

Hevo Data

Data Processing Addendum

This Data Protection Addendum ("**Addendum**") dated _____ ("**Effective Date**") forms part of the principal agreement dated _____, or the Terms of Service, as applicable ("**Principal Agreement**"), between _____ ("**Customer**", including its successors and permitted assigns) and Hevo Data, Inc. ("**Hevo**", including its successors and permitted assigns) pursuant to which Hevo or any Hevo Affiliate (*as defined below*) provides Services (*as defined below*) to the Customer.

Capitalized terms not otherwise defined in this Addendum shall have the meanings given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

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

1. Definitions

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

1.1.1 "**Applicable Laws**" means (a) European Union or Member State laws with respect to any Customer Personal Data in respect of which the Customer is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Customer Personal Data in respect of which the Customer is subject to any other Data Protection Laws;

1.1.2 "**Customer Identification Data**" means the Personal Data that is provided by the Customer to Hevo and/or a Hevo Affiliate, as requested by Hevo, at the time of signing up for the Services, whether through the website www.hevodata.com or through an agreement;

1.1.3 "**Customer Personal Data**" means the Personal Data Processed by Hevo and/ or a Hevo Affiliate on behalf of the Customer pursuant to the provision of the Services. Customer Personal Data would not, however, include the Customer Identification Data;

1.1.4 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.5 "**EU Data Protection Laws**" means the GDPR and as amended, replaced or superseded from time to time, laws implementing or supplementing the GDPR including as transposed into domestic legislation of each Member State;

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

- 1.1.7 “**Hevo Affiliate**” means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Hevo, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.
- 1.1.8 “**Restricted Transfer**” means:
- 1.1.8.1 a transfer of Customer Personal Data from the Customer to Hevo and/ or a Hevo Affiliate; or
 - 1.1.8.2 an onward transfer of Customer Personal Data from Hevo to a Hevo Affiliate; or
 - 1.1.8.3 an onward transfer of Customer Personal Data from Hevo and/ or a Hevo Affiliate to another Sub-Processor,
- in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established under section 13 below;
- 1.1.9 “**Services**” means the services and other activities to be supplied to or carried out by or on behalf of Hevo for the Customer pursuant to the Principal Agreement;
- 1.1.10 “**Standard Contractual Clauses**” means the contractual clauses set out in Annex 2 pursuant to the European Commission’s decision (C(2010)593) of February 05, 2010 on Standard Contractual Clauses for the transfer of Personal Data to Processors established in third party countries which do not ensure an adequate level of protection; and
- 1.1.11 “**Subprocessor**” means any person (including any third party, but excluding an employee of Hevo) appointed by or on behalf of Hevo or any Hevo Affiliate to Process Customer Personal Data on behalf of Customer in connection with the Principal Agreement
- 1.2 The terms, “**Commission**”, “**Controller**”, “**Data Subject**”, “**Member State**”, “**Personal Data**”, “**Personal Data Breach**”, “**Processing**” and “**Supervisory Authority**” shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing by Hevo Affiliate

- 2.1 Hevo warrants and represents that, before any Hevo Affiliate Processes any Customer Personal Data on behalf of the Customer, Hevo's entry into this Addendum as agent for and on behalf of that Hevo Affiliate will have been duly and effectively authorised (or subsequently ratified) by that Hevo Affiliate. Hevo shall continue to be liable for any acts or actions of any Hevo Affiliate.
- 2.2 The Customer acknowledges and agrees that any Processing under this Agreement may also be carried out by any Hevo Affiliate, and the Hevo Affiliate shall assume the obligations of Hevo, in its capacity of Processor, for any such Processing under this Agreement.

