Aha!

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**"), effective the date of the final signature, forms part of the Terms of Service found at https://www.aha.io/legal/terms_of_service (the "**Agreement**"). The DPA includes this document and Attachments 1-3, all attached hereto.

In the course of providing the Service to Customer pursuant to the Agreement, Aha! may Process Personal Data on behalf of Customer. The purpose of this DPA is to reflect the parties' agreement with regard to the Processing of Personal Data in accordance with the requirements of applicable Data Protection Laws and Regulations.

Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Affiliates. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Affiliates. Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Aha! under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Affiliates.

The terms of the Agreement are incorporated into this DPA. Any capitalized term not defined in this DPA will have the meaning ascribed to that term in the Agreement.

1. DEFINITIONS

"**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.

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

"**Data Processor**" means an entity which engages in the Processing of Personal Data on behalf of the Data Controller.

"**Data Protection Laws and Regulations**" means all local, state, national and/or foreign law, treaties, and/or regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom and the United States, applicable to either: (i) Aha! in its role as service provider Processing data under the Agreement or (ii) Customer and its Affiliates, as the case may be. For the avoidance of doubt, each party is only responsible for the local, state, national and/or foreign law, treaties, and/or regulations applicable to it.

"**Data Subject**" means the individual to whom Personal Data relates.

"**GDPR**" means 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).

"**Personal Data**" means any information relating to an identified or identifiable person that has been provided by or for Customer to the Service or collected and Processed by or for Customer through the Service.

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

"**Standard Contractual Clauses**" means the EU Standard Contractual Clauses pursuant to the European Commission's decision of 4 June 2021, and its Module 2 "Controller to Processor" incorporated herein by reference together with its Appendices, executed by and between Customer and Aha! and attached hereto as Attachment 3.

"**Sub-processor**" means any Data Processor engaged by Aha!

2. PROCESSING OF PERSONAL DATA

2.1 Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Data Controller, Aha! is a Data Processor and that Aha! will engage Sub-processors pursuant to the requirements set forth in Section 4 (Sub-Processors) below.

2.2 Customer's Processing of Personal Data. Customer shall, in its use of the Service, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data, and the means by which Customer acquired Personal Data. Customer shall ensure that the Customer is entitled to transfer the relevant Personal Data to Aha! so that Aha! and its Sub-processors may lawfully use, process, and transfer the Personal Data in accordance with this DPA and the Agreement on Customer's behalf. Aha! shall immediately inform Customer if, in its opinion, an instruction infringes Data Protection Laws and Regulations.

2.3 Aha!'s Processing of Personal Data. Aha! shall only Process Personal Data on behalf of and in accordance with Customer's instructions during the Subscription Term and in accordance with Section 7 (Return and Deletion of Personal Data). Aha! shall treat Personal Data as Confidential Information and ensure that persons Processing the Personal Data are subject to an obligation of confidentiality. Customer instructs Aha! to Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement, which includes updating the Service and preventing or addressing service or technical issues; (ii) Processing initiated by Customer's Subscribers in their use of the Service; and (iii) Processing to comply with other reasonable instructions provided by Customer (e.g., via email or support tickets) where such instructions are consistent with the terms of the Agreement.

2.4 Details of the Processing. The subject-matter and duration of Processing of Personal Data by Aha! is as described in Section 2.3 (Aha!'s Processing of Personal Data). The nature and purpose of the Processing, the types of Personal Data, and categories of Data Subjects Processed under this DPA are further specified in Attachment 2 (Description of Processing Activities) to this DPA.

3. RIGHTS OF DATA SUBJECTS

3.1 Correction, Blocking, and Deletion. To the extent Customer, in its use of the Service, does not have the ability to correct, amend, block, or delete Personal Data, as required by Data Protection Laws and Regulations, Aha! shall comply with any commercially reasonable request by Customer to facilitate such actions to the extent Aha! is legally permitted to do so. To the extent legally permitted, Customer shall be responsible for any costs arising from Aha!'s provision of such assistance.

3.2 Data Subject Requests. Aha! shall, to the extent legally permitted, promptly notify Customer if Aha! receives any requests from a Data Subject to exercise the following Data Subject rights: access, rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, objection to the Processing, or to not be subject to an automated individual decision making (each, a "**Data Subject Request**"). Taking into account the nature of the Processing, Aha! shall assist Customer by appropriate technical and organizational measures, insofar as is reasonably possible, for the fulfillment of Customer's obligation to respond to a Data Subject Request under applicable Data Protection Laws and Regulations. Aha! may respond to Data Subject Requests with information and instructions for the data subject to fulfil their request using available functionality within the service. In addition, to the extent Customer, in its use of the Service, does not have the ability to address a Data Subject Request, Aha! shall, upon Customer's request, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request to the extent Aha! is legally permitted to do so and the response to such Data Subject Request is required under applicable Data Protection Laws. To the extent legally permitted, Customer shall be responsible for any costs arising from Aha!'s provision of such assistance, including any fees associated with the provision of additional functionality.

