Amendment Agreement to the Talkable Terms of Service Agreement Regarding the Processing of Personal Data of EU Customers

(hereinafter referred to as "**DPA**")
by and between

1. Curebit, Inc. dba Talkable, 475 Valencia St, 2nd Floor, San Francisco, CA 94103, USA

- hereinafter referred to as "**Talkable**" -

and

2. [■■■]

- hereinafter referred to as "**Customer**" -

- Talkable and Customer hereinafter referred to as "**Parties**" and each as "**Party**" -

PREAMBLE

Talkable performs cloud based tracking services for Customer ("**Services**") as agreed between the Parties in Talkable's Terms of Service Agreement, entered into by and between Customer and Talkable on or about [_____] ("**Terms of Service**"). In the course of providing the Services, Talkable will get access to, store, process or otherwise use ("**Process**") personal data of Customer's end-customers ("**End-Customers**") including such data from its affiliates located in the European Union and/or European Economic Area.

This DPA regulates the data protection obligations of the Parties when processing Customer's personal data is under the Terms of Service and will ensure that such processing will only be rendered on behalf of and under the Instructions of Customer and in accordance with the EU Standard Contractual Clauses for Processors pursuant to European Commission Decision of 5 February 2010 ("**SCC**") and Art. 28 and 29 of the General Data Protection Regulation ("**GDPR**"). However, when Talkable is acting as a controller of data subjects' personal data for Talkable's Uses (as that term is defined in Section 11), this DPA and its exhibits shall not be applicable.

1. **DEFINITIONS**

– In addition to the definition in Clause 1 SCC, "**Instruction**" means any documented instruction, submitted by Customer to Talkable, directing Talkable to perform a specific action with regard to personal data, including but not limited to the rectification, erasure or restriction of personal data. Instructions shall initially be specified in the Terms of Service and may, from time to time thereafter, be amended, supplemented or replaced by Customer by separate written or text form Instructions provided that such instructions still fall with the scope of the Services. Instructions issued for the purpose of complying with statutory claims under the GDPR such as rectification, erasure or restriction of personal data fall within the scope of the Services.

– Terms used but not defined in this Section, including but not limited to “personal data”, “personal data breach”, “processing”, “controller”, “processor” and “data subject”, will have the same meaning as set forth in Art. 4 GDPR.

– “**Applicable Law**” means all laws, rules and regulations applicable to either party’s performance under this DPA, including but not limited to those applicable to the processing of personal data. This means in particular the GDPR and all national laws validly amending the applicable rules for the processing of personal data.

2. SUBJECT, DURATION, PURPOSE, AND SPECIFICATION OF PROCESSING

2.1. Talkable will, in the course of providing Services due under the Terms of Service, Process Customer’s personal data which shall be subject to the following provisions contained in this DPA.

2.2. The subject matter, duration, nature and purpose of the processing are described in in the Terms of Service, the appendices of the SCC and Sect. 9 of this DPA.

2.3. The categories of data and data subjects which may be concerned by the processing are listed in Exhibit B, Appendix 1.

2.4. This DPA amends the Terms of Service with respect to any processing of personal data provided by Customer and/or its affiliates specified in Exhibit A (each listed affiliate is hereinafter referred to as: "**EU Customer Affiliate**") as amended from time to time by written agreement between both Parties.

2.5. Customer will enter into this DPA on its own behalf and on behalf of each of the EU Customer Affiliates for which Customer is authorized to act. Alternatively, EU Customer Affiliates can co-sign this DPA.

3. STANDARD CONTRACTUAL CLAUSES

Any processing operation as described in Sect. 2. shall be subject to the SCC as contained in Exhibit B which shall prevail over any conflicting clauses in the Terms of Service or the DPA. The Parties agree that the SCC shall be directly binding between Talkable as Data Importer (as defined therein), Customer and each EU Customer Affiliate, each acting as Data Exporter (as defined therein) in relation to the personal data provided by Customer or the respective EU Customer Affiliate.

