

ON24 DATA PROCESSING ADDENDUM

This Data Processing Addendum (“Addendum”) is entered into by and between ON24 Inc., on behalf of itself and its Affiliates (“ON24”), and Client, on behalf of itself and its Affiliates (“Client”), and is effective as of the date on which Client signs this Addendum (the “Effective Date”).

1. Background

- 1.1 ON24 operates a content delivery platform that enables its business customers to create, manage, host and deliver webcasts and other content, as well as virtual events and environments, to send emails and communications to registrants, attendees and other end users, and to collect registration and other information from registrants, attendees and other end users (the “Platform”). In operating and providing the Platform, ON24 will provide services to its business customers relating to their use of the Platform (the “Services”). This Addendum applies to the Processing (defined below) of Client Personal Data (defined below), pursuant to the Services, including Personal Data received from the European Economic Area (“EEA”), the United Kingdom in the event the United Kingdom exits the European Union, and Switzerland.
- 1.2 This Addendum forms a part of the ON24 Universal Terms and Conditions, and any Master Services Agreement, Subscription Agreement, Services Agreement, Work Order, and other written or electronic agreement between ON24 and Client related to Client’s purchase of Services and ON24’s provision of the same, and any amendments thereto (collectively, the “Agreement,” which also includes any amendments hereto).
- 1.3 This Addendum supersedes any prior data processing agreements, data processing addenda or similar terms between the parties. In the event of any conflict or inconsistencies between the terms of this Addendum and any other terms in the Agreement, this Addendum will control.

2. Execution

- 2.1 To make this Addendum a part of the Agreement, Client must enter the Client-related information in the signature box below, have an authorized representative of Client sign this Addendum, and email it to ON24 at privacy@on24.com.
- 2.2 This Addendum will be considered a legally binding addendum to the Agreement once it has been signed by both ON24 and an authorized representative of Client, and such fully executed version is emailed to ON24 at privacy@on24.com. This Addendum is not valid or enforceable where signed by a Client or other entity that is not a party to an unexpired, valid and enforceable Agreement directly with ON24.

3. Certain Definitions

- 3.1. In this Addendum, the following terms will have the meanings set out below:
 - (a) “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;
 - (b) “Brexit” means any full or partial departure of the United Kingdom from the European Union;
 - (c) “CCPA” means California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100–1798.199), as amended or superseded from time to time;
 - (d) “Client Affiliate” means any Affiliate of Client that is authorized and/or permitted to use the Platform or Services pursuant to the Agreement;
 - (e) “Client Materials” means any materials or data Client enters into, collects, manages or creates using the Platform, including, but not limited to, slides, audio files, video files, photographs, and recordings generated from a Client Event;

- (f) “Client Personal Data” means any Personal Data Processed by ON24 or a Subprocessor in the provision of the Services to Client or a Client Affiliate, including (but not limited to) any contact information or other personally identifiable information of End Users of Client Events or contained in Client Materials;
- (g) “Data Breach” means accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Client Personal Data transmitted, stored or otherwise Processed by ON24 or its Subprocessors;
- (h) “Data Protection Laws” means any local, national or international laws, rules and regulations related to privacy, security, data protection, and/or the Processing of Personal Data, as amended, replaced or superseded from time to time, including: (i) the GDPR and laws of EEA Member States implementing or supplementing the GDPR; and (ii) any data protection laws of the United Kingdom substantially amending, replacing or superseding the GDPR in whether or not as a result of a Brexit (including the UK Data Protection Act 2018);
- (i) “End User” means an actual and prospective attendee, visitor and other user who has registered for or attended one or more Client Events;
- (j) “Client Event” means the webcasts, webinars, virtual environments, and other content offered or made available through the Platform by Client or Client Affiliate;
- (k) “GDPR” means EU General Data Protection Regulation 2016/679;
- (l) “Personal Data” is any information defined as “personal data”, “personal information”, or other similar terms under applicable Data Protection Laws;
- (m) “Process” means any operation or set of operations that is performed upon Client Personal Data, whether or not by automatic means, such as access, collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, return or destruction, and “processed,” or “processing” will be construed accordingly;
- (n) “Restricted Transfer” means a transfer of Client Personal Data to or by ON24 and/or a Subprocessor, to a jurisdiction that is not recognized as providing an adequate level of protection for Personal Data by applicable Data Protection Laws;
- (o) “Standard Contractual Clauses” means the standard contractual clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of protection of data subjects, which have been approved by the European Commission as adducing adequate safeguards for Restricted Transfers, or any successor clauses thereto or alternative data transfer mechanisms recognized by the European Commission pursuant to Article 46 of the GDPR, or by an equivalent competent authority to or of any equivalent contractual clauses approved by it or by another competent authority under another Data Protection Law;
- (p) “Subprocessor” means any person or entity (including any third party and any ON24 Affiliate, but excluding an employee of ON24) appointed by or on behalf of ON24 who may Process Client Personal Data;
- (q) “Supervisory Authority” means (a) an independent public authority established by a Member State pursuant to Article 51 of the GDPR; and (b) any similar regulatory authority responsible for the enforcement of Data Protection Laws; and
- (r) The terms “Data Controller,” “Data Processor,” “Data Subject,” and “Member State,” will have the same meaning as in the GDPR.
- (s) The term “Consumer” will have the same meaning as in the CCPA.

