DATA PROCESSING ADDENDUM

This **Data Processing Addendum** ("**DPA**") is incorporated by reference into and made a part of the Subscription Services Agreement ("**Agreement**") and all related orders entered into between Celerius Group, Inc. (dba FunnelEnvy) ("**Company**") and _____ ("**Client**"). This DPA sets forth certain duties and obligations of the parties with respect to the protection, security, processing, and privacy of personal data provided or made available to Company by Client as part of the Services provided by Company for Client under the Agreement. This DPA shall supplement (and not supersede) the Agreement and shall take precedence solely to the extent of any conflict between this DPA and the Agreement.

During Company's provision of Services to Client pursuant to the Agreement, Company may Process certain Personal Data provided or made available to Company by Client on behalf of Client. The parties agree to comply with the following provisions with respect to any such Personal Data, each acting reasonably and in good faith.

1. DEFINITIONS. All capitalized terms used and not expressly defined in this Addendum shall have the meanings given to them in the Agreement. "**Controller**," "**Personal Data**," "**Personal Data Breach**," "**Processor**," "**Processing**," "**Supervisory Authority**," and "**Third Party**" each have the meaning given to it in the GDPR.

1.1 "**Client Data**" means Personal Data that is uploaded or submitted to the Services by Client that Company Processes on behalf of Client as part of the Services.

1.2 "**Data Protection Laws and Regulations**" means those laws and regulations applicable to a party in connection with Processing of Personal Data under the Agreement, which may include, to the extent applicable, the laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom.

1.3 "**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

1.4 "**GDPR**" means the General Data Protection 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.

1.5 "**Security Documentation**" means Company's security documentation applicable to the Services, as updated from time to time.

1.6 "**Standard Contractual Clauses**" means the agreement executed by and between Client and Company. and attached hereto as Schedule 1 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.

1.7 "**Sub-processor**" means any Third Party engaged by Company as a Processor.

2. PROCESSING OF CLIENT DATA

2.1 Roles. Client is the Controller and Company is the Processor with regard to the Processing of Client Data under the Agreement.

2.2 Scope. Company acknowledges that Client, as a Controller, must comply with privacy, data protection, and data security laws, treaties, rules, codes, and regulations applicable to Client which require any third parties Processing Personal Data on Client's behalf to abide by certain privacy, confidentiality and security terms and restrictions for any such Personal Data provided or made available by Client to such third parties. The purpose of this DPA is to set out Company's capabilities for appropriately safeguarding Personal Data provided or made available to Company by Client (i.e., Client Data) and Company's contractual commitment to protect such Personal Data.

2.3 Client's Processing of Personal Data. In connection with Company's provision of the Services to Client, Client will provide Personal Data to Company. Such Personal Data is Client Data for the purposes of this DPA. Client shall (a) collect and Process Client Data, (b) use the Services, and (c) give Company instructions regarding the Processing of Client Data for Client, in all cases, in accordance with all applicable laws, rules, and regulations, including the Data Protection Laws and Regulations. Client is solely liable and responsible for the accuracy, quality, and legality of Client Data.

2.4 Company's Processing of Client Data. Company shall only Process Client Data on behalf of and in accordance with Client's instructions set forth in this DPA and the Agreement for the following purposes: (a) Processing in accordance with the Agreement and applicable Order Forms; (b) Processing initiated by Users in their use of the Services; and (c) Processing to comply with other documented reasonable instructions provided by Client in writing where such instructions are consistent with the terms of the Agreement. The subject-matter and purpose of Processing of Client Data by Company is solely so that Company can provide the Services to Client pursuant to the Agreement. The duration of the Processing shall be for the duration of the Agreement or

Order Form, applicable. Effective as of 25 May 2018, Company shall Process Client Data in accordance with this DPA and the GDPR requirements directly applicable to Company's provision of its Services. Client Data shall be considered Client's Confidential Information under the Agreement.