4. TALKABLE’S OBLIGATIONS

4.1. In addition to Clause 5 (a) SCC, Talkable shall in the course of providing Services, including with regard to transfers of personal data to a third country, process Customer’s personal data only on behalf of and under the documented Instructions of Customer unless required to do so otherwise by Union or Member State law to which the Talkable is subject; in such a case, Talkable shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

4.2. Talkable shall take steps necessary to ensure that any natural person acting under its authority who has access to personal data does not process them except on Instructions from the Customer, unless he or she is otherwise required to do so by Applicable Law, Union or Member State law.

4.3. Talkable ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and that the obligation will remain after termination of this DPA.

4.4. Technical and Organizational Data Security Measures

4.4.1. In addition to Clause 5 (c) SCC, the measures specified in Exhibit B, Appendix 2 are subject to technical advancements and development.

4.4.2. 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, Talkable shall implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk, as required by Art. 32 GDPR. This includes but is not limited to

- the pseudonymization and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; and
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

4.4.3. When assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

4.4.4. If Talkable significantly modifies measures specified in Exhibit B, Appendix 2, such modifications have to meet the obligations pursuant to Sect. 4.4.2 and 4.4.3. Talkable shall make available to Customer a description of such measures which enables Customer to assess compliance with Art. 32 GDPR and allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer as permitted by Clause 5 (f) SCC. Talkable and Customer shall agree on such significant modifications by signing the modified Exhibit B, Appendix 2 after every amendment. Customer shall not refuse to accept any modification that meets the requirements pursuant to Sect. 4.4.2 and 4.4.3 of this DPA.

4.4.5. Talkable shall implement a data protection management procedure according to Art. 32 para 1 lit. d) GDPR, for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures to ensure the security of the processing. Talkable will further, by way of regular self-audits, ensure that the processing of Customer's personal data conforms with the provisions as agreed with Customer or to Customer's Instructions.

4.5. Talkable shall, while taking into account the nature of the processing, assist Customer through appropriate technical and organizational measures, with the fulfilment of Customer's obligations

to respond to requests for exercising rights of data subjects in accordance with Applicable Law, in particular Art. 15 through 18 and 21 GDPR.

4.6. Taking into account the nature of the processing and the information available to Talkable, Talkable shall assist Customer with ensuring compliance with the obligations pursuant to Art. 33 through 36 GDPR (Data Security Breach Notification, Data Protection Impact Assessment, Consultation with Data Protection Supervisory Authorities).

4.7. Documentation and Audit Rights

4.7.1. Talkable may, in its discretion provide data protection compliance certifications issued by a commonly accepted certification issuer which has been audited by a data security expert, by a publically certified auditing company or by another customer of Talkable.

4.7.2. In case Customer has justifiable reason to believe that Talkable is not complying with the terms and conditions under this agreement, in particular with the obligation to implement and maintain the agreed technical and organizational data security measures, and only once per year, Customer is entitled to audit Talkable. This audit right can be exercised by (i) requesting additional information, (ii) accessing the databases which process Customer's personal data or (iii) by inspecting Talkable's working premises whereby in each case no access to personal data of other customers or Talkable's confidential information will be granted. Alternatively, Customer may also engage third party auditors to perform such tasks on its behalf. The costs associated with such audits and/or for providing additional information shall be borne by Customer unless such audit reveals Talkable's material breach with this DPA.

4.7.3. Customer may, in its discretion and in exchange for the audit, rely on data protection certifications issued by a commonly accepted certification issuer which has been audited by a data security expert or by a publicly certified auditing company.

4.7.4. If Customer intends to conduct an audit at Talkable's working premises, Customer shall give reasonable notice to Talkable and agree with Talkable on the time and duration of the audit. In the case of a special legitimate interest, such audit can also be conducted without prior notice. Both Parties shall memorialize the results of the audit in writing.

4.8. Notification Duties

4.8.1. In addition to Clause 5 (d) SCC, Talkable shall inform Customer without undue delay in text form (e.g. letter, fax or e-mail) of the events listed in Clause 5 (d) SCC and the following events:

- Requests from third parties including from a data protection supervisory authority regarding Customer's personal data;
- Threats to Customer's personal data in possession of Talkable by garnishment, confiscation, insolvency and settlement proceedings or other incidents or measures by third parties. In such case, Talkable shall immediately inform the respective responsible person/entity that Customer holds the sovereignty and ownership of the personal data.

