

## DATA PROCESSING AGREEMENT

This Data Processing Agreement is entered by and between you or the entity you represent (hereinafter to be referred to as the “**Data Controller**”) and Dataimporter Limited, having its business correspondence office at 12 Puriri Street Takapuna, Auckland, New Zealand 0622 (hereinafter to be referred to as the “**Data Processor**”). The Data Controller and the Data Processor are sometimes referred to herein individually as a “**Party”** and collectively as the “**Parties**.”

**Data Protection Terms and Definitions**

*Definitions*

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

'**the data exporter**' means the controller who transfers the personal data;

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

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

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

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

**‘Standard Contractual Clauses’** shall mean the standard contractual clauses, as approved by the European Commission in Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, in the form attached at the Annex to this Addendum

*Terms*

**1. Relationship of the parties**

Customer (the controller) appoints Dataimporter as a processor, or service provider, to process the personal data that is the subject of the Agreement and as more particularly described in Schedule A (the "Data"). Each party shall comply with the obligations that apply to it under Applicable Data Protection Law.

**2. Lawfulness of the Data**

Customer hereby represents and warrants that Customer complies with the requirements of the Applicable Data Protection Law in collecting and transferring the Data to Dataimporter and permitting Dataimporter to act as a processor of the Data, including any additional requirements applicable to specific categories of information, such as national identifiers, special categories of personal data, or sensitive personal data. In particular, Customer shall make all disclosures and obtain all consents necessary to allow: (i) Customer to disclose, provide or make available the Data to Dataimporter in compliance with Applicable Data Protection Law; and (ii) Dataimporter to process, store, retain, use, disclose, and otherwise deal with the Data in accordance with the Agreement (including this Addendum) and with the Applicable Data Protection Law.

**3. Purpose and Confidentiality**

Dataimporter shall treat the Data as Confidential Information, as defined in the Agreement. Dataimporter shall process, store, retain, use, or disclose the Data as a processor, or service provider, in accordance with the use and confidentiality obligations set out in the Agreement, and in accordance with documented instructions from Customer, as more particularly described in Schedule A (the "Permitted Purpose”). Where otherwise required by the Applicable Data Protection Law, Dataimporter shall notify Customer prior to such processing unless Dataimporter is prohibited by law from doing so. Dataimporter shall inform Customer if in its opinion an instruction of Customer infringes Applicable Data Protection Law. Dataimporter shall not sell the Data, nor process, store, retain, use, or disclose the Data (i) for any purposes other than the Permitted Purpose, or (ii) outside of the direct business relationship between Dataimporter and Customer. Dataimporter certifies that it understands these restrictions and will comply with them.

**4. Security**

* 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, without prejudice to any other security standards agreed upon by the Parties, the Data Controller and the Data Processor shall implement appropriate technical and organizational measures to ensure a level of security of the Processing of Personal Data appropriate to the risk. These measures shall include as appropriate:

		1. measures to ensure that the Personal Data can be accessed only by authorized personnel for the purposes set forth in Schedule A of this Data Processing Agreement;
		2. in assessing the appropriate level of security, the Data Controller and the Data Processor shall take into account all reasonable risks presented by the Processing of the Personal Data, for example from accidental or unlawful destruction, loss, or alteration, unauthorized or unlawful storage, Processing, access or disclosure of Personal Data;
		3. the pseudonymization and encryption of Personal Data;
		4. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
		5. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident
		6. a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing of Personal Data;
		7. measures to identify vulnerabilities with regard to the Processing of Personal Data in systems used to provide Services to the Data Controller;
	2. The Data Processor shall at all times have in place an appropriate written security policy with respect to the Processing of Personal Data, outlining the measures set forth in Article 4.1.
	3. At the written request of the Data Controller (no more than once per calendar year), the Data Processor shall demonstrate the measures it has taken pursuant to this Article 4, and, if requested by the Data Controller (no more than once per calendar year), shall cooperate with the Data Controller (or its third-party designee) to audit such measures. Any such request shall be given by the Data Controller to the Data Processor with at least 60 days’ prior written notice to the Data Processor. If the Data Controller elects to use a third-party designee to carry out the audit, such third-party must first enter into a confidentiality agreement with the Data Processor. Any such audit shall be limited solely to the scope of the Data Processor´s operations as they relate to the Processing of Personal Data provided to the Data Processor pursuant to the Service Agreement. The Data Processor shall reasonably cooperate with such audits carried out by or on behalf of the Data Controller and shall provide written responses (on a confidential basis) to all reasonable requests for information made by the Data Controller related to its Processing of Personal Data, including responses to information security and audit questionnaires. The Data Processor shall provide the Data Controller and/or the Data Controller´s auditors with reasonable access to any information relating to the Processing of the Personal Data as may be reasonably required by the Data Controller to ascertain the Data Processor´s compliance with this Data Processing Agreement.

