**Hevo Data**

**Data Processing Addendum**

This Data Processing Addendum ("**Addendum**") forms part of the principal agreement or the Terms of Service, as applicable ("**Principal Agreement**"), by and between the Customer and Hevo pursuant to which Hevo (or any Hevo Affiliate) provides Services to the Customer.

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 The terms Customer, Effective Date, Hevo, Hevo Affiliate, Services and any other undefined term shall have the meanings attributed to them under the Principal Agreement.

1.2 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 the data protection or privacy laws applicable to the Customer Personal Data;

1.1.5 "**EU Data Protection Laws**" means the GDPR and as amended, replaced or superseded from time to time, laws implementing or supplementing the GDPR including as transposed into domestic legislation of each Member State;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 I pursuant to the European Commission's decision (EU) 2021/914 of June 04, 2021 on Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. ; 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.

1.3 Capitalized terms not otherwise defined in this Addendum shall have the meanings given to them in the Principal Agreement.

## 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 With respect to the processing of the Customer Personal Data, either (a) the Customer is the Controller and Hevo and/or Hevo Affiliate are the Processor of Customer Personal Data or (b), the Customer is the Processor and Hevo and/or Hevo Affiliates are the Sub-Processor of the Customer Personal Data (if the Customer is instructing Hevo on behalf of a third-party Controller of the Customer Personal Data). co

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 If the California Consumer Privacy Act (CCPA) applies, then the Parties acknowledge and agree that Hevo and/or Hevo Affiliates is a 'service provider' for the purposes of processing the Customer's Personal Data. In such cases, Hevo and/or Hevo Affiliates (a) will not 'sell' (as defined in the CCPA) any Customer Personal Data; and (b) will not collect, retain, share disclose, or use any Customer Personal Data, except as necessary to perform services for Customer, or as otherwise permitted by CCPA. Hevo and/or Hevo Affiliates acknowledges that it understands and will comply with the restrictions set forth in this Section 3.6. Further, the processing of Customer Identification Data will be in accordance with Hevo's Privacy Policy, which is

available at https://www.hevodata.com/privacy/customers.

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 (or the third-party controller of Customer Personal Data) 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.

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 applicable Data Protection Law.

**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 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 III

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 appointmentHevo 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 applicable 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 13.1 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. For the avoidance of doubt, the Standard Contractual Clauses shall not apply in case of transfers other than Restricted Transfers.

13.4 If the Customer is the Controller of the Customer Personal Data, then Part A (Transfer from Controller to Processor) of Annex I will govern the transfer of data to Hevo. If the Customer is the Processor of the Customer Personal Data, then Part B (Transfer from Processor to Processor) of Annex I will govern the transfer of data to Hevo.

## 14. General Terms

*Governing law and jurisdiction*

14.1 Without prejudice to clauses 17 (Governing Law) and 18 (Choice of forum and jurisdiction) 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.

## ANNEX I: STANDARD CONTRACTUAL CLAUSES

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 the requirements of 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, 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 Standard Contractual Clauses ('Clauses').

### PART A: TRANSFER FROM CONTROLLER TO PROCESSOR

### SECTION I

*Clause 1*
**Purpose and scope**

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (GDPR) for the transfer of personal data to a third country.

(b) The Parties:
   (i) the Customer who is transferring the personal data ('data exporter'), and

   (ii) Hevo as the entity in a third country receiving the personal data from the data exporter (hereinafter 'data importer')

   have agreed to these Clauses.

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex II.

*Clause 2*
**Effect and invariability of the Clauses**

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

*Clause 3*
**Third-party beneficiaries**

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e); and

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

*Clause 4*
**Interpretation**

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

*Clause 5*
**Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

*Clause 6*
**Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex II.

*Clause 7*
**Docking clause**

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by providing the details as required under Annex II and executing the agreement as required by the Parties.

(b) Once it has completed executing the agreement as required by the Parties, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer, as the case may be.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

## SECTION II – OBLIGATIONS OF THE PARTIES

*Clause 8*
**Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

### 8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

### 8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex II, unless on further instructions from the data exporter.

### 8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

### 8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

### 8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex II. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

### 8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information

shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

### 8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex II.

### 8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

### 8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data

exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

(f) The Parties agree that the data exporter or the independent auditor appointed by the data exporter will undertake such an audit or inspection in accordance with clause 12 of the Addendum.

*Clause 9*
**Use of sub-processors**

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 10 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

*Clause 10*
**Data subject rights**

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

*Clause 11*
**Redress**

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

    (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

    (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

*Clause 12*
**Liability**

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

*Clause 13*
**Supervision**

(a) Where the data exporter is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex II, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex II shall act as competent supervisory authority.]

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation

to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex II shall act as competent supervisory authority.]

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

## SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

*Clause 14*

**Local laws and practices affecting compliance with the Clauses**

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

*Clause 15*

**Obligations of the data importer in case of access by public authorities**

**15.1 Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

**15.2 Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## SECTION IV – FINAL PROVISIONS

*Clause 16*
**Non-compliance with the Clauses and termination**

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored

within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

*Clause 17*
**Governing law**

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

*Clause 18*
**Choice of forum and jurisdiction**

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

## PART B: TRANSFER FROM PROCESSOR TO PROCESSOR

## SECTION I

*Clause 1*

**Purpose and scope**

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (GDPR) for the transfer of personal data to a third country.

(b) The Parties:

(iii) the Customer who is transferring the personal data ('data exporter'), and

(iv) Hevo as the entity in a third country receiving the personal data from the data exporter (hereinafter 'data importer')

have agreed to these Clauses.