4.8.2. For the purpose of complying with Clause 5 (d) SCC and for enabling Customer to comply with its own data breach notification obligations pursuant to Art. 33 para 2 GDPR, Talkable shall notify Customer without undue delay after becoming aware of a personal data breach. Such notice will, at a minimum, include the following information:

- a description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- information pursuant to Sect. 4.10;
- description of the likely consequences of the personal data breach; and
- description of the measures taken or proposed to be taken by the Customer to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4.8.3. Talkable shall inform Customer immediately if, from its point of view, an Instruction of Customer may lead to a violation of the GDPR or other Union or Member State data protection provisions. Until the Customer either confirms or alternates the Instruction, Talkable may refuse to comply.

4.9. Rectification, Erasure (Deletion), Restriction

4.9.1. If legally required and not pursuable by Customer or if within the services description contained in the Terms of Service, Talkable shall rectify, erase (delete) or restrict (block) Customer's personal data upon Customer's request. Any deletion of Customer's personal data pursuant to this Sect. 4.9 shall be executed in such a manner that restoring or recovering such data is rendered impossible.

4.9.2. At Customer's request, Talkable shall conduct a data protection-compliant destruction of data carriers and other material if so provided by Customer. Alternatively, at the request of Customer, Talkable shall provide the data carriers and other material to Customer or store it on Customer's behalf.

4.9.3. Unless Union or Member State law requires a retention of the personal data, Talkable shall, upon completion of the Services in consultation with Customer, either delete or return all Customer's personal data in its possession to Customer.

4.9.4. If a data subject concerned addresses Talkable with claims for rectification, erasure or restriction, Talkable shall refer the data subject to Customer.

4.10. Talkable will inform Customer of the name and the official contact details of its data protection officer if Talkable is, by Applicable Law, required to appoint a data protection officer. If Talkable is not required to appoint a data protection officer, Talkable shall name a person responsible for dealing with questions relating to applicable data protection law and data security in the context of performing this DPA.

4.11. In the case claims based on Art. 82 GDPR are raised against Customer, Talkable shall reasonably support Customer with its defense.

4.12. Talkable will make available to Customer all information necessary to demonstrate compliance with the obligations laid down in DPA and Art. 28 GDPR.

4.13. Takable will on request make available a records of its processing activities based on Art. 30 GDPR unless the exception of Art. 30 para 5 GDPR applies.

5. CUSTOMER'S OBLIGATIONS

5.1. In addition to Clause 4 (b) SCC, Customer shall provide all Instructions pursuant to this DPA to Talkable in written or electronic form.

5.2. Customer may issue Instructions at any time as to the type, scope and procedures of the processing to the extent this is so provided in the Terms of Service. Verbal Instructions shall be confirmed in written form immediately thereafter. Customer shall notify Talkable in writing of the names of the persons who are entitled to issue Instructions to Talkable. Any consequential costs incurred resulting in Customer's failure to comply with the preceding sentence shall be borne by Customer. In any event, the managing directors and personnel/human resource management of Customer are entitled to issue Instructions.

5.3. Customer shall inform Talkable immediately if processing by Talkable might lead to a violation of data protection regulations.

5.4. In the case claims based on Art. 82 GDPR are raised against Talkable, Customer shall reasonably support Talkable with its defense.

5.5. Customer shall name a person responsible for dealing with questions relating to applicable data protection law and data security in the context of performing this DPA.

6. SUBPROCESSING

6.1. In addition to the provisions contained in Clause 11 SCC, any subprocessor is obliged, before initiating the processing, to commit itself in writing to comply with the same data protection obligations as the ones under this DPA or legal Act within the meaning of Art. 28 para 3, 4 and 6 GDPR vis-à-vis Customer (the agreement must meet provide at least the level of data protection required by under this DPA). Where the subprocessor fails to fulfil its data protection obligations, Talkable shall remain fully liable to the Customer for the performance of the subprocessor's obligations.

6.2. Where a subprocessor refuses to be bound by the same data protection obligations as the ones under this DPA, Customer may consent thereto whereby such consent shall not be unreasonably withheld.