**5. Improvements to Security**

1. The Parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures. The Data Processor will therefore evaluate the measures as implemented in accordance with Article 4 on an on-going basis and will supplement and improve these measures in order to maintain compliance with the requirements set out in Article 4. The Parties will negotiate in good faith any additional cost, if any, to implement material changes required by specific updated security requirements required by applicable data protection law or by data protection authorities of competent jurisdiction.
2. Where a change in EU Data Protection Law requires an improvement in security measures and an amendment to the Service Agreement is necessary in order to execute such improvement (including instances where the Data Controller instructs the Data Processor to make such improvement), the Parties shall negotiate an amendment to the Service Agreement in good faith.

**6.** **Information Obligations and Incident Management**

When the Data Processor becomes aware of an Incident that impacts the Processing of the Personal Data that was provided under the Services Agreement, it shall promptly notify the Data Controller about the Incident within 48 hours of its becoming aware of the Incident. The Data Processor shall reasonably cooperate with the Data Controller and shall follow the Data Controller’s reasonable instructions with regard to such Incidents that solely affect Personal Data that was provided to the Data Processor under the Services Agreement in order to enable the Data Controller to perform a thorough investigation into the Incident, to formulate a correct response, and to take suitable further steps in respect of the Incident.

The term “**Incident**” means:

any unauthorised or accidental access, Processing, deletion, loss or any form of unlawful Processing of the Personal Data;

or any breach of the security and/or confidentiality obligations set forth in Articles 3 and 4 of this Data Processing Agreement resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the Personal Data, or any indication of such breach having taken place or being about to take place.

Any notifications made to the Data Controller pursuant to this Article 7 shall be addressed to the contact provided by the Data Controller as set forth in Appendix 1, attached hereto and incorporated herein by this reference, and shall contain:

a description of the nature of the Incident, including where possible the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

the name and contact details of the Data Processor’s data protection officer or other appropriate contact;
a description of the likely consequences of the Incident as can be reasonably determined at the time of the notification; and
a description of the measures taken or proposed to be taken by the Data Processor to address the Incident including, where appropriate, measures to mitigate its possible adverse effects.

**7. Contracting with Subprocessors**

1. The Data Controller hereby authorises the Data Processor to engage subcontractors to perform the Processing activities set forth in Clause 9. The Data Processor shall inform the Data Controller of any addition or replacement of such Subprocessor. A list of Subprocessors is available in Annex III.
2. Notwithstanding the Data Controller’s authorization as provided in the preceding paragraph, the Data Processor shall remain liable for any Subprocessor that breaches its obligations under this Data Processing Agreement.
3. The Data Processor shall ensure that the Subprocessor is bound by the same data protection obligations as the Data Processor under this Data Processing Agreement, including but not limited to the obligation to implement appropriate technical and organisational measures in such a manner that the Processing will meet the requirements of the EU Data Protection Law.
4. The Data Controller may request that the Data Processor audit its Subprocessor or provide confirmation that such an audit has occurred (or, where available, obtain or assist customer in obtaining a third-party audit report concerning the Subprocessor’s operations) to ensure compliance with its obligations imposed by the Data Processor in conformity with this Data Processing Agreement.
5. Objection Right for new Sub-processors. The Data Controller may object to Dataimporter’s appointment or replacement of a sub-processor prior to its appointment or replacement, provided such objection is in writing and based on reasonable grounds relating to data protection. In such an event, the parties agree to discuss commercially reasonable alternative solutions in good faith. If the parties cannot reach a resolution within ninety (90) days from the date of Dataimporter’s receipt of Customer’s written objection, Customer may discontinue the use of the affected Services by providing written notice to Dataimporter. Such discontinuation will be without prejudice to any fees incurred by Customer prior to the discontinuation of the affected Services. If no objection has been raised prior to Dataimporter replacing or appointing a new sub-processor, Dataimporter will deem Customer to have authorized the new sub-processor.

