Tribe Data Processing Agreement (DPA)

This Data Processing Agreement ("Addendum"), applies to agreements between Tribe Technologies Inc ("Tribe"), and entities who subscribe for Tribe's services and who are subject to Applicable Law ("Customer") (collectively referred to as the "Parties"), sets forth the terms and conditions relating to the privacy, confidentiality and security of Personal Data (as defined below) associated with services to be rendered by Tribe to Customer pursuant to the subscription agreement entered into between the Parties (the "Master Agreement").

THESE TERMS (WHICH TOGETHER WITH ANY ONLINE ORDER PROCESS OR ORDER FORM OFFERED BY TRIBE THROUGH THE WEBSITE WHICH INCORPORATE THESE TERMS BY REFERENCE ("ORDER FORM") ARE COLLECTIVELY REFERRED TO AS THE "AGREEMENT") CONTAIN IMPORTANT LIMITATIONS ON REPRESENTATIONS, WARRANTIES, CONDITIONS, REMEDIES AND LIABILITIES THAT ARE APPLICABLE TO THE SERVICES. ACCORDINGLY, YOU SHOULD READ THESE TERMS CAREFULLY BEFORE USING THE SERVICES. EITHER BY CLICKING A BOX INDICATING YOUR ACCEPTANCE OR BY EXECUTING AN ORDER FORM THAT REFERENCES THESE TERMS, YOU AGREE TO THE TERMS HEREOF. IF YOU ARE AN AGENT OR EMPLOYEE OF AN ENTITY YOU REPRESENT AND WARRANT THAT (I) THE INDIVIDUAL ACCEPTING THIS AGREEMENT IS AUTHORIZED TO ACCEPT THIS AGREEMENT ON SUCH ENTITY'S BEHALF AND TO BIND SUCH ENTITY, AND (II) SUCH ENTITY HAS FULL POWER, CORPORATE OR OTHERWISE, TO ENTER INTO THIS AGREEMENT AND PERFORM ITS OBLIGATIONS HEREUNDER. IF YOU DO NOT ACCEPT THESE TERMS, THEN DO NOT USE THE WEBSITE OR ANY OF ITS CONTENT OR SERVICES.

I. Definitions

- (A) "Applicable Law" means all applicable laws and regulations relating to the privacy, confidentiality, security and protection of Personal Data, including, without limitation: the Personal Information Protection and Electronic Documents Act ("PIPEDA"), the European Union ("EU") General Data Protection Regulation 2016/679 ("GDPR"), with effect from 25 May 2018, and EU Member State laws supplementing the GDPR; the EU Directive 2002/58/EC ("e-Privacy Directive"), as replaced from time to time.
- (B) "Data Controller" means a person who alone or jointly with others determines the purposes and means of the Processing of Personal Data.
- (C) "Data Processor" means a person who Processes Personal Data on behalf of the Data Controller.
- (D) "Data Security Measures" means technical and organisational measures that are aimed at ensuring a level of security of Personal Data that is appropriate to the risk of the Processing, including protecting Personal Data against accidental or unlawful loss, misuse, unauthorised access, disclosure, alteration, destruction, and all other forms of unlawful Processing, including measures to ensure the confidentiality of Personal Data.
- (E) "Data Subject" means an identified or identifiable natural person to which the Personal Data pertain.
- (F) "Instructions" means this Addendum and any further written agreement or documentation through which the Data Controller instructs the Data Processor to perform specific Processing of Personal Data.
- (G) "Personal Data" means any information relating to an identified or identifiable natural person Processed by Tribe in accordance with Customer's Instructions pursuant to this Addendum; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- (H) "Personal Data Breach" a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.
- (I) "Process", "Processed", or "Processing" means any operation or set of operations performed upon Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage,

adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- (J) "Services" means the services offered by Tribe and subscribed for by Customer under the Master Agreement.
- (K) "Standard Contractual Clauses" means the agreement executed by and between Customer and Tribe and attached hereto as Exhibit A pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.
- (L) "Sub-Processor" means the entity engaged by the Data Processor or any further Sub-Processor to Process Personal Data on behalf and under the authority of the Data Controller.