2.5 Personnel. Company shall ensure that its personnel engaged in the Processing of Client Data are informed of the confidential nature of the Client Data, have received appropriate training on their responsibilities and have executed written, industry standard confidentiality agreements. Company shall ensure that Company's access to Client Data is limited to those of its personnel performing Services in accordance with the Agreement.

3. RIGHTS OF DATA SUBJECTS. Company shall, to the extent legally permitted, promptly notify Client if Company receives a request from a Data Subject to exercise the Data Subject's rights under the GDPR ("Data Subject Request"). Taking into account the nature of the Processing, Company shall assist Client by using appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Client's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Client, in its use of the Services, does not have the ability to address a Data Subject Request, Company shall upon Client's request provide commercially reasonable efforts to assist Client in responding to such Data Subject Request, to the extent Company is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Client shall be responsible for any costs arising from Company's provision of such assistance.

4. SUB-PROCESSORS

4.1 Appointment of Sub-processors. Client acknowledges and agrees that Company may engage Sub-processors in connection with the provision of the Services. Company has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this Agreement with respect to the protection of Client Data to the extent applicable to the nature of the Services provided by such Sub-processor.

4.2 List of Current Sub-processors and Notification of New Sub-processors. Client hereby approves and authorizes the following list of Company's current Sub-processors for the Services which includes the identities of those Sub-processors and their country of location ("Sub-processor Lists"). Company shall provide Client notification of any potential new Sub-processors before authorizing any new Sub-processors to Process Client Data.

Sub-Processor	Location	Service
Amazon Web Services	United States	Secure cloud platform for compute and storage

4.3 Objection Right for New Sub-processors. Client may object to Company's use of a new Sub-processor by notifying Company promptly in writing within 10 business days after receipt of Company's notice. In the event Client objects to a new Sub-processor, as permitted in the preceding sentence, Company will use reasonable efforts to make available to Client a change in the Services or recommend a commercially reasonable change to Client's configuration or use of the Services to avoid Processing of Client Data by the objected-to new Sub-processor without unreasonably burdening the Client. If Company is unable to make available such change within a reasonable period of time, which shall not exceed 30 days, Client may terminate the applicable Order Forms with respect only to those Services which cannot be provided by Company without the use of the objected-to new Sub-processor by providing written notice to Company. Company will refund Client any prepaid fees covering the remainder of the term of such Order Forms following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Client.

4.4 Responsibility. Company shall be liable for the acts and omissions of its Sub-processors to the same extent Company would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

5. SECURITY

5.1 Controls for the Protection of Client Data. Company has implemented and shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk posed by the Processing. Company's measures will include those set forth in the Security Documentation. Company regularly monitors compliance with these measures. Company will not materially decrease the overall security of the Services during a subscription term.

5.2 Third-Party Certifications and Audits. Company has obtained the third-party certifications and audits set forth in the Security Documentation. Upon Client's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Company shall make available to Client (or Client's

independent, third-party auditor) a copy of Company's then most recent third-party audits or certifications, as applicable.

6. CLIENT DATA INCIDENT MANAGEMENT AND NOTIFICATION. Company maintains security incident management policies and procedures specified in the Security Documentation. and shall, notify Client without undue delay, but in no event in less than 48 hours, after becoming aware of a Personal Data Breach with regard to Client Data transmitted, stored or otherwise Processed by Company or its Sub-processors of which Company is aware (a "**Client Data Incident**"). Company shall use commercially reasonable efforts to identify the cause of such Client Data Incident and take those steps as Company deems necessary and reasonable in order to remediate the cause of such a Client Data Incident to the extent the remediation is within Company's reasonable control. The obligations herein shall not apply to incidents that are caused by Client or Client's Users.

7. RETURN AND DELETION OF CLIENT DATA. Company shall return Client Data to Client or, to the extent allowed by applicable law, delete Client Data in accordance with the procedures and timeframes specified in the Security Documentation, or as requested by Client.

8. GDPR AND ONWARD TRANSFER

8.1 Assistance. As required by the GDPR, Company shall provide Client with reasonable cooperation and assistance needed to fulfil Client's obligation under the GDPR.

