data inputted by Customer, Authorised User, or Qubit on Customer's behalf	● Use of Products	● Employees of Customer or Authorised User
● Data about End Users or mobile application collected by Customer and sent to Qubit via a pre-determined data layer implemented by Customer, 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 Customer	● 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 Customer	● 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 Customer	● End User
● Geolocation data inferred from IP address	● Improvements to the online experience of	● End User

	customers of Customer	

3. RIGHTS AND OBLIGATIONS OF COMPANY

3.1 Customer acknowledges and agrees that:

(a) it is Customer's responsibility as Controller to ensure that its use of the Products complies with all Data Protection Laws applicable to Customer (including, in particular, (i) 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), (ii) adhering to any applicable requirement to provide notice to Data Subjects of the use of Qubit as Processor.);

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

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

(e) Customer specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data, to the extent applicable under the CCPA.

3.2 Qubit shall Process Customer Data only on Instructions from Customer. Customer 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 the Customer to Qubit with regard to the Processing of Customer Data. If Customer requests Qubit to Process Customer Data outside the scope of this Addendum, it is Customer's obligation to enter into an additional agreement with Qubit and Customer 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, Customer undertakes to assist Qubit with regard to the verification of the active legitimation and subject matter in the defense of the claim.

3.4 Customer 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 Customer or Customer's End Users. Customer shall be solely responsible for ensuring that Customer 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 Between the parties, regardless of the Qubit entity that is the contracting party of the Agreement, for the purpose of Data Protection Laws and this Addendum, Qubit Digital Limited shall always be the Processor and any other Qubit Affiliate is the Sub-processor. Where the Qubit entity that is a party to the Agreement is not Qubit Digital Limited, that Qubit entity is carrying out the obligations on behalf of Qubit Digital Limited hereunder.

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

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

4.4 To the extent not prohibited by applicable Data Protection Laws and applicable national laws, Qubit shall notify Customer 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 Customer may, at its sole expense, seek to defend against or contest such action in lieu of and on behalf of Qubit.

4.5 Qubit shall, to the extent legally permitted, promptly (and in any event within five (5) working days of receipt) notify Customer if Qubit receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making, each such request being a "Data Subject Request", or any other. Taking into account the nature of the Processing, Qubit shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to a Data Subject Request under Data Protection Laws. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Qubit shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such

Data Subject Request, to the extent Qubit is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws. To the extent legally permitted, Customer shall be responsible for any costs arising from Qubit's provision of such assistance

4.6 Qubit shall assist Customer within the scope of its ability to comply with Customer's obligations pursuant to Articles 32 to 36 of the General Data Protection Regulation and UK GDPR (as applicable) taking into account the nature of processing and the information available to Qubit.

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 Customer 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 and UK GDPR (as applicable).

5. SECURITY OBLIGATIONS OF QUBIT

5.1 Qubit shall implement appropriate technical and organizational measures to protect the Customer Data as described in the Annex 1. In particular, Qubit shall implement technical and organizational measures to provide the on-going confidentiality, integrity, availability and resilience of processing systems and services (including protection against (i) unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data, (ii) retaining, using, disclosing, or selling the Personal Data (a) for a commercial purpose other than providing the Services and as specified by Customer's documented instructions; or (b) outside of the direct business relationship between the Customer and Qubit). Customer 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 Customer without undue delay after becoming aware of a Security Incident and assist Customer with its third party notification and communication obligations, taking into account the nature of Processing and the information available to Qubit. However, Customer 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. In addition to the extent Customer has notification or communication obligations in case of a Security Incident, Qubit undertakes to provide reasonable cooperation and support to Customer at Customer's sole expense.

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 for Qubit Sub-processors).

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 Customer such information as is requested by Customer 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 Customer 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 Customer at Customer's written request.

7.3 In cases of official requests of data protection authorities with jurisdiction over the Processing hereunder, or, in case Customer has reasonable grounds to assume that a Security Incident has taken place, Customer may upon at least fourteen days prior written notice to Qubit conduct a site visit of the applicable Qubit operations center at Customer's expense by a representative of Customer 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 Customer is in a competitive relationship with Qubit, Qubit shall have the right to object to Customer.

8. SUB-PROCESSORS

8.1 Customer 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, in substance, 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 Customer consents to the Sub-processors identified on the Qubit Infrastructure and Sub-processors list available at: www.qubit.com/infrastructure-and-subprocessors, including their locations and processing activities. The website includes a mechanism to subscribe to notifications of new Sub-processors for Services and if Customer 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 Customer may object to Qubit's use of a new Sub-processor by notifying Qubit promptly in writing within ten (10) business days of receipt of Qubit's notice in accordance with the mechanism set out in Section 8.2. hereof. If Customer does not object within the deadline, the consent to the change of Sub-processor shall be deemed to be given. If Customer objects to a new Sub-processor, as permitted in the preceding sentence, Qubit will use reasonable efforts to make available to Customer 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 Sub-processor without unreasonably burdening the Customer. If Qubit is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer 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 Customer 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 Customer.

8.4 Qubit shall be liable for the acts and omissions of its Sub-processors to the same extent Qubit would be liable if performing the services of each Sub-processor directly under the terms of this DPA.

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 Qubit shall ensure that any transfer of Personal Data by Qubit or Qubit's Sub-Processors to countries outside the European Economic Area, and the United Kingdom shall be performed only under conditions outlined in the GDPR or UK GDPR (if applicable), specifically their Section V.

11. GENERAL

11.1 Upon expiry or termination of the Services Agreement or this Addendum, or upon earlier request by Customer, Qubit shall – at the choice of Customer - return to Customer 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. Upon request, Qubit shall provide written confirmation to the Customer 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 Customer regarding data protection and privacy issues regarding the Customer'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 as part of the Agreement between parties and shall be effective upon Effective Date of the Agreement.

DocuSigned by:
Steve Harris
3398638F949A430...

Date: 9/29/2021
Name: Steve Harris
Position: CFO
Company: Qubit Digital Limited

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.