3.2. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

4. Processing of Personal Data

4.1. The parties acknowledge and agree that with regard to the Processing of Client Personal Data, Client is the Data Controller, and ON24 is the Data Processor.

4.2. ON24 will, and will ensure that Subprocessors will Process Client Personal Data only on Client's documented instructions, or where Processing is required by applicable laws to which ON24 or Subprocessors are subject; in the latter case, ON24 will notify the Client of the legal requirement before Processing, unless the law prohibits such notification.

4.3. Client on its own behalf and as agent for each relevant Client Affiliate instructs ON24 (and authorizes ON24 to instruct each Subprocessor) to, as reasonably necessary for the provision of the Services (including any additional services used by Client or Client Affiliate, which may be subject to supplemental terms): (a) Process Client Personal Data; (b) transfer Client Personal Data to any country or territory provided such complies with Section 12 (Cross-border Transfers) below; and (c) engage any Subprocessors, provided such complies with Section 11 (Subprocessing) below.

4.4. Pursuant to, and as required under the CCPA, ON24 will process Client Personal Data to the extent necessary to provide the Services described in the Agreement and only for the purposes as instructed by Client in a manner consistent with this Addendum. ON24 will not retain, use, or disclose such Client Personal Data for any purpose other than to perform the Services, which for the avoidance of doubt prohibits ON24 from retaining, using, or disclosing Client Personal Data outside of the direct business relationship with Client or for any other commercial purpose. ON24 will not sell, rent, release, disclose, disseminate, make available, transfer or otherwise communicate such Client Personal Data to any third party for monetary or other valuable consideration. ON24 certifies that it understands the restrictions set out in this Section 4 and will comply with them. Client agrees that ON24 may de-identify or aggregate Client Personal Data and other data related to the Services to render it Anonymous Data, which may then be used for the purposes of operating and improving ON24's services and operations, and other research, analytics and related purposes. ON24 may maintain Anonymous Data as part of its own records and information, and such data shall no longer be subject to the Agreement or this Addendum. "Anonymous Data" means data that has been de-identified and/or aggregated with other data to such an extent that Client and Client Affiliates are no longer identifiable, and individuals are no longer identified, identifiable, linked or linkable, or otherwise ascertainable by reference to or combination with other datasets.

4.5. Client agrees that (a) Client's submission of Client Personal Data and instructions for the Processing of Personal Data will comply with Data Protection Laws and Client will at all relevant times remain duly and effectively authorized to give the instruction set out in this Section (Processing of Personal Data) on behalf of each relevant Client Affiliate; (b) Client and any Client Affiliate will, in the use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws; and (c) Client will provide any required notices to and obtain any required consents from Data Subjects related to the Processing of Client Personal Data as contemplated in this Addendum and the Agreement, or as otherwise instructed by Client.

4.6. Annex 1 to this Addendum sets out the subject matter and duration of the Processing, the nature and purpose of the Processing, and the categories of Personal Data and Data Subjects, as required by Article 28(3) of the GDPR; Annex 1 does not confer and rights or obligations on either party. Either of the parties may make reasonable amendments to Annex 1 as they reasonably consider necessary to meet the requirements of Article 28(3) of the GDPR by providing the other party with an updated or an additional Annex 1.