4. SUB-PROCESSORS

4.1 Appointment of Sub-processors. Customer acknowledges and agrees that (a) Aha!'s Affiliates may be retained as Sub-processors and (b) Aha! and Aha!'s Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Service.

4.2 Identification of Current Sub-processors and Notification of New Sub-processors. A current list of Sub-processors (including their country of location) for the Service is published at https://www.aha.io/legal/subprocessors. Customers can select the 'Follow' button at that location to subscribe to notifications of new sub-processors for the Service. If Customer subscribes, Aha! shall provide notification of a new Sub-processor(s) at least ten (10) business days in advance before authorizing such new Sub-processor(s) to process Personal Data in connection with the provision of the applicable Service.

4.3 Objection Right for New Sub-processors. Customer may reasonably object to Aha!'s use of a new Sub-processor (e.g., making Personal Data available to the specific Sub-processor may violate applicable Data Protection Laws and Regulations) by notifying Aha! promptly in writing within ten (10) days after receipt of Aha!'s notice in accordance with the mechanism set out in Section 4.2. Such notice from Customer shall explain the reasonable grounds for the objection. Upon receipt of such notice, Aha! will use reasonable efforts to make available to Customer a change in the Service or recommend a commercially reasonable change to Customer's configuration or use of the Service to avoid processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Aha! is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Customer may terminate the Account with respect only to that Service which cannot be provided by Aha! without the use of the objected-to new Sub-processor by providing written notice to Aha! Upon such termination, Aha! will refund Customer any prepaid fees covering the remainder of the Subscription Term following the effective date of termination with respect to such terminated Service, without imposing a penalty for such termination on Customer.

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

5. SECURITY

5.1 Controls for the Protection of Personal Data. Aha! shall maintain a comprehensive information security program that includes administrative, physical, and technical safeguards for protection of the security, confidentiality, and integrity of Personal Data that are appropriate to (a) the size, scope, and type of Aha!'s business; (b) the amount of resources available to Aha!; (c) the type of information that Aha! will store; and (d) the need for security and confidentiality of such information. Aha! shall regularly monitor compliance with these safeguards. Aha! will not materially decrease the overall security of the Service during a Subscription Term.

5.2 Third-Party Certifications. A current list of the third-party certifications obtained by Aha! is published at https://www.aha.io/legal/security. Aha! shall maintain its ISO27001 certification during the Subscription Term. Upon Customer's request, and subject to the confidentiality obligations set forth in the Agreement, Aha! shall make available to Customer (or Customer's independent, third-party auditor) information regarding Aha! compliance with the obligations set forth in this DPA in the form of the summary audit report(s) for its current third-party certifications.

6. PERSONAL DATA INCIDENT MANAGEMENT AND NOTIFICATION

Aha! maintains an incident response plan and procedures as part of its third-party certifications. Aha! shall notify Customer without undue delay (no more than 48 hours) of any breach relating to Personal Data (within the meaning of applicable Data Protection Laws and Regulations) of which Aha! becomes aware. Such notification shall include a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned), likely consequences of the breach, mitigating or remedial measures taken in response to the breach, and a contact point for more information related to the breach. Aha! shall provide commercially reasonable cooperation and assistance in identifying the cause of such breach and take commercially reasonable steps to remediate the cause to the extent the remediation is within Aha!'s control. Except as required by applicable Data Protection Laws and Regulations, the obligations herein shall not apply to incidents that are caused by Customer or Other Services.

7. RETURN AND DELETION OF PERSONAL DATA

Upon termination of the Service for which Aha! is Processing Personal Data, Aha! shall delete all Personal Data in Aha!'s possession and securely destroy such Personal Data unless applicable law prevents it from destroying all or part of Personal Data. Upon Customer's request prior to the aforementioned deletion and subject to the technical limitations of the Service, Aha! shall return all Personal Data in its possession.

8. EUROPEAN-SPECIFIC TERMS

8.1 GDPR. Aha! will Process Personal Data in accordance with the GDPR requirements directly applicable to Aha!'s provisioning of the Service.

8.2 Data Protection Impact Assessment. Upon Customer's request, Aha! shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Service, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Aha! Aha! shall provide reasonable assistance to Customer in the cooperation or prior consultation with the supervisory authority, to the extent required under the GDPR.

8.3 Transfer Mechanisms. As of the effective date of this DPA, Aha! self-certifies to and complies with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, as administered by the US Department of Commerce. For transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their member states, the UK, and Switzerland, to countries which do not ensure an adequate level of data protection within the meaning of applicable Data Protection Laws and Regulations of the foregoing territories, to the extent such transfers are subject to such applicable Data Protection Laws and Regulations: (a) Aha!'s EU-U.S. and Swiss-U.S. Privacy Shield Framework self-certifications apply; and (b) The Standard Contractual Clauses set forth in Attachment 3 to this DPA apply, subject to Attachment 1.

To the extent Customer transfers Personal Data from the United Kingdom to Aha! by signing this DPA, Customer and Aha! conclude the UK Standard Contractual Clauses annexed to EU Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under

Directive 95/46/EC, which are hereby incorporated by reference and completed as follows: (i) the “data exporter” is Customer and the “data importer” is Aha!; (ii) the governing law in Clause 9 and Clause 11.3 is the law of the country of the United Kingdom in which Customer is established; (iii) Appendix 1 and Appendix 2 are Annex I and Annex II to this DPA respectively, and (iv) the optional indemnification clause is struck. In addition, the following changes apply: (i) references to Data Protection Law are replaced with references to applicable UK data protection law; (ii) references to the EU or Member States are replaced with references to the United Kingdom, (iii) references to EU authorities are replaced with references to the competent UK authority; and (iv) references to the Member State governing law in Clause 9 and Clause 11.3 of the Standard Contractual Clauses are replaced with references to the law of England and Wales.

9. CALIFORNIA-SPECIFIC TERMS

With reference to the California Consumer Privacy Act, Cal. Civ. Code §1798.100 et seq., and its implementing regulations (“**CCPA**”), the parties acknowledge and agree that Aha! is a “Service Provider” and may receive Personal Data of California consumers pursuant to the business purpose of providing the Service to Customer in accordance with the Agreement. Aha! shall not: (i) sell the Personal Data; (ii) retain, use, or disclose the Personal Data for any purpose other than for the specific purpose of performing the Service, including retaining, using, or disclosing the Personal Data for a commercial purpose other than providing the Service; and (iii) retain, use, or disclose the Personal Data outside of the direct business relationship between Customer and Aha! Aha! certifies that it understands the restrictions in this Section 9 and will comply with them in accordance with the requirements of the CCPA.

10. LEGAL EFFECT

The terms of this DPA will end simultaneously and automatically with the termination of the Agreement, provided however any obligation imposed on Aha! under this DPA in relation to the Processing of Personal Data shall survive any termination or expiration of the Agreement. This DPA is part of and subject to the terms of the Agreement. Customer’s remedies (including those of its Affiliates) with respect to any breach by Aha! of the terms of this Agreement will be subject to any aggregate limitation of liability that applies to the Customer under the Agreement. With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and the Agreement, the provisions of this DPA shall prevail with regard to the parties’ data protection obligations.

IN WITNESS WHEREOF, the parties’ authorized signatories have duly executed this DPA and referenced attachments and appendices:

Customer: ____________________
(Full Legal Entity Name)

By:______________________________

Name:____________________________

Title:_____________________________

Date:_____________________________

Address:__________________________
____

Email:____________________________

Phone:____________________________

AHA! LABS INC.

By:______________________________

Name: ____________________________

Title: ____________________________

Date: ____________________________

Address: 20 Gloria Circle
Menlo Park, CA 94025, USA

Email: support@aha.io

Phone: +1-650-331-3170

Attachment 1

ADDITIONAL TERMS TO THE STANDARD CONTRACTUAL CLAUSES

1. Application of Standard Contractual Clauses. The Standard Contractual Clauses in Attachment 3 and the additional terms in this Attachment 1 will apply to: (a) the Customer that has executed the DPA; and (b) its Affiliates which are authorized to use the Service pursuant to the Agreement. For the purpose of the Standard Contractual Clauses and this Section 1, the aforementioned entities shall be deemed "**Data Exporter**" and Aha! shall be "**Data Importer**." The Standard Contractual Clauses only apply only to Personal Data that is transferred from the European Economic Area (EEA) and Switzerland, to outside the EEA, either directly or via onward transfer, to any country or recipient not recognized by the European Commission as providing an adequate level of protection for personal data.

2. Government and Law Enforcement Orders. Upon receipt of any legally binding order or request for disclosure of Personal Data by a competent government authority or law enforcement authority, Data Importer shall use reasonable efforts to redirect the relevant authority to Data Exporter pursuant to Clause 15 of the Standard Contractual Clauses. Data Exporter agrees that Data Importer can provide information to such relevant authority as reasonably necessary to redirect the order or request. In the event Data Importer is prohibited by applicable laws from notifying Data Exporter of the relevant authority's request or order, Data Importer shall use reasonable efforts to challenge such request or order.

3. Processing Instructions. The DPA and the Agreement are Data Exporter's complete and final instructions to Data Importer for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 8.1 of the Standard Contractual Clauses, the following is deemed an instruction by Data Exporter to process Personal Data: (a) Processing in accordance with the Agreement; (b) Processing initiated by Subscribers in their use of the Service; and (c) Processing to comply with other reasonable instructions provided by Data Exporter (e.g., via email or support tickets) where such instructions are consistent with the terms of the Agreement.

4. Appointment of new Sub-processors and List of current Sub-processors. Pursuant to Clause 9 of the Standard Contractual Clauses, Data Exporter acknowledges and expressly agrees that (a) Data Importer's Affiliates may be retained as Sub-processors; and (b) Data Importer and Data Importer's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services in accordance with the process in Section 4 of the DPA. Data Importer shall make available to Data Exporter the current list of Sub-processors in accordance with Section 4.2 of the DPA.

5. Notification of New Sub-processors and Objection Right for new Sub-processors. Pursuant to Clause 9 of the Standard Contractual Clauses, Data Exporter acknowledges and expressly agrees that Data Importer may engage new Sub-processors as described in Sections 4.2 and 4.3 of the DPA.

6. Copies of Sub-Processor Agreements. The parties agree that the copies of the Sub-processor agreements that must be sent by Data Importer to Data Exporter pursuant to Clause 9 of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by Data Importer beforehand, and that such copies will be provided by Data Importer only upon reasonable request by Data Exporter.

7. Audits. The parties agree that the audits described in Clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with the following specifications: Upon Data Exporter's request, and subject to the confidentiality obligations set forth in the Agreement or otherwise agreed by the parties, Data Importer shall make available to Data Exporter (or Data Exporter's independent, third-party auditor that is not a competitor of Data Importer) information regarding Data Importer's compliance with the obligations set forth in the DPA. Data Exporter may contact Data Importer in accordance with the "Notice" provisions of the Agreement to request an audit of the procedures relevant to the protection of Personal Data, no more than once per calendar year during the term of the Agreement unless Data Exporter has reason to believe Data Importer is in breach of its compliance obligations set forth in the DPA. Data Exporter shall reimburse Data Importer for any time expended for any such on-site audit at Data Importer's then-current professional services rates, which shall be made available to Data Exporter upon request. Before the commencement of any such on-site audit, Data Exporter and Data Importer shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Data Exporter shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Data Importer. Data Exporter shall promptly notify Data Importer with information regarding any non-compliance discovered during the course of an audit.

8. Certification of Deletion. The parties agree that the certification of deletion of Personal Data that is described in Clause 16(d) shall be provided by Data Importer to Data Exporter only upon Data Exporter's request.

9. Conflict. In the event of any conflict or inconsistency between the DPA and the Standard Contractual Clauses in Attachment 3, the Standard Contractual Clauses shall prevail.

Attachment 2

DESCRIPTION OF PROCESSING ACTIVITIES

Data subjects
Customer may submit personal data to the Service, the extent of which is determined and controlled by Customer and which may include, but is not limited to, personal data relating to the following categories of data subject:

Natural persons who are End-Users of the Service.

Categories of data
The personal data transferred concern the following categories of data:

Subscriber or End-User names, contact information, and e-mail addresses, solely as required to access and use the Service.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data:

None.

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

- Processing necessary to provide, maintain, and update the Service provided to Customer;
- Providing customer and technical support to Customer; and
- Disclosures in accordance with the Agreement, as compelled by law.

Attachment 3

By signing the signature page of the DPA, the parties will be deemed to have signed this Attachment 3.

Standard Contractual Clauses (processors)

Standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

SECTION I

Clause 1
Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties: (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2
Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3
Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions: (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7; (ii) Clause 8.1(b), 8.9(a), (c), (d) and (e); (iii) Clause 9(a), (c), (d) and (e); (iv) Clause 12(a), (d) and (f); (v) Clause 13; (vi) Clause 15.1(c), (d) and (e); (vii) Clause 16(e); (viii) Clause 18(a) and (b);

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9
Use of sub-processors

(a) OPTION 2: GENERAL WRITTEN AUTHORISATION. The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least ten (10) business days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10
Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to: (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13; (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer’s responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III - LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15
Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17
Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18
Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX TO ATTACHMENT 3 STANDARD CONTRACTUAL CLAUSES

ANNEX I

A. LIST OF PARTIES

Data exporter(s): The data exporter is the legal entity, acting in the role of controller, which has purchased Service from data importer pursuant to the Agreement and is identified as Customer on the signature page of this DPA.

Data importer(s): The data importer, acting in the role of processor, is identified as Aha! Labs Inc on the signature page of this DPA.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred: Natural persons who are Subscribers or End-Users of the Service.

Categories of personal data transferred: The data exporter may submit personal data to the data importer's Services to the extent determined and controlled by the data exporter, which shall be limited to Subscriber or End-User names, contact information and e-mail addresses, solely as required to access, and use the Service of the data importer.

Sensitive data transferred (if appropriate): None.

The frequency of the transfer: Transfer of personal data may occur continuously throughout the duration of the Agreement.

Nature of the processing: The data importer will process personal data as necessary to provide the Service under the Agreement

Purpose of the data transfer and further processing: The objective of Processing of personal data by the data importer is the performance of the Service pursuant to the Agreement in place between the data exporter and the data importer.

The period for which the personal data will be retained: Personal data will be retained for the duration of the Agreement in place between the data exporter and data importer and then until the expiry of the data backup retention period.

Purpose of the data transfer and further processing: Personal data is transferred and processed in order to identify, authenticate and communicate with Subscribers and End-Users pursuant to the Agreement.

For transfers to sub-processors the subject matter, nature and duration of the processing: Transfers and processing by sub-processors are as described in this section B.

C. COMPETENT SUPERVISORY AUTHORITY

The Data Protection Authority of Ireland.

Ireland

Data Protection Commission
21 Fitzwilliam Square
D02 RD28 Dublin 2

Tel. +353 76 110 4800
Email: info@dataprotection.ie
Website: http://www.dataprotection.ie/

APPENDIX TO ATTACHMENT 3 STANDARD CONTRACTUAL CLAUSES

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Aha! maintains a comprehensive information security program that includes administrative, physical, and technical safeguards for protection of the security, confidentiality, and integrity of Personal Data that are appropriate to (a) the size, scope, and type of Aha!'s business; (b) the amount of resources available to Aha!; (c) the type of information that Aha! will store; and (d) the need for security and confidentiality of such information. Aha! regularly monitors compliance with these safeguards and maintains ISO27001 certification which includes independent third party audits. Refer to the *Aha! Labs ISO27001 Statement of Applicability v2.7* or later for a comprehensive list of implemented security controls.

Aha! encrypts all communication between customers and our data centers and across public networks using TLS with selected secure ciphers. Aha! encrypts all customer data at rest, including personal data, using strong encryption.

Aha! performs comprehensive risk assessments at least annually as part of our ISO27001 certified ISMS to evaluate threats to confidentiality, integrity, and availability of information assets including personal information. Aha! implements a resilient architecture with technical redundancies to help ensure resilience of the service including automatic failovers as well as formal disaster recovery planning, backups, and testing.

Aha! performs security and privacy awareness training and assessment for all personnel on-hire and periodically which includes attendance tracking and a comprehension assessment.

Aha! implements technical security testing as part of secure software development processes and performs independent third party security testing to evaluate the effectiveness of technical security measures.

Aha! maintains strong authentication and authorization controls for the application and data repositories and provides customer-configurable features for additional security controls such as multi-factor authentication and integration with a customer identity provider (SSO).

Aha! processing systems reside in data centers with strong physical security controls and certifications such as ISO27001 and SOC2 Type 2 attestation.

Aha! implements application and system log collection, automated analysis, intrusion detection systems, and alerts which are monitored by senior personnel and escalated as needed.

Aha! centrally manages system configurations in a secured repository with change tracking and change management which also includes hardening and least privilege configurations. Aha! validates configurations through security scanning and remediates deviations from approved configurations.

Aha! requests a minimal amount of non-sensitive personal information to use the service including name and a functional email address. The provided information may be a pseudonym and is not required to identify a natural person. Aha! users may access, review, correct or update their personal information through an authenticated profile and may request deletion of data either through automated means where supported, through a customer administrator, or through Aha! support requests.

Aha! does not use customer or production data in test, development, or non-production environments and implements strong separation of production and non-production environments. Aha! implements change management policies, processes, and controls to formally approve changes prior to production deployment.

Aha! sub-processors are managed as part of our supplier management program which includes annual security and contractual checks.