II. Roles and Responsibilities of the Parties

- (A) The Parties acknowledge and agree that Customer is acting as a Data Controller, and has the sole and exclusive authority to determine the purposes and means of the Processing of Personal Data Processed under this Addendum, and Tribe is acting as a Data Processor on behalf and under the Instructions of Customer.
- (B) Any Personal Data will at all times be and remain the sole property of Customer and Tribe will not have or obtain any rights therein.

III. Obligation of the Tribe

Tribe agrees and warrants to:

- (A) Process Personal Data disclosed to it by Customer only on behalf of and in accordance with the Instructions of the Data Controller and Annex 1 of this Addendum, unless Tribe is otherwise required by Applicable Law. Tribe shall inform Customer if, in Tribe's opinion, an Instruction provided infringes Applicable Law.
- (B) Ensure that any person authorised by Tribe to Process Personal Data in the context of the Services is only granted access to Personal Data on a need-to-know basis, is subject to a duly enforceable contractual or statutory confidentiality obligation, and only processes Personal Data in accordance with the Instructions of the Data Controller.
- (C) Inform Customer promptly and without undue delay of any formal requests from Data Subjects exercising their rights of access, correction or erasure of their Personal Data, their right to restrict or to object to the Processing as well as their right to data portability, and not respond to such requests, unless instructed by the Customer in writing to do so. Taking into account the nature of the Processing of Personal Data, Tribe shall assist Customer, by appropriate technical and organisational measures and at Customer's cost, insofar as possible, in fulfilling Customer's obligations to respond to a Data Subject's request to exercise their rights with respect to their Personal Data.
- (D) Notify Customer immediately in writing of any subpoena or other judicial or administrative order by a government authority or proceeding seeking access to or disclosure of Personal Data. Customer shall have the right to defend such action in lieu of and on behalf of Tribe. Customer may, if it so chooses, seek a protective order. Tribe shall reasonably cooperate with Customer in such defense.
- (E) Provide reasonable assistance to Customer, at Customer's cost, in complying with Customer's obligations under Applicable Law.
- (F) Maintain internal record(s) of Processing activities, copies of which shall be provided to Customer by Tribe or to supervisory authorities upon request.
- (G) Remain in compliance with GDPR, CCPA, PIPEDA and all other Applicable Laws with respect to any and all of Customer's users while they are using the Tribe Services.

IV. **Data storage and transfers**

- (A) Tribe stores and Processes all data, including Personal Data, in the US and/or Canada. Tribe has and shall continue to enter into any written agreements as are necessary (in its reasonable determination) to comply with Applicable Law concerning any cross-border transfer of Personal Data, whether to or from Tribe.

- (B) Where required in order to comply with applicable Data Protection Laws, the Standard Contractual Clauses attached hereto as Exhibit A and the additional terms set forth in this Section 9.3 shall apply only to Personal Data that is transferred from the EEA to outside the EEA, either directly or via onward transfer, to any country or recipient: (i) not recognized by the European Commission as providing an adequate level of protection for personal data, and (ii) not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for personal data, including but not limited to Binding Corporate Rules for Processors:
- (C) The Standard Contractual Clauses and the additional terms specified in this Section apply to (i) the legal entity that has executed the Standard Contractual Clauses as a data exporter and those of its Affiliates that are subject to the Data Protection Laws if and to the extent Tribe Processes Personal Data for which such Affiliate(s) qualify as the Controller. For purposes of the Standard Contractual Clauses, the aforementioned entities shall be deemed "data exporters";
- (D) Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer agrees that Tribe may engage Sub-processors in connection with the provision of the Services in accordance with Section V below;
- (E) Customer agrees that the copies of the Sub-processor agreements to be provided by Tribe to Customer pursuant to Clause 5(j) of the Standard Contractual Clauses (where applicable) may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by Tribe, and such copies will be provided by Tribe only upon written request by Customer and subject to any obligations of confidentiality to which Tribe may be bound, and further provided, if Tribe is contractually restricted from disclosing any such agreements to Customer, Tribe will use reasonable efforts to require such Sub-processor to permit it to disclose the agreement to Customer; Customer agrees that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Tribe to Customer only if requested by the Customer in writing.