5. ON24 Personnel

ON24 will take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to Client Personal Data, ensuring that such individuals are subject to confidentiality obligations or professional or statutory obligations of confidentiality.

6. Security

ON24 will implement appropriate technical and organizational measures, as set forth in Annex 2 (Technical and Organizational Measures), that are designed to provide a level of security appropriate to the risks presented by the Processing of Client Personal Data. In assessing the appropriate level of security, ON24 will take account in particular of the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

7. Personal Data Breach

ON24 will notify Client without undue delay if it discovers a Data Breach involving Client Personal Data, and will provide information (as available) to assist Client to meet any obligations to report a Data Breach under the Data Protection Laws. ON24 will co-operate with Client and take such reasonable steps as are agreed in good faith by the parties to assist in the investigation, mitigation and remediation of each Data Breach. To the extent that Client is responsible for a Personal Data Breach Client will reimburse ON24 for all costs reasonably and properly incurred by ON24 performing its obligations under this Section (including internal costs and third party costs including legal fees).

8. Data Subject and Consumer Rights

ON24 will promptly notify Client if it receives a request from a Data Subject or Consumer entitled to exercise a request under applicable law regarding Client Personal Data as it pertains to that Data Subject or Consumer. Upon request, ON24 will provide Client with reasonable assistance as necessary to Client's fulfilment of its obligations under applicable laws to respond to such requests relating to their Personal Data. Taking into account the nature of the Processing, such assistance will include, where practicable, implementation of reasonable and appropriate technical and organizational measures to allow Client to respond effectively to such requests.

9. Data Protection Impact Assessment and Prior Consultation

Upon request and subject to the nature of the relevant Processing by and information available to ON24, ON24 will provide reasonable assistance to Client with any data protection impact assessments and any prior consultations to any Supervisory Authority, which are required under applicable Data Protection Law. Client will reimburse ON24 in full for all costs reasonably and properly incurred by ON24 in performing its obligations under this Section (including internal costs and third party costs including legal fees).

10. Audit Rights

10.1 Upon Client's written request, ON24 will make available to Client information reasonably necessary to demonstrate ON24's compliance with this Addendum, and will allow for and contribute to inspections by a qualified, independent third-party auditor appointed by Client, in relation to the Processing of Client Personal Data by ON24 or its Subprocessors.

10.2 Client will give ON24 reasonable notice of any audit or inspection to be conducted under this Section and will (and ensure that each of its mandated auditors will) take all reasonable steps to avoid causing any damage, injury or disruption to the premises, equipment, personnel and business of ON24 or any Subprocessor during the course of such an audit. Except as otherwise required by applicable law or a relevant Supervisory Authority, any audit or inspection will be conducted within normal business hours no more than once in any calendar year. Client will reimburse ON24 in full for all costs reasonably and properly incurred by ON24 performing its obligations under this Section (including internal costs, third party costs including legal fees, and costs incurred by ON24 with respect to audits of other Subprocessors). Any information obtained under this Section will be kept confidential and not disclosed to any person without the express consent of ON24, and Client will ensure that any auditor, agent, personnel or other person or entity that participates in such audit is subject to appropriate written confidentiality obligations.

11. Subprocessing

11.1 Client authorizes ON24 to appoint (and permit each Subprocessor appointed in accordance with this Section to appoint) Subprocessors. Client expressly agrees that ON24 Affiliates may be engaged as Subprocessors,

and that ON24 may continue to use those other Subprocessors already engaged by ON24 as of the date of this Addendum. ON24 will make available a current list of ON24 Subprocessors at www.on24.com/about-us/gdpr/subprocessors, including the names and a description of the Processing to be undertaken by the Subprocessor, and will update the list prior to adding any additional Subprocessors. Client may subscribe to email notifications of new Subprocessors at www.on24.com/about-us/gdpr/subprocessors. ON24 will provide notice of new Subprocessors prior to authorizing new Subprocessors to Process Personal Data in connection with the Services by updating the Subprocessor list at www.on24.com/about-us/gdpr/subprocessors via email notification if Client has subscribed to email notifications about new Subprocessors. Client may object to the appointment of a new Subprocessor by sending written notice to ON24 at privacy@on24.com within ten (10) business days of the notice of new Subprocessors; Client's notice of objection should state the basis for Client's objection. Client agrees that it will not unreasonably object to the use of a Subprocessor. If Client does not object to the appointment of the Subprocessor within ten (10) business days, the Client shall be deemed to have approved and agreed to such appointment.

