Data Processing Addendum

This Data Processing Addendum ("**Addendum**") forms part of the terms of service or services agreement ("**Services Agreement**") between TENSOR SOCIAL with registered office at 819 Santee St. Los Angeles, CA 90014"**TENSOR SOCIAL**"; and you, "**Customer**".

RECITALS:

(A) The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Services Agreement. Except as modified below, the terms of the Services Agreement shall remain in full force and effect.

(B) In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Services Agreement. Except where the context requires otherwise, references in this Addendum to the Services Agreement are to the Services Agreement as amended by, and including, this Addendum.

(C) Customer and TENSOR SOCIAL have entered into a Services Agreement pursuant to which TENSOR SOCIAL will provide certain Services. TENSOR SOCIAL's liability for this Addendum is limited to the period of the validity of the Services Agreement, i.e. the period during which TENSOR SOCIAL is contracted by Customer for the provision of the Services.

(D) To the extent that the provision of such services involves the processing of Customer Personal Data, the parties have agreed to enter into this Addendum for the purposes of ensuring compliance with the applicable data protection legislation.

1. Definitions

1.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "**Applicable Laws**" means any relevant data protection laws, applicable to the Services Agreement, including, but not limited to, the GDPR;

1.1.2 "**Customer Personal Data**" means any Personal Data of Influencers Processed by a Contracted Processor on behalf of Customer for the performance of the Services Agreement;

1.1.3 "**Contracted Processor**" means TENSOR SOCIAL or a Sub-processor;

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

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

1.1.6 "**Restricted Transfer**" means a transfer of Customer Personal Data to TENSOR SOCIAL, where such transfer would be prohibited by Applicable Laws in the absence of the Standard Contractual Clauses.

1.1.7 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of TENSOR SOCIAL for Customer pursuant to the Services Agreement. Namely, Scraping of public data on behalf of Customer;

1.1.8 "**Standard Contractual Clauses**" means the agreements between TENSOR SOCIAL and Customer and attached hereto as Schedule 3 and Schedule 4 pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection and the European Commission's decision (C(2001)1539) of 15 June 2001 on Standard Contractual Clauses for the transfer of personal data to third countries, under Directive 95/49/EC respectively;

1.1.9 "**Subprocessor**" means any person (excluding an employee of TENSOR SOCIAL or any of its sub-contractors) appointed by or on behalf of TENSOR SOCIAL to Process Personal Data on behalf of Customer for the performance of the Services Agreement; and

1.1.10 "**TENSOR SOCIAL Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with TENSOR SOCIAL, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

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

1.3 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Processing of Customer Personal Data

2.1 The Customer hereby acknowledges and agrees that TENSOR SOCIAL acts as a Processor for the purposes of Services Agreement, and any personal data Scraped and provided to Customer, and/or any third party on behalf of Customer, by TENSOR SOCIAL in connection with the Services Agreement is provided strictly for the purposes of matching Influencers with businesses for the promotion and potential future partnership ("**Authorized Processing of Customer Personal Data**"), and that Customer acts as a sole and separate Controller with respect to such purposes.

2.2 Customer hereby represents and warrants that it, and/or any third party on its behalf, (i) shall Process the Customer Personal Data solely in compliance and as permitted under the Applicable Laws; and (ii) shall not Process the Customer Personal Data for any purpose other than for the Authorized Processing of Customer Personal Data.

2.3 TENSOR SOCIAL is unaware of any additional uses of the Customer Personal Data except for the Authorized Processing and, in any event, Customer is responsible for the compliance with

Applicable Laws as the Controller of Customer Personal Data, whichever other way it is Processed.

2.4 This addendum shall apply only to the extent that the Applicable Laws apply to the processing of Customer Personal Data.

2.5 TENSOR SOCIAL shall not, when acting as a Processor of Customer, Process Customer Personal Data other than on the Customer's documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case TENSOR SOCIAL shall, to the extent permitted by Applicable Laws and commercially practicable, inform the Customer of that legal requirement before the relevant Processing of that Personal Data.

2.6 Annex 1 to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Customer Personal Data as required by article 28(3) of the GDPR. Nothing in Annex 1 confers any right or imposes any obligation on any party to this Addendum.

3. INDEPENDENT CONTROLLERS

3.1 This section applies solely in those circumstances where parties may both be considered independent controllers of personal data, the parties acknowledge and agree that the relevant party will comply with any obligations applicable to it under Applicable Laws with respect to the processing of that data. Both parties shall keep a record of all Processing activities with respect to Personal Data covered under this DPA as required under GDPR.