3. Processing of Customer Personal Data

- 3.1 The Customer is the Controller and Hevo and/or Hevo Affiliate are the Processor of Customer Personal Data. To the extent any Customer Identification Data is considered Personal Data, Hevo and/or Hevo Affiliate would be the Controller of such Customer Identification Data, and would Process such data in accordance with Hevo's privacy policy, which is available at www.hevodata.com/privacy/customers.
- 3.2 Each party will comply with its respective obligations under Applicable Laws with respect to processing of Customer Personal Data.
- 3.3 The Customer acknowledges that the Customer Personal Data may be Processed from a Hevo Affiliate, from time to time, subject to such Hevo Affiliate being bound by all of the obligations applicable to Hevo under this Addendum and Hevo being responsible for the Hevo Affiliate's obligations under this Addendum.
- 3.4 The subject-matter of the data processing covered by this Addendum is the provision of the Services and the processing will be carried out for the duration of the Principal Agreement, except insofar as Hevo and/or Hevo Affiliate is required to process such data thereafter, in accordance with its obligations under applicable law. Hevo shall have provided the Customer relevant details of any Hevo Affiliate which acts as a Processor under this Addendum.
- 3.5 Hevo and each relevant Hevo Affiliate shall:
- 3.5.1 comply with applicable Data Protection Laws in the Processing of Customer Personal Data; and
 - 3.5.2 not Process Customer Personal Data other than on the Customer's documented instructions, or as set out in the Principal Agreement or this Addendum or as otherwise notified by the Customer from time to time, unless Processing is required by Applicable Laws to which the Customer is subject, in which case Hevo and/or Hevo Affiliate shall to the extent permitted by Applicable Laws inform the Customer of that legal requirement before the relevant Processing of that Personal Data.
- 3.6 Annex 1 to this Addendum sets out certain information regarding Hevo or and each Hevo Affiliate's or its Subprocessors' Processing of the Customer Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection

Laws). Nothing in Annex 1 confers any right or imposes any obligation on any party to this Addendum.

4. Responsibilities of Customer; Indemnity

4.1 The Customer:

4.1.1 instructs Hevo and each Hevo Affiliate (and authorises Hevo and each Hevo Affiliate to instruct each Subprocessor) to:

4.1.1.1 Process Customer Personal Data; and

4.1.1.2 in particular, transfer Customer Personal Data to any country or territory,

as reasonably necessary for the provision of the Services and consistent with the Principal Agreement;

4.1.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 4.1; and

4.1.3 warrants and represents that it has complied with applicable Data Protection Laws in respect of any obligations that it has under applicable Data Protection Laws with respect to it being the Controller of Customer Personal Data. The Customer further represents and warrants that it has collected the Customer Personal Data in accordance with applicable Data Protection Laws.

4.2 Customer's instructions to Hevo and each Hevo Affiliate for the processing of Customer Personal Data shall comply with all Applicable Laws. Customer shall be responsible for the Customer Personal Data and the means by which Customer acquired Customer Personal Data.

4.3 The Customer agrees to defend, indemnify and hold harmless Hevo and/or the relevant Hevo Affiliate from and against all claims, actions, third party claims, direct losses, damages and expenses incurred by Hevo and/ or the relevant Hevo Affiliate as a result of or in connection with the Customer's non-compliance with any applicable Data Protection Laws.

5. Hevo and Hevo Affiliate Personnel

Hevo and each Hevo Affiliate shall take reasonable steps to ensure the reliability of any employee, agent or contractor of Hevo and the Hevo Affiliate who may have access to the Customer Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Customer Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to Hevo or the Hevo Affiliate, as applicable, ensuring that all such individuals are subject to required confidentiality obligations.

6. Security

6.1 Hevo's and Hevo Affiliate's Security Measures

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

- 6.1.2 In assessing the appropriate level of security, Hevo and each Hevo Affiliate shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.
- 6.1.3 Hevo and each Hevo Affiliate shall be responsible to ensure that each of its Subprocessors complies with the obligations as set out in this Section 6.