11.2 The parties will work in good faith to resolve Client's objections to the appointment of any Subprocessors. During this time, there may be an impact to the provision of the Services; Client agrees that ON24 is not liable for any such impact. If the parties are unable to resolve Client's objection within 90 days, Client may terminate without penalty the portion of the Agreement pertaining to the Services that ON24 states it cannot provide without the use of the objected-to Subprocessor, and ON24 will refund Client any prepaid but unused amounts for such portion; otherwise the Agreement shall remain in full force and effect.

11.3 With respect to each Subprocessor, ON24 will: (a) exercise commercially reasonable care in the assessment, appointment and oversight of the relevant Processing activities of Subprocessors; (b) include terms in the contract between ON24 and each Subprocessor which offer an equivalent level of protection for Client Personal Data as those set out in this Addendum, taking into account the nature of the services performed by the Subprocessor; (c) if the arrangement involves a Restricted Transfer, ensure that adequate contractual measures are in place as required by Data Protection Laws, and where the Client Personal Data is from the EEA or Switzerland the Standard Contractual Clauses will be incorporated into the agreement between ON24 and the Subprocessor; and (d) remain liable to the Client for any failure by each Subprocessor to fulfil its obligations in relation to the Processing of Client Personal Data.

12. **Cross-border Transfers**

Client and ON24 will execute the Standard Contractual Clauses attached hereto as Annex 3, which will apply with respect to any information originating within the EEA and Switzerland.

13. **Deletion or Return of Personal Data**

Upon the termination or expiration of the Agreement (unless continued Processing is subject to a new or amended agreement) and to the extent not prohibited by applicable law, ON24 will within 90 days (the "Cessation Date") cease Processing and delete or return the Client Personal Data. If Client does not inform ON24 of its choice of either return or deletion of such Client Personal Data at least 30 days prior to the Cessation Date, then Client will be deemed to have chosen deletion. The parties agree that ON24 is not required to return or delete any Anonymous Data at the conclusion of the Agreement.

14. **Limitation of Liability**

The aggregate liability of ON24 arising out of or related to this Addendum, whether in contract, tort or under any other theory of liability, is subject to the limitations on liability in the Agreement.

15. **General Terms**

15.1 **No Legal Advice.** Notwithstanding anything to the contrary in this Addendum, ON24 will not be required to provide legal advice to Client and nothing provided by ON24 will be construed by Client as legal advice.

15.2 **Termination.** The parties agree that this Addendum and the Standard Contractual Clauses will terminate automatically upon: (a) termination of the Agreement; or (b) expiry or termination of all service contracts entered into by ON24 with Client pursuant to the Agreement; or (iii) termination or completion of statements of work, work orders or similar documents, thereunder, whichever is later.

- 15.3 Third Party Rights. A person who is not a Party to this Addendum will have no right to enforce any term of this Addendum; the rights to rescind or vary this Addendum are not subject to the consent of any other person.
- 15.4 Business Interest Cloud. Client hereby elects, and expressly requests and consents, to participate in the ON24 Business Interest Cloud feature, as part of the Services, and agrees to the Business Interest Cloud Terms and Conditions set forth at <http://www.on24.com/bic-terms/>.
- 15.5 Changes in Data Protection Laws. If any variation is required to this Addendum (including the Standard Contractual Clauses) as a result of a change in Data Protection Law, either party may provide written notice to the other party of that change in law. The parties will discuss and negotiate in good faith any necessary variations to this Addendum to address such changes.
- 15.6 Severance. Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum will remain valid and in force. The invalid or unenforceable provision will be either (a) 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.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Agreement as of the Effective Date.

Client Legal Name: _____


Signature _____

Name _____

Title _____

Date Signed _____

ON24, Inc. _____

Signature  _____

Name A7E442E99E554BB...
Steven Vattuone _____

Title CFO _____

Date Signed 7/16/2020 _____

ANNEX 1: DETAILS OF PROCESSING OF CLIENT PERSONAL DATA

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

1. Subject matter and duration of the Processing of Client Personal Data:

The subject matter and duration of the Processing of Client Personal Data are set out in the Agreement and this Addendum.