6.3. Talkable provides a website that lists all subcontractors to access personal data of its Customer as well as the limited or ancillary services they provide (the "Data Subprocessors"): [insert link]. Customer specifically authorizes and instructs Talkable to engage the Data Subprocessors listed on this website. At least 14 days before authorizing any new subcontractor to access personal data, Talkable will update its website, notify Customer and grant the opportunity to object to such change. Upon Customer's request, Talkable will provide all information necessary to demonstrate that the subprocessor will meet all requirements pursuant to Sect. 6.1 and 6.3. In the case Customer objects to the subprocessing, Talkable can choose to either not engage the subprocessor or to terminate the DPA with two (2) months prior written notice.

6.4. Third-party providers that maintain IT systems whereby access to Customer's personal data is not needed but can technically also not be excluded do not qualify as subprocessors within the meaning of this Sect. 6. They can be engaged based on regular confidentiality undertakings and subject to Talkable's reasonable monitoring.

7. LIABILITY

7.1. Customer and Talkable shall be each liable for damages of concerned data subjects according to Art. 82 GDPR (external liability):

7.1.1. Customer and Talkable shall be liable for all the damage caused by processing which infringes the GDPR.

7.1.2. Talkable's liability under Sect. 7.1.1 shall be limited to the damage caused by processing where it has not complied with obligations of the GDPR specifically directed to Talkable or where it has acted outside or contrary to lawful Instructions of the Customer.

7.1.3. Customer and Talkable shall be exempt from liability under Sect. 7.1.1 and 7.1.2 if they prove to not be in any way responsible for the event giving rise to the damage.

7.1.4. Where more than one Customer and Talkable, or both, the Customer and Talkable, are involved in the same processing and under Sect. 7.1.1 and 7.1.2 are responsible for any damage caused by processing, each Customer or Talkable shall be held liable for the entire damage.

7.1.5. Sect. 7.1.1, 7.1.2, 7.1.3 and 7.1.4 shall apply only, where more beneficial for End-Customer as compared to Clause 3 and 6 SCC. In any other case, Clauses 3 and 6 SCC shall prevail.

7.1.6. Customer and Talkable shall be entitled to claim back from the other Talkable or Customer that part of the compensation corresponding to their part of responsibility for the damage.

7.2. As regards the internal liability and without any effect as regards the external liability towards data subjects, the Parties agree that notwithstanding anything contained hereunder, when providing the Services, Talkable's liability for breach of any terms and conditions under this DPA shall be subject to the liability limitations agreed in the Terms of Service. Further, no EU Customer Affiliate shall become beneficiary of the DPA without being bound by this DPA and without accepting this liability limitation. Customer will indemnify Talkable from any exceeding claims of its EU Customer Affiliates or data subjects who claim rights based on alleged violation of this DPA including the SCC.

8. COSTS FOR ADDITIONAL SERVICES

If Customer's Instructions lead to a change from or increase of the agreed Services or in the case of Talkable's compliance with its obligations pursuant to Sects 4.6, 4.9 or 4.11 to assist Customer with Customer's own statutory obligations, Talkable is entitled to charge reasonable fees for such tasks which are based on the prices agreed for rendering the Services and/or notified to Customer in advance.

9. CONTRACT PERIOD

The rights, benefits and obligations of this DPA shall commence with the initiation of the Services and shall terminate with termination of the agreed Services under the Terms of Service.

10. MODIFICATIONS

Talkable may modify or supplement this DPA, with notice to Customer, (i) if required to do so by a supervisory authority or other government or regulatory entity, (ii) if necessary to comply with Applicable Law, (iii) to implement standard contractual clauses laid down by the European Commission or (iv) to adhere to an approved code of conduct or certification mechanism approved or certified pursuant to Articles 40, 42 and 43 of the GDPR.

11. TALKABLE'S USES

11.1. In respect of some processing of data subjects' personal data beyond providing the Services to the Customer, Talkable acts as an independent controller under Applicable Law. Specifically, Talkable may collect and process personal data for the purposes of providing various aspects of Talkable's services to data subjects beyond those relating to the Services (for example, for data subjects' ongoing access to and use of Talkable's software), conducting research and analysis to enable Talkable to improve its products and features (including optimization of Talkable's marketing campaigns), and communicating with data subjects for Talkable's marketing and promotional purposes ("Talkable's Uses"). Customer acknowledges and agrees that Talkable is the controller for Talkable's Uses.