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex II.

*Clause 2*

**Effect and invariability of the Clauses**

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

*Clause 3*

***Third-party beneficiaries***

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b);

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

*Clause 4*

***Interpretation***

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

*Clause 5*

***Hierarchy***

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

*Clause 6*

**Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex II.

*Clause 7*

**Docking clause**

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by providing the details as required under Annex II and executing the agreement as required by the Parties.

(b) Once it has completed executing the agreement as required by the Parties, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer, as the case may be.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

## SECTION II – OBLIGATIONS OF THE PARTIES

*Clause 8*

***Data protection safeguards***

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

**8.1 Instructions**

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

**8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex II, unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

**8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

**8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

**8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex II. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data

processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

### 8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

### 8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex II.

### 8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

### 8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent

auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

*Clause 9*

***Use of sub-processors***

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub- processors at least 10 days, in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

*Clause 10*

***Data subject rights***

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical

and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

*Clause 11*

***Redress***

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

*Clause 12*

***Liability***

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and

the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

*Clause 13*

***Supervision***

(a) Where the data exporter is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex II, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.]

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with

written confirmation that the necessary actions have been taken.

## SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

*Clause 14*

***Local laws and practices affecting compliance with the Clauses***

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a

disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

*Clause 15*

***Obligations of the data importer in case of access by public authorities***

**15.1 Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer. The data exporter shall forward the notification to the controller.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for

the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

### 15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the controller.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## SECTION IV – FINAL PROVISIONS

*Clause 16*

***Non-compliance with the Clauses and termination***

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority and the controller of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

*Clause 17*

***Governing law***

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

*Clause 18*

***Choice of forum and jurisdiction***

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(f) The Parties agree that those shall be the courts of Ireland.

(g) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(h) The Parties agree to submit themselves to the jurisdiction of such courts.

## ANNEX II : DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

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

(A) *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.

(B) *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.

(C) *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
- App credentials to access third party applications

(D) *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

(E) *Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

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.

(F) *The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).*

The personal data will be transferred to Hevo on a continuous basis in the course of using the Services.

(G) *Nature of the processing*

Hevo 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.

(H) *Purpose(s) of the data transfer and further processing*

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

(I) *The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

Hevo will retain the personal data received under the DPA as long as needed to provide the Services. Hevo may further, retain the personal data, as necessary, only to comply with its legal obligations – to maintain accurate accounting, financial, and other operational records, resolve disputes, and enforce agreements. Hevo has established internal policies for the deletion of personal data following termination of a subscription to the Service.

(J) *For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*

Please refer to Annex III for the details on the sub-processors and the purpose of the processing activity The duration of the processing would be as long as the features enabled by such sub- processors are availed, while utilizing the Services.

(K) *The obligations and rights of Customer*

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

(L) *Technical and Organisational Measures Including Technical And Organisational Measures To Ensure The Security Of The Data:*

**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:**

a. *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.

b. *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.

5) **Security Certifications and Reports:**

Hevo is:

- SOC 2 Type 2 certified
- Audited for compliance with HIPAA

**(M)** *Competent Supervisory Authority:*

The competent supervisory authority in accordance with Clause 13 is Data Protection Commission, Ireland.

## ANNEX III

| Sub-Processor | Purpose | Location | Nature of Customer Data Processed |
|---|---|---|---|
| Hevo Technologies India Private Limited | Business, technical, and support operations | India | Customer Personal Data, Customer Identification Data |
| Amazon Web Services, Inc. (AWS) | Cloud infrastructure and compute services | Multi-region (as per Customer requirements) | Customer Personal Data, Customer Identification Data |
| Google Cloud Platform (GCP) | Cloud infrastructure and compute services | N. Virginia, United States | Customer Personal Data, Customer Identification Data |
| Coralogix | Application logging, observability, and session replay | Ireland, Europe | User session replay data, application logs, Customer Personal Data, Customer Identification Data, click events |
| Microsoft Clarity | User session replay, analytics, and heatmaps | Washington, United States | User session replay data, application logs, Customer Personal Data, Customer Identification Data, click events |

## ANNEX IV

UK Addendum to the EU Standard Contractual Clauses

Background

This Annex is appended to the EU Standard Contractual Clauses ("EU SCC"), located at Annex I.

Except as defined herein, terms used in this Annex have the meaning given to them in the EU SCC

In the event of a Restricted Transfer, the parties enter into this Addendum as issued by the ICO and as amended from time to time to the extent necessary to provide Appropriate Safeguards for Restricted Transfers in accordance with Article 46 of the UK GDPR.

**Part 1: Tables:**

| | |
|---|---|
| **Table 1:** | |
| Details of the Parties | The details of the exporter and the importer are specified in the DPA. |
| **Table 2:** | |
| Selected SCCs, Modules and Selected Clauses | The version of the Approved EU SCCs shall be the version of the EU SCCs included in Annex I of this document. |
| **Table 3:** | |
| Annex IA: List of Parties. | See the details of the data exporter and data importer provided in the DPA and the EU SCC. |
| Annex IB: Description of Transfer | The description of the transfer is mentioned in Annex II of this document. |
| Annex II: Technical and Organisational Measures | The technical and organizational measures of the data importer are mentioned in Annex II of this document. |
| Annex III: List of Sub-processors | The list of sub-processors is mentioned at Annex III of this document. |
| **Table 4:** | |
| Ending this addendum when the approved addendum changes: | Neither Party shall have the right to end this Addendum pursuant to Section 19. |

**Part 2: Mandatory Clauses:**

| | |
|---|---|
| Mandatory Clauses | Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the<br>Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses. |