6.2 **Customer's Security Responsibilities**

- 6.2.1 Without prejudice to Hevo's and the relevant Hevo Affiliate's obligations under Section 6.1 (Hevo's and Hevo Affiliate's Security Measures):
 - 6.2.1.1 Customer is solely responsible for its use of the Services, including: (i) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Personal Data; (ii) securing the account authentication credentials, systems and devices Customer uses to access the Services; and (iii) backing up the Customer Personal Data; and
 - 6.2.1.2 Customer acknowledges that Hevo and each Hevo Affiliate has no obligation to protect Customer Personal Data that Customer elects to store or transfer outside of Hevo's and each Hevo Affiliate's and its Sub-processors' systems (for example, offline or online premises storage.)
- 6.2.2 Customer is responsible for reviewing Hevo's and Hevo Affiliate's Security Measures and evaluating for itself whether the Services, Hevo's and Hevo Affiliate's Security Measures and Hevo's and Hevo Affiliate's security commitments under this Section will meet Customer's needs, including with respect to compliance with Data Protection Laws. Customer acknowledges and agrees that the Security Measures undertaken by Hevo and Hevo Affiliates meet a level of security appropriate to the risk in respect of the Customer Personal Data, and the Customer will be responsible if the Security Measures do not meet the standard of appropriateness as required by the GDPR.

7. **Subprocessing**

- 7.1 The Customer authorises Hevo and each Hevo Affiliate to appoint (and permit each Subprocessor appointed in accordance with this section 7 to appoint) Subprocessors in accordance with this section 7 and subject to any restrictions in the Principal Agreement.
- 7.2 Hevo and each Hevo Affiliate may continue to use those Subprocessors already engaged by Hevo and each Hevo Affiliate as at the date of this Addendum, subject to Hevo and each

Hevo Affiliate in each case as soon as practicable meeting the obligations set out in section 7.4. A list of such sub-processors is provided at [Annex 3](#)

7.3 Hevo and/or the relevant Hevo Affiliate shall give Customer prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within 10 (ten) days of receipt of that notice, Customer notifies Hevo and/or the relevant Hevo Affiliate in writing of any objections (on reasonable grounds) to the proposed appointment Hevo and/or the relevant Hevo Affiliate shall work with Customer in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Subprocessor.

7.4 With respect to each Subprocessor, Hevo and/or the relevant Hevo Affiliate shall:

7.4.1 ensure that the arrangement between on the one hand (a) Hevo, or (b) the relevant Hevo Affiliate, and on the other hand the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Customer Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR;

7.4.2 if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) Hevo, or (b) the relevant Hevo Affiliate, and on the other hand the Subprocessor, or before the Subprocessor first Processes Customer Personal Data procure that it enters into an agreement incorporating the Standard Contractual Clauses with the Customer; and

7.4.3 provide to Customer for review such copies of Hevo's or the relevant Hevo Affiliate's agreements, as applicable, with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as Customer may request from time to time.

8. **Data Subject Rights**

8.1 Taking into account the nature of the Processing, Hevo and/or the relevant Hevo Affiliate shall assist the Customer by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligations, as reasonably understood by Customer, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

8.2 As of the Effective Date of this Addendum for the duration of the period that Hevo and/or the relevant Hevo Affiliate provides the Services, Hevo and/or the relevant Hevo Affiliate shall:

8.2.1 without undue delay, notify Customer if Hevo and/or the relevant Hevo Affiliate or any of its Subprocessors receives a request from a Data Subject under any Data Protection Law in respect of Customer Personal Data; and

8.2.2 reasonably assist the Customer in responding to any requests received from a Data Subject, to the extent possible, if the Customer has requested, in writing, Hevo's assistance. It is clarified that Hevo and/or the relevant Hevo Affiliate or any of its Subprocessors shall not respond to that request except as required by Applicable Laws to which Hevo and/or the relevant Hevo Affiliate or any of its

Subprocessors is subject, as applicable, in which case Hevo and/or the relevant Hevo Affiliate shall to the extent permitted by Applicable Laws inform Customer of that legal requirement before Hevo and/or the relevant Hevo Affiliate or any of its Subprocessors responds to the request.