V. Sub-Processing

(A)Tribe shall not share, transfer, disclose, make available or otherwise provide access to any Personal Data to any third party, or contract any of its rights or obligations concerning Personal Data, unless Tribe has entered into a written agreement with each such third party that imposes obligations on the third party that are substantively similar as those imposed on Tribe under this Addendum. Tribe shall only retain third parties that are capable of appropriately protecting the privacy, confidentiality and security of the Personal Data. A list of Tribe's current Sub-Processors are set out at https://tribe.so/subprocessors. Tribe shall provide Customer with thirty (30) days' prior notice before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services, giving Customer reasonable opportunity to object to the appointment of such Sub-processor(s).

Where Customer permits the integration of the Service with third party services, such integration may allow for the transfer of data to such third party (subject to Customer's consent through the configuration of the integration by Customer). Such third parties shall not be considered Sub-Processors for the purpose of this section and it is Customer sole obligation to ensure that it has the appropriate agreements in place with such third party in respect of the processing of such data.

VI. Compliance with Applicable Laws

- (A) Each party covenants and undertakes to the other that it shall comply with all Applicable Laws in the use of the Services.
- (B) Without limiting the above, (i) Customer is responsible for ensuring that it has a lawful basis for the processing of Personal Information in the manner contemplated by this Agreement, and has adequate record of such basis (whether directly or through another third party provider); and (ii) Tribe is not responsible for determining the requirements of laws applicable to Customer's business or that Tribe's provision of the Services meet the requirements of such laws. As between the parties, Customer is responsible for the

lawfulness of the Processing of the Customer Personal Data. Customer will not use the Services in conjunction with Personal Data to the extent that doing so would violate applicable Data Protection Laws.

- (C) If a Data Subject brings a claim directly against Tribe for a violation of their Data Subject rights in breach of Applicable Laws and such claim does not arise from a breach by Tribe of the terms of this Agreement, Customer will indemnify Tribe for any cost, charge, damages, expenses or loss arising from such a claim, to the extent that Tribe has notified Customer about the claim and given Customer the opportunity to cooperate with Tribe in the defense and settlement of the claim. Subject to the terms of the Agreement, Customer may claim from Tribe amounts paid to a Data Subject for a violation of their Data Subject rights caused by Tribe's breach of its obligations under GDPR.

VII. Data Security

(A) Tribe shall develop, maintain and implement a comprehensive written information security program that complies with Applicable Law and good industry practice. Tribe's information security program shall include appropriate administrative, technical, physical, organisational and operational safeguards and other security measures designed to (i) ensure the security and confidentiality of Personal Data; (ii) protect against any anticipated threats or hazards to the security and integrity of Personal Data; and (iii) protect against any Personal Data Breach, including, as appropriate:

- a) The encryption of the Personal Data;
- b) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
- c) The ability to restore the availability and access to the Personal Data in a timely manner in the event of a physical or technical incident; and
- d) A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures adopted pursuant to this provision for ensuring the security of the Processing.

(B) Tribe shall supervise Tribe personnel to the extent required to maintain appropriate privacy, confidentiality and security of Personal Data. Tribe shall provide training, as appropriate, to all Tribe personnel who have access to Personal Data.

(C) Promptly (and in any event within 90 days) following the expiration or earlier termination of the Master Agreement, Tribe shall return to Customer or its designee, if so requested during such period, or if not so requested securely destroy or render unreadable or undecipherable, each and every original and copy in every media of all Personal Data in Tribe's, its affiliates' or their respective subcontractors' possession, custody or control. In the event applicable law does not permit Tribe to comply with the delivery or destruction of the Personal Data, Tribe warrants that it shall ensure the confidentiality of the Personal Data and that it shall not use or disclose any Personal Data after termination of this Addendum.

VIII. Data Breach Notification

(A) Tribe shall promptly inform Customer in writing of any Personal Data Breach of which Tribe becomes aware. The notification to Customer shall include all available information regarding such Personal Data Breach, including information on:

- a) The nature of the Personal Data Breach including where possible, the categories and approximate number of affected Data Subjects and the categories and approximate number of affected Personal Data records;
- b) The likely consequences of the Personal Data Breach; and
- c) The measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Tribe shall cooperate fully with Customer in all reasonable and lawful efforts to prevent, mitigate or rectify such Breach. Tribe shall provide such assistance as required to enable Customer to satisfy Customer's obligation to notify the relevant supervisory authority and Data Subjects of a personal data breach under Articles 33 and 34 of the GDPR, if applicable.