2. The categories of Data Subject to whom Client Personal Data relates:

- Actual and prospective attendees, visitors and other users (i.e., End Users) of Client Events and users of other Client Materials via the Platform
- Client personnel, agents, affiliates, subsidiaries and others who have been authorized to access, manage and use the Platform on Client's behalf ("Authorized Users"), and other Client personnel

3. The nature and purpose of the Processing of Client Personal Data:

- Collection, storage and management of registration and other information from End Users of Client Events and Client Materials
- Facilitate Client's creation, management, hosting, delivery, sharing and distribution of Client Events and Client Materials
- Facilitate reminders, notices, and other email and other communications (including by email) to End Users, and to permit Client to personalize Client Materials, Client Events and communications to End Users
- Manage Platform access by Authorized Users and prevent unauthorized access
- Track attendance by End Users and prevent unauthorized access
- Generate and provide reporting and analytics to Client related to Client Events and other Services
- Support, maintenance and managed services related to Client's Use of the Platform and Services

4. The types of Client Personal Data to be Processed:

- Name, email and other contact details
- Company, position/title, company contact details, and other business information
- Other information Client chooses to or requests ON24 to collect as part of Client Event registration or attendance
- Video, images, audio and other content
- Name, title, company email, and other information requested of Authorized Users
- Client Event analytics and usage statistics

ANNEX 2: TECHNICAL AND ORGANISATIONAL MEASURES

1. Any Processing of Personal Data will take place on data processing systems for which commercially reasonable technical and organizational measures for protecting Personal Data have been implemented. ON24 will maintain reasonable and appropriate technical, physical, and administrative measures to protect Client Personal Data under its possession or control against unauthorized or unlawful Processing or accidental loss, destruction or damage, taking into account the harm that might result from unauthorized or unlawful processing or accidental loss, destruction or damage and the sensitivity of the Client Personal Data.
2. Security measures will be designed to:
 - (a) deny unauthorized persons access to data-processing equipment used for processing Personal Data (equipment access control);
 - (b) prevent the unauthorized reading, copying, modification or removal of media (data media control);
 - (c) prevent the unauthorized input of Personal Data and the unauthorized inspection, modification or deletion of stored Personal Data (storage control);
 - (d) prevent the use of automated data-processing systems by unauthorized persons using data communication equipment (user control);
 - (e) provide that persons authorized to use an automated data-processing system only have access to the Personal Data covered by their access authorization (data access control);
 - (f) enable ON24 to verify and establish to which individuals Client Personal Data have been or may be transmitted or made available using data communication equipment (communication control);
 - (g) enable identification of which Client Personal Data have been put into automated data-processing systems and when and by whom the input was made (input control);
 - (h) prevent the unauthorized reading, copying, modification or deletion of Client Personal Data during transfers of those data or during transportation of storage media (transport control);
 - (i) include commercially reasonable disaster recovery procedures to provide for the continuation of services under the Agreement and backup of Client Personal Data; and
 - (j) include appropriate technical security solutions are implemented and managed to protect the confidentiality, integrity and availability of Client Personal Data.
3. Where appropriate, data will be encrypted in transmission and at rest, using industry-standard cryptographic techniques and secure management of keys.
4. ON24 will take reasonable steps to ensure the reliability of its employees and other personnel having access to Client Personal Data, and will limit access to Client Personal Data to those Personnel who have a business need to have access to such Client Personal Data, and have received reasonable training regarding the handling of Personal Data and Data Protection Laws.
5. On request and subject to written confidentiality obligations, ON24 will provide the Company with access to its relevant data security policies and procedures.

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: ON24, Inc.

Address: 50 Beale Street, Eighth Floor, San Francisco, CA 94105

Tel.:415-369-8000; fax: 415-369-8388; e-mail: legal@on24.com

Other information needed to identify the organisation: N/A

.....
(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 data¹;
- (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.

¹ Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

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 importer²

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;

² Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia*, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

- (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 or 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 Clauses³. 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

³ This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

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): Steven Vattuone

Position: CFO

Address: 50 Beale Street, Eighth Floor, San Francisco, CA 94105

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

Signature  A7E442E99E554BB...

(stamp of organisation)