9. **Personal Data Breach**

9.1 Hevo and/or the relevant Hevo Affiliate shall notify Customer without undue delay upon Hevo and/or the relevant Hevo Affiliate or any Subprocessor becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information to allow the Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

9.2 Hevo and/or the relevant Hevo Affiliate shall co-operate with the Customer and take such reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

10. **Data Protection Impact Assessment and Prior Consultation**

Hevo and/or the relevant Hevo Affiliate shall provide reasonable assistance to the Customer with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Customer reasonably considers to be required of the Customer by Articles 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to, Hevo and/or the relevant Hevo Affiliate or any Subprocessor.

11. **Deletion of Customer Personal Data**

11.1 Subject to sections 11.2, Hevo and/or the relevant Hevo Affiliate shall without undue delay and in any event within 30 (thirty) calendar days of the date of cessation of any Services involving the Processing of Customer Personal Data (the “**Cessation Date**”), at the Customer’s request, delete and procure the deletion of all copies of those Customer Personal Data from its Subprocessors.

11.2 Hevo, Hevo Affiliates and their Subprocessors may retain Customer Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Hevo, the relevant Hevo Affiliate and their Subprocessors shall ensure the confidentiality of all such Customer Personal Data and shall ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

12. **Audit rights**

12.1 Subject to sections 12.2 and 12.3, upon Customer’s written request, at reasonable intervals, Hevo and/or the relevant Hevo Affiliate shall make available to Customer which is not a competitor of Hevo, information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by the Customer or an auditor mandated by the Customer, at the Customer’s cost, in relation to the Processing of the Customer Personal Data by Hevo and/or the relevant Hevo Affiliate and their Subprocessors, provided that such audit right is available to the Customer once yearly. Hevo and or the

relevant Hevo Affiliate shall assist in these audits in the form of provision of required information and facilitating interviews of relevant Hevo and/or the relevant Hevo Affiliate employees. However, Hevo and/or the relevant Hevo Affiliate will not be able to provide access to the SaaS platform operated by Hevo and/or the relevant Hevo Affiliate or otherwise let the auditors interact with the platform.

12.2 Information and audit rights of the Customer only arise under section 12.1 to the extent that the Principal Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

12.3 Customer shall give Hevo and/or the relevant Hevo Affiliate reasonable notice of any audit or inspection to be conducted under section 12.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to Hevo, the relevant Hevo Affiliate, and their Subprocessors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. Hevo, the relevant Hevo Affiliate and their Subprocessors need not give access to its premises for the purposes of such an audit or inspection:

12.3.1 to any individual unless he or she produces reasonable evidence of identity and authority; or

12.3.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Customer undertaking an audit has given notice to Hevo that this is the case before attendance outside those hours begins.

13. **Restricted Transfers**

13.1 Subject to section 13.3, the Customer (as "data exporter") and Hevo and/or the relevant Hevo Affiliate and their Subprocessors, as appropriate, (as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from the Customer to Hevo and/ or the relevant Hevo Affiliate or their Subprocessors.

13.2 The Standard Contractual Clauses shall come into effect under section 12.1 on the later of:

13.2.1 the data exporter becoming a party to them;

13.2.2 the data importer becoming a party to them; or

13.2.3 commencement of the relevant Restricted Transfer.

13.3 Section 13.1 shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

14. **General Terms**

Governing law and jurisdiction

- 14.1 Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses:
- 14.1.1 the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and
 - 14.1.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.

Order of precedence

- 14.2 Nothing in this Addendum reduces Hevo's obligations under the Principal Agreement in relation to the protection of Personal Data or permits Hevo and/ or the relevant Hevo Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Principal Agreement. In the event of any conflict or inconsistency between the provisions of this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.
- 14.3 Subject to section 14.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Principal Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

Severance

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

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out above or subject to the Customer's agreement to this Addendum through Customer's signup on Hevo platform or during the course of use of the Hevo platform.