3.2 Each party will comply with the obligations applicable to it under the Applicable Laws with respect to the processing of Personal Data covered under this DPA, including but not limited to: (i) providing the other party contact details for each party's Data Protection Officer which are accurate and up to date; (ii) providing reasonable information and assistance to the other party conducting data protection impact assessments as required by Data Protection Laws; and (iii) providing reasonable information and assistance to the other party regarding consultations between that party and a Supervisory Authority. The objective of Processing of Personal Data by both parties is the performance of the Services pursuant to the Services Agreement.

3.3 Each party is separately responsible for honoring Data Subject access requests under Applicable Laws (including its rights of access, correction, objection, erasure and data portability, as applicable) and responding to correspondence, inquiries and complaints from data subjects. Each party shall provide reasonable and timely assistance to the other party as necessary to help facilitate compliance with this section.

3.4 Both parties agree that their respective liability under this section shall be apportioned according to each parties' respective responsibility for the harm (if any) caused by each respective party.

3.5 **Liability Cap Exclusions.** Nothing in this section will affect the remaining terms of the Services Agreement relating to liability (including any specific exclusions from any limitation of liability).

4. Security

4.1 TENSOR SOCIAL shall take reasonable steps to ensure that access to the Customer Personal Data is limited to those individuals who need to know / access the relevant Customer Personal Data, as necessary for the purposes of the Services Agreement, and that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4.2 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, TENSOR SOCIAL shall in relation to the Customer Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

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

5. Subprocessing

5.1 The Customer generally authorises TENSOR SOCIAL to appoint (and permit each Subprocessor appointed in accordance with this section to appoint further down the line) Subprocessors. Customer specifically authorises the engagement of TENSOR SOCIAL's Affiliates as Subprocessors.

5.2 TENSOR SOCIAL may continue to use those Subprocessors already engaged by TENSOR SOCIAL as at the date of this Addendum as specified in a separate notice prior to this addendum.

5.3 With respect to each Subprocessor, TENSOR SOCIAL shall ensure that the arrangement between on the one hand (a) TENSOR SOCIAL, or (b) the relevant Subprocessor; and on the other hand the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Customer Personal Data as those set out in article 28(3) of the GDPR;

5.4 TENSOR SOCIAL shall be liable for the acts and omissions of its Subprocessors to the same extent it would be liable if performing the Services of each Subprocessor directly under the terms of this Addendum, except as otherwise set forth in the Agreement.

6. Data Subject Rights

6.1 TENSOR SOCIAL shall assist Customer by implementing appropriate technical and organisational measures, insofar as this is commercially and technically possible, for the fulfilment of Customer's obligations, to respond to requests to exercise Data Subject rights under Applicable Laws. TENSOR SOCIAL may require Customer to cover the costs of such assistance in the event that such assistance may interfere with the normal operation of TENSOR SOCIAL and/or create an unreasonable burden on TENSOR SOCIAL, and/or require TENSOR SOCIAL to make material changes to its products and services, subject to TENSOR SOCIAL's sole discretion.

6.2 TENSOR SOCIAL shall:

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

6.2.2 not respond, and shall take reasonable efforts to ensure that any Subprocessor does not respond, to that request except on the documented instructions of Customer, or as required by Applicable Laws to which the Contracted Processor is subject.

7. Personal Data Breach

7.1 TENSOR SOCIAL shall notify Customer without undue delay upon TENSOR SOCIAL becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information to allow each Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under Applicable Laws. Customer agrees that an unsuccessful security incident will not be subject to this Section, if it results in no unauthorized access to Customer Personal Data or to any of Contracted Processors' equipment or facilities

containing Customer Personal Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, or similar incidents.

7.2 Customer is solely responsible for providing in advance an email to which notifications regarding Personal Data Breach should be sent, and ensuring that such email address is current and valid. The default email address for the purpose of sending notification under this Section shall be the email address specified in the Customer dashboard made available by TENSOR SOCIAL at the time of the notification or that which was noted in the notices section of the Services Agreement (if those email addresses differ, both shall be regarded valid for notice purposes).

7.3 TENSOR SOCIAL shall co-operate with Customer and take such reasonable commercial steps to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

7.4 Customer shall use the Services in an appropriate manner, taking into account the level of security necessary for securing the Customer Personal Data.

8. Data Protection Impact Assessment and Prior Consultation

TENSOR SOCIAL shall provide reasonable assistance, as commercially and technically feasible, and at Customer's expense, to Customer with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Customer reasonably considers to be required by article 35 or 36 of the GDPR, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors, and in accordance with TENSOR SOCIAL's standard practices.

9. Deletion of Customer Personal Data

9.1 During the term of the Services Agreement, taking into account the nature of the Processing, TENSOR SOCIAL shall make reasonable efforts to comply with any reasonable request from Customer to delete information of a user of the Customer, insofar as this is possible, unless the GDPR and/or any other Applicable Laws require storage of the Customer Personal Data. TENSOR SOCIAL shall delete only Customer Personal Data associated with the Processing on behalf of the Customer. TENSOR SOCIAL may require Customer to the cover the costs of such assistance in the event that such assistance may interfere with the normal operation of TENSOR SOCIAL and/or create an unreasonable burden on TENSOR SOCIAL, and/or require TENSOR SOCIAL to make material changes to its products and services, subject to TENSOR SOCIAL's sole discretion.

9.2 TENSOR SOCIAL shall promptly and in any event within 180 days of the date of cessation of any Services involving the Processing of Customer Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those Customer Personal Data Processed for the performance of the Services, insofar as this is possible taking into account the nature and functionality of the Services.

9.3 Each Contracted Processor may retain a copy of Customer Personal Data: (i) in accordance with its data retention policies specified to Customer in advance (as may be updated from time to time), and/or (ii) for the purpose of the establishment, exercise or defence of legal claims, including without limitation, detection and prevention of fraudulent activities.

9.4 If requested by Customer, TENSOR SOCIAL shall provide written approval to Customer that it has complied with this section within 90 days of the Cessation Date.

10. Audit rights

Upon prior written request by Controller, Processor agrees to cooperate and within reasonable time provide Controller with: (a) a summary of the audit reports demonstrating Processor's compliance with

its obligations under this Addendum, after redacting any confidential and commercially sensitive information; and (b) confirmation that the audit has not revealed any material vulnerability in Processor's systems, or to the extent that any such vulnerability was detected, that Processor has fully remedied such vulnerability. If the above measures are not sufficient to confirm compliance with EU Data Protection law or reveal some material issues, subject to the strictest confidentiality obligations, Processor allows Controller to request an audit of Processor's data protection compliance program by external independent auditors, which are jointly selected by the Parties. The external independent auditor cannot be a competitor of Processor, and the Parties will mutually agree upon the scope, timing, and duration of the audit. Processor will make available to Controller the result of the audit of its data protection compliance program. Controller must reimburse Processor for all expenses and costs for such audit, unless the audit identifies material deficiencies in Processor's practices or breaches of this Addendum. The audit right hereunder may be exercised once in a calendar year during the Term and in addition where it is reasonably suspected that a Personal Data Breach has occurred. However, should the audit reveal any non-conformity; the Controller shall be entitled to have its auditor perform follow-up audits to the extent necessary to protect its interests under this Addendum.

11. Restricted Transfers

11.1 Customer and TENSOR SOCIAL hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from Customer to TENSOR SOCIAL and from TENSOR SOCIAL to Customer.

11.2 Schedule 3 or 4 shall apply depending on which party is regarded an importer or exporter of Customer Personal Data.

12. General Terms

Governing law and jurisdiction

12.1 Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses:

12.1.1 the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Services Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

12.1.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Services Agreement.

Order of precedence

12.2 In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

12.3 In the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Services Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

Severance

12.4 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

Changes to this Addendum

12.5 TENSOR SOCIAL may change this Addendum by sending an email notification to Customer, at least 30 days prior to any such taking effect, in the event that such change does not: (i) result in a degradation of the overall security of the Services; (ii) expand the scope of, or remove any restrictions on, TENSOR SOCIAL's Processing of Customer Personal Data; and (iii) otherwise have a material adverse impact on Customer's rights under this Addendum, as reasonably determined by TENSOR SOCIAL, unless such change is required by Applicable Laws. For the avoidance of doubt, TENSOR SOCIAL may change the types of data specified under "*The types of Customer Personal Data to be Processed*" to the extent such change is made in accordance with this Section.

SCHEDULE 1: DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

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

Subject matter and duration of the Processing of Customer Personal Data

As set out in the Services Agreement, provision of information on Influencers through Scraping upon Customer request and instruction. All during the validity of the Services Agreement.

The nature and purpose of the Processing of Customer Personal Data

TENSOR SOCIAL will Process (including Scraping, as applicable to the Services and the instructions set forth in this Addendum, collect, record, organise, structure, store, alter, retrieve, use, disclose, combine, erase and destroy) Customer Personal Data for the purpose of providing the Services and any related technical support to Customer in accordance with this Addendum.

The types of Customer Personal Data to be Processed

Any public information made available by Influencers on social media networks, including, but not limited to aliases, names, email addresses, interests, follower lists, posts made, pictures uploaded and stats of the interaction by followers to those Influencer activities.

The categories of Data Subject to whom the Customer Personal Data relates

Influencers (end users of various social networks) as defined in the Services Agreement with publicly available profiles.

SCHEDULE 2: TECHNICAL AND ORGANISATIONAL MEASURES

Description of the minimum technical and organisational security measures to be implemented by the data importer in accordance with Appendix 2 of the Standard Contractual Clauses Controller- Processor.

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, TENSOR SOCIAL shall in relation to the Customer Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR, and as shall be further specified upon request by Customer.

Data importer currently observes the security practices described in this Schedule 2. Notwithstanding any provision to the contrary otherwise agreed to by data exporter, data importer may modify or update these practices at its discretion provided that such modification and update does not result in a material degradation in the protection offered by these practices.

(1) Protective measures for **physical access control:**
Provider secures access to the premises via ID readers, so that only authorised persons have access. The ID cards can be blocked individually; access is also logged. Furthermore, an alarm system is installed in the premises of Provider, preventing infiltration by unauthorised persons. The alarm system is linked to a locking mechanism for the doors. In addition, a security service carries out inspection rounds.
(2) Protective measures for **system access control:**
each employee has access to the systems/services of Provider via his/her own employee access. The access rights involved are limited to the responsibilities of the respective employee and/or team. Provider regulates access to its own systems via password procedures and the use of SSH keys of at least 1024 bits in length. The SSH keys strengthen the productive systems against attacks that target weak passwords, as the password-based access to the relevant systems is disabled. Provider has, in addition, a regulation for the creation of passwords. This guarantees higher security also for systems that offer password-based access. Passwords must meet the following requirements: At least 8 characters long At least 1 letter in upper-case At least 1 letter in lower-case At least 1 number At least 1 non-alphanumeric character The systems of Provider are protected by firewalls that reject all incoming connections by default. Only connection types defined by exception are accepted.
(3) Protective measures for **data access control:**
All servers and services at Provider are subject to continuous monitoring. This includes the logging of personal access in the user interface. Due to the close proximity of the employees, a visual inspection is possible at any time. Locking and/or logging off when leaving work is prescribed in writing and is practised.
(4) Protective measures for **transfer control:**
The handling of local data storage devices, e.g. USB sticks, at Provider is regulated via agreements. Access to the systems from outside the company network is possible only via secure VPN access. The traffic between the systems of Provider is protected via L2TP, IPsec (or equivalent protection).
(5) Protective measures for **input control:**
Employees of Provider do not work directly at database level, but instead use applications to access the data. IT employees access the system via individual access and use a common login, as there are very few employees and these sit in close proximity of each other and monitor each other by agreements and visual inspections.
(6) Protective measures for **availability control:**
Provider ensures the availability of data in several ways. On the one hand, there is regular backup of the entire system. This steps in if the other availability measures fail. In operation mode, Provider ensures availability through the use of high availability clusters. Critical services are operated redundantly in multiple data centres and controlled by a high-availability system. The Provider workstations are also protected with the usual measures. For example, virus scanners are installed, laptops are encrypted.
(7) Protective measures for **separation control:**

To separate data, Provider uses logically separate databases so that no accidental reading of data by unauthorised persons can occur. Access to the data itself is also restricted by the fact that employees use services (applications) which control access.

SCHEDULE 3: CLAUSES WHERE THE DATA IMPORTER IS A PROCESSOR - STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

Standard Contractual Clauses (processors)

The Standard Contractual Clauses where the data importer acts as a Processor can be accessed at: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087, and are part to this Addendum when TENSOR SOCIAL acts as a Processor.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses.
The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.
See Schedule 1 of this Addendum

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) are set out in Schedule 2 of this Addendum.

SCHEDULE 4: CLAUSES WHERE THE DATA IMPORTER IS A CONTROLLER - STANDARD CONTRACTUAL CLAUSES (CONTROLLERS)

Standard Contractual Clauses (controllers)

The Standard Contractual Clauses where the data importer acts as a Controller can be accessed at: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32001D0497, and are part to this Addendum when, and:

a. both TENSOR SOCIAL and Customer act as Controllers; and/or

b. TENSOR SOCIAL acts as a data exporter and Customer acts as a data importer.

ANNEX B TO THE STANDARD CONTRACTUAL CLAUSES

This Annex B forms part of the Clauses.
The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Annex.
See below for when TENSOR SOCIAL acts as a data exporter and Customer acts as a data importer.

Data exporter
The data exporter is:
TENSOR SOCIAL, when it acts as a Processor.

Data importer The
data importer is:
Customer.

Data subjects
The personal data transferred concern the following categories of data subjects: Influencers (end users of various social networks) as defined in the Services Agreement with publicly available profiles.

Categories of data
The personal data transferred concern the following categories of data: any public information made available by Influencers on social media networks.

Special categories of data (if appropriate)
The personal data transferred does not contain sensitive personal data.

Processing operations
TENSOR SOCIAL will Process (including Scraping, as applicable to the Services and the instructions set forth in this Addendum, collect, record, organise, structure, store, alter, retrieve, use, disclose, combine, erase and destroy) Customer Personal Data for the purpose of providing the Services and any related technical support to Customer in accordance with this Addendum.