11.2. For purposes of Talkable's Uses, Talkable will individually determine the purposes and means of processing personal data to the extent not explicitly prohibited under the Terms of Service, and will comply with the obligations applicable to it under Applicable Law with respect to the processing of personal data.

12. WRITTEN FORM

Any side agreements to this DPA as well as changes and amendments of this DPA, including this Sect. 12, shall be in writing.

13. INDEMNIFICATION

1. In addition to any indemnity obligations pursuant to the Terms of Service, each party (the "**Indemnifying Party**") shall be liable for and shall indemnify the other party (the "**Indemnified Party**") against any and all claims, actions, liabilities, losses, damages and expenses (including legal expenses) incurred by the Indemnified Party resulting from a violation of this DPA by the Indemnifying Party, including without limitation those arising out of any third-party demand, claim or action, including by a data protection authority, or any material breach of contract, negligence, fraud, willful misconduct, breach of statutory duty, or non-compliance with any Applicable Law. For the avoidance of doubt, the parties acknowledge and agree that the terms of this indemnification provision do not supersede, but rather are in addition to and are in no way inconsistent with any indemnification provision of the Terms of Service.

14. MISCELLANEOUS

14.1. For the determination of the data protection obligations, entitlement to provide orders and control, responsibilities, liabilities and consequences of objectives, the DPA shall prevail over all other agreements between the Parties.

14.2. The Services may only be amended, supplemented or changed upon the written agreement of the Parties.

14.3. In the event a clause under the Terms of Service has been found to violate the GDPR including all other Applicable Laws, the Parties will mutually agree on modifications to the Terms of Service to the extent necessary to ensure data privacy-law compliant processing.

Signatures:

_____	_____
[Customer]	Curebit, Inc. dba Talkable

Exhibit A – List of EU Customer Affiliates

Please list names and addresses of all EU Customer Affiliates or “None” if not applicable:

- _____
- _____
- _____
- _____
- _____

Exhibit B – Standard Contractual Clauses for Processors

Standard Contractual Clauses for Processors

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Customer and each of the EU Customer Affiliates as listed in Exhibit A are hereinafter referred to as the "**Data Exporter**" with respect to the personal data provided by that Data Exporter.

Talkable as defined in the DPA is hereinafter referred to as the "**Data Importer**".

The Data Exporter(s) and the Data Importer, each a "party" and collectively "the parties" HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the Data Exporter to the Data Importer of the personal data specified in **Appendix 1**.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the Data Exporter'* means the controller who transfers the personal data;

(c) *'the Data Importer'* means the processor who agrees to receive from the Data Exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the Data Importer or by any other subprocessor of the Data Importer who agrees to receive from the Data Importer or from any other subprocessor of the Data Importer personal data exclusively intended for processing activities to be carried out on behalf of the Data Exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law***'** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the Data Exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the Data Exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the Data Importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the Data Exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the Data Exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the Data Exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the Data Exporter

The Data Exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the Data Exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the Data Importer to process the personal data transferred only on the Data Exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the Data Importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the

transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the Data Importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the Data Exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the Data Importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the Data Importer

The Data Importer agrees and warrants:

(a) to process the personal data only on behalf of the Data Exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the Data Exporter of its inability to comply, in which case the Data Exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the Data Exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the Data Exporter as soon as it is aware, in which case the Data Exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the Data Exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the Data Exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the Data Exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the Data Exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the Data Exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the Data Exporter;

(h) that, in the event of subprocessing, it has previously informed the Data Exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the Data Exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor, is entitled to receive compensation from the Data Exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the Data Exporter, arising out of a breach by the Data Importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the Data Exporter has factually disappeared or ceased to exist in law or has become insolvent, the Data Importer agrees that the data subject may issue a claim against the Data Importer as if it were the Data Exporter, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

   The Data Importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the Data Exporter or the Data Importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the Data Exporter or the Data Importer, unless any successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The Data Importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the Data Importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the Data Exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The Data Exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the Data Importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the Data Exporter under the applicable data protection law.