Customer

Signature _____

Name _____

Title _____

Date Signed _____

Hevo Data, Inc.

Signature _____

Name _____

Title _____

Date Signed _____

ANNEX 1: DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

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

Subject matter and duration of the Processing of Customer Personal Data

- Hevo will process Customer Personal Data as necessary to provide the Service pursuant to the Principal Agreement, and as further instructed by Customer in its use of the Service. Hevo will process Personal Data for the duration that the Customer uses the Service, unless otherwise agreed in writing.

The nature and purpose of the Processing of Customer Personal Data

- Hevo will process Customer Personal Data as necessary to provide the Service pursuant to the Terms of Service, and as further instructed by Customer in its use of the Service.

The types of Customer Personal Data to be Processed

Customer may submit Personal Data to the Service, the extent of which is determined and controlled by Customer in its sole discretion, and which may include but is not limited to the following categories of Personal Data:

- First and Last Name
- Contact Information including email address, phone number, social media profiles
- Professional life data including employer, designation
- Personal life data including salutation, marital status, family details etc.
- Locational data
- Data available on social media (e.g., Facebook, Twitter, etc.) profiles, status and information
- Event and survey registration, attendance, and response data
- Engagement data, namely, articles, posts, and the like that is “followed”, “liked” or “disliked”
- Internet cookies
- Communication data like emails, chat, voicemail etc. Also, includes feedback and support related communication data.
- Comments and posts submitted to websites, mobile apps, and online communities

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

Customer may submit or share Personal Data in the course of using the Service, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

- Prospects, customers, business partners and vendors of data exporter
- Employees or contact persons of data exporter’s prospects, exporter’s customers, exporter’s business partners and exporter’s vendors
- Employees, agents, advisors, freelancers of data exporter
- Data exporter’s affiliates authorized by data exporter to use the Service

The obligations and rights of Customer

The obligations and rights of Customer are set out in the Principal Agreement and this Addendum.

ANNEX 2: STANDARD CONTRACTUAL CLAUSES

These Clauses are deemed to be amended from time to time, to the extent that they relate to a Restricted Transfer which is subject to the Data Protection Laws of a given country or territory, to reflect (to the extent possible without material uncertainty as to the result) any change (including any replacement) made in accordance with those Data Protection Laws (i) by the Commission to or of the equivalent contractual clauses approved by the Commission under EU Directive 95/46/EC or the GDPR (in the case of the Data Protection Laws of the European Union or a Member State); or (ii) by an equivalent competent authority to or of any equivalent contractual clauses approved by it or by another competent authority under another Data Protection Law (otherwise).

If these Clauses are not governed by the law of a Member State, the terms "Member State" and "State" are replaced, throughout, by the word "jurisdiction".

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: Hevo Data, Inc.

Address:

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

Other information needed to identify the organisation:

.....
(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.

Background

The data exporter has entered into a data processing addendum (“DPA”) with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. The servers to which Customer Personal Information may be transferred are located in a country which do not offer adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the Customer agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the data importer’s execution of, and compliance with, the terms of these Clauses.

Clause 1

Definitions

For the purposes of the Clauses:

- (a) *'personal data', 'special categories of data', 'process/processing', 'Customer', '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 exporter 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 reasonable 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, at the cost of the data exporter;
- (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 will keep the data exporter intimated of any subprocessors that it appoints;
- (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 intimation to the data exporter of such subprocessor. Where the data importer subcontracts its obligations under the Clauses, 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.
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.....

On behalf of the data importer:

Name (written out in full):

Position:

Address:

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

Signature.....

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 _____, (the “Customer”) who has executed the Principal Agreement with Hevo.