8.2 Standard Contractual Clauses. The Standard Contractual Clauses apply to any transfers of Client Data under this DPA from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to Company's facilities in countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations, to the extent such transfers are subject to such Data Protection Laws and Regulations.

(a) Instructions. For the purposes of Section 2 of the DPA and Clause 5(a) of the Standard Contractual Clauses, the following acts are deemed an instruction by the Client to process Client Data: (a) Client's entering into the Agreement and applicable Order Forms are deemed instructions to Process Client Data as is necessary to perform services under the Agreement; (b) Users actions that initiate Processing while using the Services; and (c) Client's other documented reasonable written instructions provided by Client (e.g., via email) where such instructions are consistent with the terms of the Agreement.

(b) Notification of New Sub-processors and Objection Right for new Sub-processors. Pursuant to Clause 5(h) of the Standard Contractual Clauses, Client acknowledges and expressly agrees that Company may engage new Sub- processors as described in the DPA.

(c) Copies of Sub-processor Agreements. The parties agree that Company may redact the copies of the Sub-processor agreements that must be provided by Company to Client pursuant to Clause 5(j) of the Standard Contractual Clauses to remove commercial information, confidential information, and clauses unrelated to the Standard Contractual Clauses or their equivalent. Company will provide copies of the Sub-processor agreements, only upon request by Client.

(d) Audits and Certifications. The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the following specifications. Client request an on-site audit of the procedures relevant to the protection of Client Data, and Client and Company shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Client shall be responsible. Client shall promptly notify Company with information regarding any non-compliance discovered during the course of an audit.

8.3 Certification of Deletion. The parties agree that the certification of deletion of Client Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Company to Client only upon Client's request.

8.4 Conflict. In the event of any conflict or inconsistency between the body of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

The parties by their authorized representatives have entered into this Data Processing Addendum as of the date set forth below.

Client:	**Company: Celerius Group, Inc.**
Signature: _____	Signature: 
Printed: _____	Printed: Arun Sivashankaran
Title: _____	Title: CEO
Date: _____	Date: 06 / 03 / 2018

SCHEDULE 1 - STANDARD CONTRACTUAL CLAUSES

Commission Decision C(2010)593
Standard Contractual Clauses (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

Name of the data exporting organisation:.....

Address:.....

Tel.: .....; fax: .....; e-mail: .....

Other information needed to identify the organisation:

……
(the data **exporter**)

And

Name of the data importing organisation: Celerius Group, Inc.

Address: 120 S El Camino Real, Suite 17, Millbrae CA 94030

Tel.: 888.562.2779; fax: 415.619.5497; e-mail: security@funnelenvy.com

Other information needed to identify the organisation: N/A

(the data **importer**)

each a “party”; together “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 of 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, namely [insert country]

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. 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, namely [insert country]

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:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

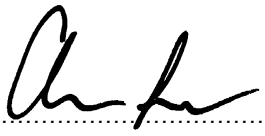
On behalf of the data importer:

Name (written out in full): Arun Sivashankaran

Position: CEO

Address: 120 S El Camino Real, Suite 17, Millbrae CA 94030

Other information necessary in order for the contract to be binding (if any): N/A

Signature 

(stamp of organisation)

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

The data exporter is (please specify briefly your activities relevant to the transfer):

The data exporter is: (i) the legal entity that has executed the Standard Contractual Clauses as a data exporter and, (ii) all Affiliates (as defined in the DPA into which these Standard Contractual Clauses are incorporated) of the data exporter on whose behalf data importer processes personal data of data subjects located in the European Economic Area (EEA), Switzerland or the United Kingdom.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Data importer is a provider of automated marketing services which may involve processing personal data provided by, and pursuant to the instructions and directions of, the data exporter in accordance with the terms of the DPA and the Subscription Services Agreement and all related orders between data exporter and data importer (the "Agreement").