3. The Data Importer shall promptly inform the Data Exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the Data Importer, or any subprocessor, pursuant to paragraph 2. In such a case the Data Exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the Data Exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The Data Importer shall not subcontract any of its processing operations performed on behalf of the Data Exporter under the Clauses without the prior written consent of the Data Exporter. Where the Data

Importer subcontracts its obligations under the Clauses, with the consent of the Data Exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the Data Importer under the Clauses (This requirement may be satisfied by the subprocessor co-signing the contract entered into between the Data Exporter and the Data Importer which is based on the terms and conditions of this Agreement.). Where the subprocessor fails to fulfil its data protection obligations under such written agreement the Data Importer shall remain fully liable to the Data Exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the Data Importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the Data Exporter or the Data Importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the Data Exporter is established.

4. The Data Exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the Data Importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the Data Exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the Data Importer and the subprocessor shall, at the choice of the Data Exporter, return all the personal data transferred and the copies thereof to the Data Exporter or shall destroy all the personal data and certify to the Data Exporter that it has done so, unless legislation imposed upon the Data Importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the Data Importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The Data Importer and the subprocessor warrant that upon request of the Data Exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the Data Exporter(s):		**On behalf of the Data Importer:**	
[_____]		**TALKABLE**	
Signature:	_____	Signature:	_____
Print Name:	_____	Print Name:	_____
Print Title:	_____	Print Title:	_____
Date:	_____	Date:	_____

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data Exporter
[description of your EU customer that contracts with Talkable and sends over the data.].

Data Importer

TALKABLE is engaged in providing an enterprise software-as-a-service-platform for online tracking services serving online businesses. Talkable is a referral marketing platform that allows its clients' customers (the "Customers") to share offers with their friends via email and social share channels.

Data Subjects
The processing can include the following categories of Data Subjects:

- *Customers.*
- *Data Exporter's employees, contractors, or agents (collectively, the "Admin Users") in their capacity as administrative users of the Services.*

Categories of Data

Customers' first names, last names, email addresses, coupon codes, cart details, billing/shipping addresses, IP addresses, subtotal of purchases made by Customers, and certain personal custom attributes of Customers (e.g. height, eye color, or hair color, etc.).

Admin Users' email addresses.

Special Categories of Data (if appropriate)
None

Processing Operations

- Talkable provides its customers (i.e. the Data Exporters) with the ability to generate a "refer-a-friend" functionality on their website.
- If this functionality is activated, an End-Customer ("**Advocate**") refers another (potential) End-Customer ("**Friend**") to the customer and both will be rewarded for a successful referral. The referred Friend gets a discount off the first purchase from the customer, third-party gift card, or product reward.
- In order for this to take place, the Advocate enters his own email address and the email address of the Friend on the customer's website or sends the Friend a referral link to the customer's website via email or through various social media and messaging platforms. The Friend is then assigned a coupon code, which can be redeemed during the first purchase on the customer's website.
- The Advocate can be identified when logged into the customer's website; the customer will then pass the Advocate's email to Talkable in order to identify the Advocate and generate a future reward for the referral. The Advocate will receive a reward once the Friend has successfully made a purchase on the customer's website.
- Talkable receives End-Customers' data, including name, email address, and IP address, and shipping address through shopping cart integration.

- Talkable uses stored personal data and customer data for reports generation inside the Talkable platform only on behalf of Data Exporter. Talkable sends emails to end customers: coupon codes, verification emails, etc.
- Talkable engages third party web-hosting services.

[*Signatures on following page*.]

On behalf of the Data Exporter(s):		**On behalf of the Data Importer:**	
[_____]		**CUREBIT, INC. dba TALKABLE**	
Signature:	_____	Signature:	_____
Print Name:	_____	Print Name:	_____
Print Title:	_____	Print Title:	_____
Date:	_____	Date:	_____

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

Description of the technical and organizational security measures implemented by the Data Importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Sub-Processors will be bound to adhere to similar but not identical organizational security measures which shall not fall below the level of data security as agreed herein. Any organizational security measures are subject to change as technical standards evolve and such changes can be implemented by Data Importer. If so requested, data importer will provide data exporter with a description of the then current measures.

The technical and organizational security measures of subprocessor AWS may be found here: https://aws.amazon.com/security/?nc=sn&loc=0.

