DATA PROCESSING ADDENDUM

This Data Processing Agreement ("**DPA**") forms part of of the Terms of Service and Privacy Policy ("**Agreement**") by and between **AhaChat LLC** (“**Processor**”) having its place of business at 1942 Broadway St. STE 314C, Boulder, United States of America and _____ having its place of business _____ (“**Customer**”) and shall be effective as of _____ (“**Effective Date**”). Any terms not defined in this Addendum shall have the meaning set forth in the Agreement. In the event of a conflict between the terms and conditions of this Addendum and the Agreement, the terms and conditions of this Addendum shall supersede and control.

WHEREAS

(A) The Customer acts as a Data Controller.
(B) The Customer wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor.
(C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
(D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1 "**Agreement**" means this Data Processing Agreement and all Schedules;

1.1.2 "**Customer Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of Customer pursuant to or in connection with the Principal Agreement;

1.1.3 "**Contracted Processor**" means a Subprocessor;

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

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

1.1.6 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

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

1.1.8 "**Data Transfer**" means:

1.1.8.1 a transfer of Customer Personal Data from the Customer to a Contracted Processor; or

1.1.8.2 an onward transfer of Customer Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.9 "**Services**" means any product or service provided by KDKDW to the Customer according to the Agreement.

1.1.10 "**Subprocessor**" means any person appointed by or on behalf of a Processor to process Personal Data on behalf of the Customer in connection with the Agreement.

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

2. Processing of Customer Personal Data

2.1 Processor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Customer Personal Data; and

2.1.2 not Process Customer Personal Data other than on the relevant Customer's documented instructions.

2.2 The Customer instructs Processor to process Customer Personal Data.

3. Processor Personnel

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

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Customer Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

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

5. Authorized Sub-Processors

5.1 Customer agrees that the Processor may engage with authorized Sub-processors to process Customer Data. The Sub-processors currently engaged by Processor are:

- Google LLC
- Facebook, Inc.
- Stripe, Inc.
- Paddle.com Market Limited.

Customer hereby authorizes these specific Sub-processors.

5.2. A list of Processor's current Authorized Sub-Processors (the "List") will be made available to Controller, either attached hereto, at a link provided to Controller, via email or through other means made available to Controller. Such List which may be updated by Processor from time to time. The List may provide a mechanism to subscribe to notifications of new Authorized Sub-Processors and the Controller agrees to subscribe to such notifications where available. At least ten (10) days before enabling any third party other than Authorized Sub-Processors to access or participate in the Processing of Personal Data, Processor will add such third party to the List. Controller may reasonably object to such an engagement on legitimate grounds by informing Processor in writing within ten (10) days of receipt of the aforementioned notice by Controller. Controller acknowledges that certain sub-processors are essential to providing the Services and that objecting to the use of a sub-processor may prevent Processor from offering the Services to Controller.

5.3. If Controller reasonably objects to an engagement in accordance with Section 5.2, and Processor can't provide a commercially reasonable alternative within a reasonable period of time, Processor may terminate this Addendum. Termination shall not relieve the Controller of any fees owed to the Processor under the Agreement.

5.4. If Controller does not object to the engagement of a third party in accordance with Section 5.2 within ten (10) days of notice by Processor, that third party will be deemed an Authorized Sub-Processor for the purposes of this Addendum.

5.5. Processor will enter into a written agreement with the Authorized Sub-Processor imposing on the Authorized Sub-Processor data protection obligations comparable to those imposed on Processor under this Addendum with respect to the protection of Personal Data. In case an Authorized Sub-Processors fails to fulfill its data protection obligations under such written agreement with Processor, Processor will remain liable to Controller for the performance of the Authorized Sub-Processor's obligations under such agreement.

5.6. If Controller and Processor have entered into Standard Contractual Clauses as described in Section 11 (Data Transfer), (i) the above authorizations will constitute Controller's prior written consent to the subcontracting by Processor of the processing of Personal Data if such consent is required under the Standard Contractual Clauses, and (ii) the parties agree that the copies of the agreements with Authorized Sub-Processors that must be provided by Processor to Controller pursuant to Clause 5(j) of the Standard Contractual Clauses may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by the Processor beforehand, and that such copies will be provided by the Processor only upon request by Controller.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Processor shall assist the Customer by implementing appropriate technical and organisational measures, insofar as this is possible, for he fulfilment of the Customer obligations, as reasonably understood by Customer, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

6.2.1 promptly notify Customer if it receives a request from a Data Subject under any Data Protection Law in respect of CustomerPersonal Data; and

6.2.2 ensure that it does not respond to that request except on the documented instructions of Customer or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Customer of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 Processor shall, to the extent permitted by law, notify Customer without undue delay upon Processor becoming aware of a Personal Data Breach affecting Customer

Personal Data, providing Customer with sufficient information to allow the Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Processor shall cooperate with the Customer and take reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

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

9. Deletion or return of Customer Personal Data

If you are a resident of the EEA, upon termination or expiration of the Agreement, Processor shall delete or return to Customer all Customer Data and copies in its possession or control, save that this requirement shall not apply to the extent Processor is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data Processor shall securely isolate and protect from any further processing, except to the extent required by applicable law.

10. Audit rights

10.1 Subject to this section 10, Processor shall make available to the Customer on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Customer or an auditor mandated by the Customer in relation to the Processing of the Customer Personal Data by the Contracted Processors.

10.2 Information and audit rights of the Customer only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. Data Transfer

11.1 The Customer acknowledges and accepts that Processor may transfer Personal Data processed under this Addendum outside the European Economic Area ("EEA") or Switzerland as necessary to provide the Services.

11.2 If Processor transfers Personal Data protected under this Addendum to a jurisdiction for which the European Commission has not issued an adequacy decision, Processor will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Data Protection Laws.

12. General Terms

12.1 Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law;

(b) the relevant information is already in the public domain.

12.2 Notices. All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

13. Governing Law and Jurisdiction

13.1 This Agreement is governed by the laws of England and Wales.

13.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of England and Wales, subject to possible appeal to the Supreme Court of the United Kingdom in London.

Data Processor

Company name: AhaChat LLC
Company country: Vietnam
Name: Ty Nguyen
Position: CEO

Signature: 

Data Processor (Customer)

Company name:
Company country:
Name:
Position:

Signature: