DATA PROCESSING AGREEMENT

This Data Processing Agreement (the "**Agreement** ") is made as of May 15th 2018 by and between Soomla, Inc. having its place of business at 260 Madison Ave, Suite 204, New York, NY 10016 United States ("**Provider**") and _____ ("**Client**").

The parties entered into a terms and conditions agreement dated ____ whereby Provider provides services (the "**Services**") to Client (the "**Services Agreement**"). The terms used in this Agreement shall have the meanings set forth below. Capitalized terms not defined herein shall have the meaning set forth in the Services Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall apply, with respect to the processing of Personal Data, in addition to the terms of the Services Agreement. Except where the context requires otherwise, references in this Agreement to the Agreement are to the Services Agreement as amended by, and including, this Agreement. Each reference to the Agreement below means this Agreement including its Schedules and Appendices.

In the course of providing the Services to Client pursuant to the Services Agreement, Provider may Process Personal Data on behalf of Client and the parties agree to comply with the following provisions with respect to any Personal Data.

1. Effectiveness.

1.1 **Legal Authority**. Client signatory represents to Provider that he or she has the legal authority to bind Client and is lawfully able to enter into contracts (e.g., is not a minor).

1.2 **Termination**. This Agreement will terminate upon the earliest of: (i) termination of the Agreement as permitted hereunder or by the Provider's Terms and Conditions (and without prejudice to the survival of accrued rights and liabilities of the parties and any obligations of the parties which either expressly or by implication survive termination) or (ii) as agreed by the parties in writing. Provider's obligations hereunder shall survive the termination of the Services Agreement until such time Provider no longer has access to, hosts or retains Personal Data.

2. Definitions.

"**Client Personal Data**" means any Personal Data in connection with the users of Client's Mobile Applications (End Users) Processed by Provider (or a Sub-processor) on behalf of Client pursuant to or in connection with the Agreement;

"**Data Protection Laws**" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, and the GDPR, applicable to the Processing of Client Personal Data under the Agreement which are applicable to Client.

"**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)

"**Sub-processor**" means any person (including any third party, but excluding an employee of Provider or any of its sub-contractors) appointed by or on behalf of Processor to Process Personal Data on behalf of Client under the Agreement

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

3. Processing of Personal Data.

3.1 **Roles of the Parties**. The parties acknowledge and agree that with regard to the Processing of Client Personal Data, Client is the Data Controller, Provider is a Data Processor and that Provider will engage Sub-processors pursuant to the requirements set forth in Section 5 "**Sub-processors**" below. Provider shall be allowed to exercise its own discretion in the selection and use of such means as it considers necessary to pursue those purposes, subject to the requirements of this Agreement.

3.2 **Client Authority**. Client represents and warrants that it is and will at all relevant times remain duly and effectively authorized to give the instruction set forth in Section 3.4 below on behalf of itself.

3.3 **Client's Processing of Personal Data**.

(a) Client warrants that it has all necessary rights to provide the Personal Data to Provider for the Processing to be performed in relation to the Services and shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Client acquired Personal Data.

(b) To the extent required by applicable Data Protection Laws, Client is responsible for ensuring that any necessary data subject notices with respect to and consents to this Processing are obtained, and for ensuring that a record of such notices and/or consents is maintained. Should such a consent be revoked by the data subject, Client is responsible for communicating the fact of such revocation to Provider, and Provider remains responsible for implementing any Client instruction with respect to the further processing of that Personal Data.

(c) Client shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws.

Client's instructions for the Processing of Personal Data shall comply with Data Protection Laws

3.4 **Provider's Processing of Personal Data**.

(a) Provider shall only Process Client Personal Data for the purpose of the provision of the Services under the Agreement and in accordance with Client's documented instructions, which are consistent with the terms of the Services Agreement, unless Processing is required by Data Protection Laws to which Provider (or the applicable sub-processor) is subject, in which case Provider shall to the extent permitted by the Data Protection Laws inform Client of that legal requirement before the relevant Processing of that Client Personal Data.

(b) The Services Agreement and any Order Forms thereunder, or other duly documented instructions are Client's complete and final instructions to Provider for the Processing of Client Personal Data. Any additional or alternate instructions must be agreed upon separately. Such instructions constitute: The processing of Client Personal Data (i) in accordance with the Services Agreement, and any Order Forms under the Services Agreement, including without limitation with the transfer of Client Personal Data to any country or territory; and (ii) to comply with other documented instructions provided by Client where such instructions are consistent with the terms of the Services Agreement.

(c) Where Provider considers that an instruction infringes GDPR or of any other legal provision of the Union or of Member States bearing on data protection, it shall immediately inform Client of this. Where Provider is obliged to transfer Personal Data to a third country or an international organization, under Union law or Member State law to which Provider is subject, Provider shall inform Client of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3.5 **Tracking Technologies**: Client acknowledges that in connection with the performance of the Services, Provider employs the use of unique identifiers, SDK's and similar tracking technologies ("**Tracking Technologies**"). Client shall maintain appropriate notice, consent, opt-in and opt-out mechanisms as and to the extent are required by Data Protection Laws to enable Provider to deploy Tracking Technologies lawfully on, and collect data from, the devices of Client's end users in accordance with Provider's Privacy Policy.

3.6 **Details of the Processing**. The subject-matter of Processing of Client Personal Data by Provider is the performance of the Services pursuant to the Services

Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Client Personal Data and categories of Data Subjects Processed under this Agreement, as required by article 28(3) of the GDPR are further specified in **Exhibit A** to this Agreement, as may be amended by the parties from time to time. For avoidance of doubt, at no time will the Personal Data Processed by Provider include information that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric, data concerning health or data concerning an individual's sex life or sexual orientation.

4. Provider Personnel.

4.1 **Contractual Obligations**. Provider shall ensure that the persons authorized to process Personal Data hereunder: (i) are bound by appropriate contractual obligations or are under an appropriate statutory obligation of confidentiality; and (ii) process Personal Data only on instructions from Client, unless required to do so by Union, Member State, or other applicable law.

4.2 **Access**. Provider shall restrict its personnel from Processing Client Personal Data without authorization by Provider and shall limit the Processing to that which is needed for the specific individual's job duties in connection with Provider's provision of the Services under the Services Agreement.

5. Sub-processors.

5.1 **Appointment of Sub-processors**. For the purpose of the appointment of Sub-processors, Client acknowledges and agrees that Provider may engage third-party Sub-processors in connection with the provision of the Services, including without limitation the Processing of Client Personal Data subject to the provisions of this Section 5.

5.2 **List of Current Sub-processors and Notification of New Sub-processors**. When requested by the Client, the Provider shall make available to Client an up-to-date list of all Sub-processors used for the processing of Client Personal Data. Client authorizes Provider to engage any Sub-processors listed in **Exhibit B**.

5.3 **Objection Right for New Sub-processors**. Provider shall give Client prior written notice of the appointment of any new Sub-processor, including full details of the Processing to be undertaken by the Sub-processor. If, within fifteen (15) days of receipt of that notice, Client notifies Provider in writing of any objections (on reasonable grounds) to the proposed appointment, then (i) Provider shall work with Client in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Sub-processor; and (ii) where such a change cannot be made within thirty (30) days from Provider's receipt of Client's notice, notwithstanding anything in the Agreement, Client may by written notice to Provider with immediate effect terminate the Agreement to the extent that it relates to the Services which require the use of the proposed Sub-processor.

5.4 **Sub-processing Agreement; Liability**. Provider has or shall enter into a written agreement with each Sub-processor (the "**Sub-processing Agreement**") containing data protection obligations not less protective than those in this Agreement in particular providing sufficient guarantees to implement appropriate technical and organizational measures with respect to the protection of Client Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor. Provider shall be liable for the acts and omissions of its Sub-processors to the same extent Provider would be liable if performing the services of each Sub-processor directly under the terms of this Agreement.

5.5 **Copies of Sub-Processor Agreements**. Provider shall provide to Client for review copies of the Sub-processor agreements as Client may reasonably request from time to time. The parties agree that all commercial information may be removed by the Provider beforehand.

5.6 **Other Sharing**. Client acknowledges that in the provision of the Services, Provider, on receipt of instructions from Client, may transfer or faciliate the transfer of Client Personal Data to and otherwise interact with third parties other than Provider's Sub-processors, as described above. Client agrees that if and to the extent such transfers occur, Client is responsible for entering into separate contractual arrangements with such third parties binding them to comply with obligations in accordance with Data Protection Laws. For avoidance of doubt, such third party data processors are not Subprocessors and Provider shall not bear any responsibility or liability for sharing information with such parties.

6. Security.

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, Provider shall in relation to the Client Personal Data implement and maintain throughout the term of this Agreement, the technical and organizational measures set forth in **Exhibit C** (the "**Security Measures**"). Client acknowledges and agrees that it has reviewed and assessed the Security Measures and deems them to provide a level of security appropriate to the risk in respect of Client Personal Data.

7. Data Subject Rights.

Provider will, in a manner consistent with the functionality of the Service, enable Client to: (i) access the Client Data; (ii) rectify inaccurate Customer Client; (iii) restrict the processing of Client Data; (iv) delete Client Data; and (v) export Client Data. Provider will do this by implementing appropriate technical and organizational measures, insofar as this is possible. Provider shall promptly notify Client if it receives a request from a Data Subject under any Data Protection Laws in respect of Client Personal Data and will respond only on the documented instructions of Client. If required to respond under Data Protection Laws to which Provider is subject, Provider shall, to the extent permitted by such Data Protection

Laws inform Client of that legal requirement before it responds to the request. To the extent legally permitted, Client shall be responsible for any costs arising from Provider's provision of such assistance.

8. Personal Data Breach.

8.1 **Notification of Data Breach.** Provider shall, to the extent permitted by law, notify Client within not more than twenty four (24) hours upon Provider or any Sub-processor becoming aware of a Personal Data Breach affecting Client Personal Data, providing Client with sufficient information and documentation to allow Client to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

8.2 **Assistance to Client** Provider shall co-operate with Client and take such reasonable commercial steps as are directed by Client to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8.3 No admission. Provider's notification of or response to a Personal Data Breach under this Section 8 (Personal Data Breach) will not be construed as an acknowledgement by Provider of any fault or liability with respect to the Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation.

Provider shall provide reasonable assistance to Client with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Client reasonably considers to be required of it 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 Client Personal Data by, and taking into account the nature of the Processing and information available to, Provider or the Sub-processors.

10. Return or Destruction of Personal Data.

10.1 **Return or Deletion**. Subject to the provisions of Section 10.2 below, at Client's election, made by written notice to Provider following thirty (30) days of the date of cessation of any Services involving the Processing of Client Personal Data (the "**Cessation Date**"), Provider shall, and shall procure that all Sub-processors: (i) return a complete copy of all Client Personal Data to Client in such format and manner requested by Client and reasonably acceptable to Provider; and (ii) delete and procure the deletion of all other copies of Client Personal Data Processed by Provider or any Sub-processor. Provider shall comply with any such written request within thirty (30) days of the Cessation Date.

10.2 **Retention of Copies**. Provider and each Sub-processor may retain Client Personal Data to the extent required by applicable European Union law or the law of an EU Member State and only to the extent and for such period as required by such laws and always provided that Provider shall ensure the confidentiality of all such Client Personal

Data and shall ensure that such Client Personal Data is only Processed as necessary for the purpose(s) specified in such law requiring its storage and for no other purpose.

11. **Record of Processing Activities; Documentation.**

11.1 Records. To the extent they are applicable to Provider's Processing activities for Client, Provider shall maintain all records of Processing as and to the extent required by Article 30(2) of the GDPR and shall make them available to Client upon request.

11.2 **Documentation**. Subject to the provisions of Section 12 below, at Client's written request, Provider shall provide Client with the necessary documentation for demonstrating compliance with all of Provider's obligations under this Agreement and for allowing Client or any other auditor it has authorized to conduct audits, including inspections, and for contributing to such audits.

12. Audit.

Provider shall allow Client and Client's authorized representatives to either (i) access and review up-to-date attestations, reports or extracts thereof from independent bodies (e.g. external auditors, internal audit, data protection auditors) or suitable certifications reasonably acceptable to Client to ensure compliance with the terms of this Agreement; or (ii) if the requested audit scope is not addressed the reports listed in (i) above, conduct audits or inspections to ensure compliance with the terms of this Agreement in accordance with this Section 12. Notwithstanding the foregoing, any audit must be conducted during our regular business hours, with reasonable advance notice to Provider and subject to reasonable confidentiality procedures. In addition, audits shall be limited to once per year, unless (a) Provider has experienced a Personal Data Breach within the prior twelve (12) months; (b) an audit reveals a material noncompliance; or (c) otherwise required by Data Protection Law and Regulation, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory. To the extent legally permissible, Client will be responsible for any fees charged by any auditor appointed by Client to execute any such audit.

13. Transfer of Data.

13.1 **EU US Privacy Shield**. If the Processing of Client Data involves the transfer of Personal Data out of the European Economic Area ("**EEA**"), to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws, and such transfers are subject to the Data Protection Laws ("**Restricted Transfer**"), commencing from the date of its certification under the EU US Privacy Shield Framework ("**Privacy Shield**") Provider will transfer the Client Data pursuant to its Privacy Shield certification. To this end Provider agrees to maintain its Privacy Shield certification throughout the term of the Agreement, provided Privacy Shield certification remains a valid basis under the Data Protection Laws for establishing adequate protections in respect of a transfer of Personal Data outside of the EEA, Provider will promptly notify Client if it ceases to maintain, or anticipates the revocation or

withdrawal, or is otherwise challenged by any regulatory authority as to the status of its Privacy Shield certification, or if it makes a determination that its can no longer meet its obligations under Privacy Shield.

13.2 **Standard Contractual Clauses**. Prior to the effective date of Provider's Privacy Shield certification or thereafter, at Client's request, Provider shall enter into Standard Contractual Clauses in respect of the processing of such Personal Data. In the event Standard Contractual Clauses are used, Provider shall, before the commencement of a Restricted Transfer to a Sub-processor, ensure that one of the following is in place: (i) the Standard Contractual Clauses are at all relevant times incorporated into the agreement between Provider, or a relevant intermediate Sub processor, on the one hand and Sub-processor on the other hand; (ii) that Sub-processor enters into an agreement incorporating the Standard Contractual Clauses with Client, that (iii) Provider's entry into the Standard Contractual Clauses as agent for and on behalf of that Sub-processor, will have been duly and effectively authorized (or subsequently ratified) by that Sub-processor or that (iv) another mechanism acceptable under the Data Protection Laws for the cross border transfer is in place. Client undertakes to cooperate with the applicable alternative under this Section. If executed, the Standard Contractual Clauses will be attached as Exhibit D to this Agreement and constitute a part thereof.

14. **Jurisdiction and Governing Law.**

The parties to this Agreement hereby submit to the choice of law and jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Agreement, including disputes regarding its existence, validity or termination or the consequences of its nullity, provided, however that: (i) if Standard Contractual Clauses are used in connection with this Agreement, then the parties submit to the law of the EU Member State in which the data exporter is located and (ii) if there is any conflict with the laws of the EU member state in which the Client is based, if any, the law of such EU member state would prevail only with respect to the sections concerning which there is such conflict.

15. Indemnification; Limitation of Liability.

Each party "**Indemnifying Party**") indemnifies the other party ("**Indemnified Party**") and holds it harmless against all claims, actions, third party claims, losses, damages and expenses (including reasonable attorney's fees) incurred by the Indemnified Party and arising directly or indirectly out of or in connection with a breach of this Agreement, the Agreement, the Standard Contractual Clauses and/or applicable Data Protection Laws by Indemnifying Party in accordance with the provisions of the "Indemnification" Section of the Services Agreement. Provider's liability, taken together in the aggregate, arising out of or related to this Agreement the Standard Contractual Clauses and/or applicable Data Protection Laws, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Services Agreement. For the avoidance of doubt, Provider's total liability for all claims from the Client or any third party arising out of or related to the Services Agreement and this

Agreement shall apply in the aggregate for all claims under both the Services Agreement and this Agreement.

16. Changes to Agreement

16.1 Provider may amend this Agreement if the change:

(a) is expressly permitted by this Agreement

(b) reflects a change in the name or form of a legal entity;

(c) is required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency; or

(d) does not: (i) result in a degradation of the overall security of the Service; (ii) expand the scope of, or remove any restrictions on, Provider's processing of Personal Data; and (iii) otherwise have a material adverse impact on Client's rights under this Agreement, as reasonably determined by Provider.

16.2 If Provider intends to change this Agreement under Section 16.1(c) or (d), Provider will inform Client at least 30 days (or such shorter period as may be required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency) before the change will take effect by either: (a) sending an email to Client's email address on file with Provider; or (b) alerting Client via the user interface for the Services. If Client objects to any such change, Client may terminate the Agreement by giving written notice to Provider within 90 days of being informed by Provider of the change.

[Remainder of Page Intentionally Left Blank; Signature Pages to Follow]

EXECUTED by and on behalf of:
Provider

.....

Name: Yaniv Nizan
Role: CEO
Date: May 21st 2018

EXECUTED by and on behalf of

.....

.....

Name:
Role:
Date:

EXHIBIT A TO DATA PROCESSING AGREEMENT: DETAILS OF PROCESSING

- **Duration of the Processing**: The duration of data processing shall be for the term agreed between data exporter and Provider in the Agreement or an applicable Order Form.

- **Nature and purpose of the Processing**: The scope and purpose of processing of the Data Subjects' personal data is to facilitate the provision of Provider's Services.

- **Types of Client Personal Data: The Personal Data transferred is:**
    - IP Addresses,
    - Advertising IDs: IDFA for iOS users and GAID for Android users
    - Customer supplied user IDs
    - IDs generated by other data platforms used by the customer

- **Categories of Data Subjects:**
    - End users of mobile applications

EXHIBIT B TO DATA PROCESSING AGREEMENT: AUTHORIZED SUB-CONTRACTORS

Amazon Web Services – AWS

Sentry.io

EXHIBIT C TO DATA PROCESSING AGREEMENT: SECURITY CONTROLS

ORGANIZATION OF INFORMATION SECURITY

- Security Ownership. Soomla has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures.

- Security Roles and Responsibilities. Soomla personnel with access to Client Personal Data are subject to confidentiality obligations.

PHYSICAL SECURITY

- Physical Access to Facilities. Soomla limits access to facilities where information systems that process Client Personal Data are located to identified authorized individuals.

- Video Surveillance. Soomla monitors its facilities with security cameras.

- Protection from Disruptions. Soomla uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.

- We use several services from AWS to regularly back up our data bases and prevent data loss.

- Component Disposal. Soomla uses industry standard processes to delete Client Personal Data when it is no longer needed.

COMMUNICATION AND OPERATION - Data Beyond Boundaries

- Soomla encrypts, or enables Client to encrypt, Client Personal Data that is transmitted over public networks.

- Soomla uses authentication mechanisms to ensure decryption is only possible by Client, Soomla or Soomla's sub processors

- Soomla restricts access to Client Personal Data in media leaving its facilities.

ACCESS CONTROL

Access Policy. Soomla maintains a record of security privileges of individuals having access to Client Personal Data.

Access Authorization

- Soomla maintains and updates a record of personnel authorized to access Soomla systems that contain Client Personal Data.

- Soomla deactivates authentication credentials for personnel that left the company, was fired or moved to a role that no longer requires access.

- Soomla identifies those personnel who may grant, alter or cancel authorized access to data and resources.

- Soomla ensures that where more than one individual has access to systems containing Client Personal Data, the individuals have separate identifiers/log-ins.

Least Privilege

- Technical support personnel are only permitted to have access to Client Personal Data only for customers where the situation requires it.

- Soomla restricts access to Client Personal Data to only those individuals who require such access to perform their job function.

Integrity and Confidentiality

- Soomla instructs Soomla personnel to disable administrative sessions when computers are otherwise left unattended.

- Soomla stores passwords in a way that makes them unintelligible while they are in force.

Authentication

- Soomla uses industry standard practices to identify and authenticate users who attempt to access information systems.

- Where authentication mechanisms are based on passwords, Soomla requires the password to be at least eight characters long.

- Soomla maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.

- Soomla uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.

Network Design.
Soomla has controls to avoid individuals assuming access rights they have not been assigned to gain access to Client Personal Data they are not authorized to access.

We also regularly check the effectiveness of our network design to ensure the security of the data and assess potential risks