1. Access control to premises and facilities:

- Talkable has physical offices in office buildings located in San Francisco, California. Talkable implements a Key Control Policy in order to manage the distribution and usage of keys.
- The San Francisco building is monitored by security cameras and is secured by smart, electronic, keycard enabled door locks.
- Talkable's San Francisco office requires an electronic key card to access the building beyond the lobby. Key points within the San Francisco office building are monitored by security cameras.
- Offices are secured outside of regular business hours.
- In addition, all server locations are secured as described in the AWS technical and organizational security description.

2. Access control to systems:

Technical (ID/password security) and organizational (user master data) measures for user identification and authentication:

- Password procedures: Talkable employs two authentication standards- Salt, a one-way encryption that hashes a password, as well as Scrypt, a password-based key derivation function, to require strong passwords. Access is managed within Talkable on the Users and Privileges Panel. The following user states apply to accounts: created, activated or disabled. Additional, clients can restrict these active users based on role: read, write and/or admin.
- All data is transmitted over Secure HTTPS (SHA-256 with RSA Encryption).
- Users are blocked after 20 unsuccessful login attempts
- Inactive users are logged out after 2 weeks of inactivity
- All data is encrypted inside the application database

3. Access control to data:

Requirements-driven definition of the authorization scheme and access rights, and monitoring and logging of accesses:

- Access is managed within Talkable on Users and Privileges Panel. The following user states apply to accounts: created, activated or disabled. Additionally, clients can restrict these active users based on role: read, write and/or admin.
- At implementation, the Talkable team will supply an implementation document that client's developers can use for integration. Talkable does not directly access client's network/server/database except in rare occurrences with specified scope and with explicit permission granted.
- Persons authorised to process personal data have committed themselves to confidentiality when signing a contractual NDA.

4. Disclosure Control:

Measures to transport, transmit and communicate or store data on data media (manual or electronic) and for subsequent checking:

- Talkable platform has a logging system which stores user actions of data changes
- All data is transmitted over Secure HTTPS (SHA-256 with RSA Encryption), SFTP or FTPS.
- All servers (incl'd) are situated in private network. SSH connection possible only via VPN. HTTP(S) requests via proxy to web servers. All other ports/protocols are closed. Production and Staging environment are isolated from each other on network layer. Each server group (e.g. web, app, database, redis,...) have separate firewall rule lists. Managed by Amazon Web Services Security Group. We use principle of a single-function server (app, web, database, redis, …) with separate list of needed package, users and firewall rules. All infrastructure for storage and processing is located at, and managed by, Amazon Web Services.
- Talkable offices maintain secure wired and wireless networks. The Talkable platform is hosted on a secure server. Outside of Talkable offices, developers and production environments are only accessible via a VPN.

5. Input Control:

Measures for subsequent checking whether data have been entered, changed or removed (deleted), and by whom:

Example:

- Talkable employs CloudTrail in tandem with AWS IAM.
- Talkable platform has a logging system which stores user actions of data changes
- Talkable also collects system and web server access logs

6. Job control:

Measures (technical/organizational) to segregate the responsibilities between the Data Exporter and the Data Importer:

- Logical controls inside the platform
- Separate processes for data import / export

7. Availability Control:

Measures to assure data security (physical/logical):

- Database backups occur every 24 hours and Talkable implements real time master-slave replication
- Talkable infrastructure works on Linux-based operating systems that don't require anti-virus software. All workstations are also Linux-based, except a couple that are on Windows: they have anti-virus software installed
- Talkable issues Apple MacBook computers, which leverage Unix and are not as prone to malware and viruses as other models.
- By employing Amazon Web Services to host Talkable client data, we rely on their infrastructure to be in compliance with stringent data warehousing requirements, including EU data privacy laws and the opening of an AWS region in Montreal, Canada.

8. Separation Control:

Measures to provide for separate processing (storage, amendment, deletion, transmission) of data for different purposes:

- Platform users are limited to access data of a particular site
- Client integration libraries are stored as static pre-generated files
- Custom integration processing logic is running as a separate service

On behalf of the Data Exporter(s):		**On behalf of the Data Importer:**	
[_____]		**CUREBIT, INC. dba TALKABLE**	
Signature:	_____	Signature:	_____
Print Name:	_____	Print Name:	_____
Print Title:	_____	Print Title:	_____
Date:	_____	Date:	_____