Data subjects

The personal data transferred concern the following categories of data subjects (please specify briefly activities relevant to the transfer):

The categories of data subjects whose personal data may be processed in connection with the services are determined and controlled by data exporter in its sole discretion and may include but are not limited to: customer, contacts and prospects of data exporter; employees or contractors of data exporter's customers, contacts and prospects, and; employees and contractors of data exporter.

Categories of data

The personal data transferred concern the following categories of data (please specify):

The categories of personal data are determined by data exporter in its sole discretion and may include but are not limited to: first and last name; employer; business role; professional title; contact information (e.g. email, phone, physical address); business network; business experience; business interests; localization data, and; device identification data.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

None

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Data importer will process personal data as necessary to perform the services pursuant to the Agreement. The processing operations performed on the personal data will depend on the scope of data exporter's services and data exporter's configuration of its FunnelEnvy instance. Such processing operations of personal data as necessary for data importer to provide the services may include the following: collecting. recording, organizing, storage, use, alteration, transmission, retrieval, consultation, archiving and / or destruction.

DATA EXPORTER:

Name:

Authorised Signature:

DATA IMPORTER: Celerius Group, Inc.

Name: Arun Sivashankaran

Authorised Signature

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 organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

1. Security Requirements. Data importer has implemented the technical and organizational measures set forth in this Schedule1. The measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, and unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network. These measures ensure a level of security appropriate to the risks presented by the processing and the nature of the personal data to be protected having regard to the state of the art and the cost of their implementation.

2. Security Program. Without limiting the foregoing, data importer has implemented a comprehensive, written information security program that: (a) materially conforms with the ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements, (b) is and at all times will be in compliance with all Data Protection Laws and Regulations, and (c) contains industry standard technical, physical, administrative and organizational security measures.

3. Security Measures. Data importer has in place and shall maintain the following specific security measures. Data importer has:

3.1 adopted and implemented reasonable policies and standards related to security;

3.2 assigned responsibility for information security management;

3.3 devoted adequate personnel resources to information security;

3.4 conducted appropriate background checks and requires employees, vendors and others with access to the personal data to enter into written confidentiality agreements;

3.5 conducted training to make employees and others with access to personal data aware of information security risks and to enhance compliance with its policies related to data protection;

3.6 implemented security measures designed to prevent unauthorized access to personal data through the use, as appropriate, of physical and logical entry controls, secure areas for data processing, procedures for monitoring the use of data processing, audit trails, use of secure passwords, network intrusion detection technology, authentication technology, secure log-on procedures, and virus protection, on-going monitoring of compliance with its policies related to data protection. These measures include implementation of:

(a) appropriate physical access control measures (e.g., access ID cards, card readers, desk officers, alarm systems, motion detectors, burglar alarms, video surveillance and exterior security);

(b) denial-of-use control measures to prevent unauthorized use of data protection systems (e.g., automatically enforced password complexity and change requirements, firewalls, etc.);

(c) requirements-driven authorization scheme and access rights, and monitoring and logging of system access to identify unauthorized Processing of personal data by authorized personnel;

(d) data transmission control measures to ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission, transport or storage on data media, and transfer and receipt records;

(e) encryption of any personal data transmitted electronically to a person outside data importer's IT system, transmitted over a wireless network, or stored on any movable or portable media;

(f) data entry control measures to ensure that it is possible to check and establish whether and by whom personal data has been input into data processing systems, modified, or removed;

(g) subcontractor supervision measures to ensure compliance with the DPA;

(h) measures to ensure that personal data is protected from accidental destruction or loss including, as appropriate and without limitation, data backup, retention and secure destruction policies; secure offsite storage of data sufficient for disaster recovery; and disaster recovery programs; and

(i) measures to ensure that data collected for different purposes can be processed separately including, as appropriate, physical or adequate logical separation of personal data;

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

DATA EXPORTER

Name:…….. Authorised Signature ……

DATA IMPORTER

Name: Arun Sivashankaran…….. Authorised Signature ……