Data importer

The data importer is Hevo Data, Inc. (“Hevo”).

Data subjects

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

Data exporter may submit or share Personal Data, the extent of which is determined and controlled by data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

- Prospects, customers, business partners and vendors of data exporter.
- Employees or contact persons of data exporter’s prospects, exporter’s customers, exporter’s business partners and exporter’s vendors.
- Employees, agents, advisors, freelancers of data exporter.
- Data exporter’s affiliates authorized by data exporter to use the Service.

Categories of data

The personal data transferred concern the following categories of data:

Data exporter may submit Personal Data to the Service, the extent of which is determined and controlled by data exporter in its sole discretion, and which may include but is not limited to the following categories of Personal Data:

- First and Last Name;
- Contact Information including email address, phone number, social media profiles;
- Professional life data including employer, designation;
- Personal life data including salutation, marital status, family details etc.;
- Locational data;
- Data available on social media (e.g., Facebook, Twitter, etc.) profiles, status and information;
- Event and survey registration, attendance, and response data;
- Engagement data, namely, articles, posts, and the like that is “followed”, “liked” or “disliked”;
- Internet cookies;
- Communication data like emails, chat, voicemail etc. Also, includes feedback and support related communication data; and
- Comments and posts submitted to websites, mobile apps, and online communities

Special categories of data (if appropriate)

The Customer may submit special categories of data on the platform operated by Hevo. However, Hevo does not have access to this, as it is always in encrypted form.

Processing operations

The personal data transferred will be subject to the following basic processing activities:

Data importer will process personal data as necessary to provide the Service pursuant to the Principal Agreement, and as further instructed by data exporter in its use of the Service. This includes automated extraction of data from data exporter's data sources, transformation of data as per data exporter's requirement, and loading data into data exporter's destination database/data warehouse.

DATA EXPORTER

[Populated with details of, and deemed to be signed on behalf of, the data exporter:]

Name:.....

Signed by:

Position:

Authorised Signature

Date:

DATA IMPORTER

Name: Hevo Data, Inc.

Signed by:

Position:

Authorised Signature

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

Information Security Program

1) Data Center and Network Security

Data importer hosts its Service with third-party cloud services and data-centers. Data importer relies on terms of service, contractual agreements, privacy policies, and compliance programs pertaining to these third parties in order to protect data processed by the Service.

More details on this are available here: <https://docs.hevodata.com/platform/security/infrastructure-security/>

The physical and environmental security controls for data importer are audited for SOC 2 Type II compliance.

2) Access and Site Controls

i) Preventing Unauthorized Product Access

Authentication: Customers or customer affiliates who interact with the Service via the user interface must authenticate to proceed.

Authorization: Customer Data can be accessed by any individual authorized by the Customer and having the required authentication details.

ii) Limitations of Privilege & Authorization Requirements

A limited number of Hevo's employees have access to the Service and to a subset of customer data via controlled interfaces. The intent of providing this access is to provide effective customer support, troubleshoot potential problems, detect and respond to security incidents, and implement data security.

3) Data

The data is encrypted in transit through the Service. The encryption uses industry-standard algorithms and certificates. Hevo does not store this data with itself permanently. It is deleted within a maximum of 30 days from the date of processing.

More details on this are available here:
<https://docs.hevodata.com/platform/security/customer-data-retention-and-encryption/>

4) Sub-processor Security

Hevo shall execute a written agreement with all authorized sub-processors to ensure the security of data and compliance with applicable data security laws.

Security Certifications and Reports

Hevo is:

- SOC II certified
- HIPAA certified

ANNEX 3: LIST OF SUB-PROCESSORS

Sub-Processor list as on Execution Date of this Addendum:

Entity Name	Purpose	Corporate Location
Amazon Web Services Inc.	Product hosting	Seattle, Washington
Zendesk Inc.	Support Tickets	SF, California
Intercom Inc.	Support Tickets	SF, California