IX. Audit

Tribe shall on written request (but not more than once per year, other than in the event of a breach) make available to Customer such information as may be reasonably necessary to demonstrate compliance with the obligations set forth in this Addendum and, where required by Applicable Law and at the Customer's expense, allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer. Upon prior written request by Customer (provided that it shall be not more than once per year other than in the event of a breach), Tribe agrees to cooperate and, within reasonable time, provide Customer with: (a) audit reports (if any) and all information necessary to demonstrate Tribe's compliance with the obligations laid down in this Addendum; and (b) confirmation that no audit, if conducted, has revealed any material vulnerability in Tribe's systems, or to the extent that any such vulnerability was detected, that Tribe has fully remedied such vulnerability.

X. Governing Law

This Addendum shall be governed by the laws of the jurisdiction specified in the Agreement.

ANNEX 1: SCOPE OF THE DATA PROCESSING

This Annex forms part of the Data Processing Addendum between Customer and Tribe.

The Processing of Personal Data concerns the following categories of Data Subjects:
End users of the Services provided by Tribe to Customer and Customer's administrative users

The Processing concerns the following categories of Personal Data:

- i) Name: To help data subjects identify themselves in the community and let others call them by their names or nicknames
- (ii) External user ID (Optional): To uniquely identify the data subject when the data subject is authenticated
- (iii) Email address: To send email notifications to data subjects
- (iv) Biography: For data subjects to introduce themselves to the community
- (v) Profile Pictures: For data subjects to introduce themselves to the community by uploading their picture or Avatar
- (vi) IP addresses: To log data subjects activities for future reference and to secure the community in case of spam attacks from a certain IP
- (vii) Cookie data: sessionId for authentication purpose and CSRF-Token for security purpose
- (viii) Behavioral Events: To enhance user experience and show the most relevant and recommended content to the data subjects
- (ix) Posts, replies, uploaded files and videos of data subjects: To provide the community services to data subjects.
- (X) such additional ad hoc categories as may be prompted by new fields added by Customer

The Processing concerns the following categories of Sensitive Data:

None.

The Processing concerns the following categories of data Processing activities (i.e., purposes of Processing):

Provision of the Services to Customer

ANNEX 2 - STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

Clause 1

Definitions

For 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 the 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[1]

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;

---

[1] 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.

(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[2]. 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: _____

On behalf of the data importer:

Name (written out in full): Siavash Mahmoudian Bidgoly

Position: CEO

Address: 22 Wellesley St E, Toronto, ON, Canada

Other information necessary in order for the contract to be binding (if any): None

Signature: DocuSigned by: Siavash Mahmoudian Bidgoly 36C6AC04DE7C4A6...

In the absence of signature above, by signing the Order Form to which the terms of the DPA are incorporated or made subject to, the parties will be deemed to have signed this.

Appendix 1 to the Standard Contractual Clauses Description of Processing Activities

This Appendix forms part of the DPA and Standard Contractual Clauses and must be completed and signed by the parties. By signing the Order Form to which the terms of the DPA are incorporated or made subject to, the parties will be deemed to have signed this Appendix 1.

Data exporter

The data exporter is: Customer, a user of the Services.

Data importer

The data importer is: Tribe Technologies, Inc., provider of the Subscription Services.

Data Subjects

See Annex 1 of the DPA.

Categories of data

See Annex 1 of the DPA.

Special categories of data

See Annex 1 of the DPA.

Processing operations

The personal data transferred will be processed in accordance with the Agreement and any Order Form and may be subject to the following processing activities:

- storage, transfer, deletion and other processing necessary to provide, maintain and improve the Services provided to the Data Exporter;
- to provide customer and technical support to the Data Exporter; and
- disclosures in accordance with the Agreement, and as compelled by law.

Appendix 2 to the Standard Contractual Clauses

This Appendix 2 forms part of the DPA and Standard Contractual Clauses and must be completed and signed by the parties. By signing the signature page of the Order Form which refers to the DPA, the parties will be deemed to have signed this Appendix 2.

Technical and organizational security measures implemented by the Data Importer in accordance with Clauses 4(d) and 5(c):

The Data Importer has implemented and will maintain appropriate technical and organisational measures to protect the Personal Data against misuse and accidental loss or destruction as communicated by Data Importer and as updated from time to time by Data Importer.