**8. Returning or Destruction of Personal Data**

Upon (i) termination of this Data Processing Agreement, or (ii) the Data Controller’s written request, the Data Processor shall, at the election of the Data Controller, delete, destroy or return all Personal Data, including any copies.

**9. Assistance to Data Controller**

1. The Data Processor shall reasonably assist the Data Controller, using appropriate technical and organizational means, to promptly respond to requests from Data Subjects exercising their rights under the GDPR.
2. The Data Processor shall, taking into account the nature of Processing and the information available to the Data Processor, reasonably assist the Data Controller to allow the Data Controller to comply with its obligations under the GDPR, including but not limited to ensuring compliance with the obligations pursuant to Article 4 (Security) and engaging in prior consultation with relevant government or regulatory bodies, such as supervisory authorities, required under Article 36 of the GDPR.

**10. Duration and Termination**

1. This Data Processing Agreement is effective as of the Effective Date and shall terminate upon the expiration or termination of the Service Agreement. If the Services no longer involve the Processing of Personal Data that is subject to EU Data Protection Law, this Data Processing Agreement may be terminated earlier upon mutual written agreement of the Parties.
2. Upon termination or expiration of this Data Processing Agreement, the Data Processor shall return or destroy any Personal Data provided to it by the Data Controller. Termination or expiration of this Data Processing Agreement shall not affect accrued rights or obligations of the Parties. Article 3, 9, 11, and 12 shall survive termination or expiration of this Data Processing Agreement.

**11. Miscellaneous**

1. In the event of any inconsistency between the provisions of this Data Processing Agreement and the provisions of the Service Agreement, the provisions of this Data Processing Agreement shall prevail.
2. Any disputes arising from or in connection with this Data Processing Agreement shall be governed in accordance with the laws of the State of Delaware regardless of any choice of law principles, and the Parties consent to jurisdiction and venue in New Castle County, Delaware.
3. No amendment to, or waiver of right under, this Data Processing Agreement is effective unless in writing signed by authorized representatives of the Parties. Any waiver or failure to enforce any provision of this Agreement on one occasion will not be deemed a waiver of any other provision or of such provision on any other occasion. If any provision of this Data Processing Agreement is judicially or administratively determined to be unenforceable, the provision will be reformed to most nearly approximate the Parties’ original intent, but otherwise this Agreement will continue in full force and effect.
4. This Data Processing Agreement may not be assigned in accordance with the terms of the Service Agreement.

*(Signature Page Follows)*

Signed



for and on behalf of the Data Processor

Name: Samuel Hoult

Title: Founder

Date: Apr 5, 2022

Signed

for and on behalf of the Data Controller

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

###

###

###

**SCHEDULE A**

**Description of the Processing**

This Schedule A forms part of the Agreement and the Addendum and describes the processing that Dataimporter will perform on behalf of Customer.

| Subject matter and duration of the processing | The subject matter and duration of the processing are defined in the Agreement. |
| --- | --- |
| Nature and purpose of the processing | The processing is for the purpose of Dataimporter delivering the services under the Agreement. |
| Categories of personal data processed | The personal data processed by Dataimporter is the data that the Customer requires Dataimporter to process under the Agreement. It includes the following data, to the extent that it is personal data: identifying data, commercial data, economic or financial data, and data related to transactions on good and services.  |
| Categories of data subject to which the data relates | The categories of data subject whose data will be processed by Dataimporter under the Agreement include: Customer’s customers, Customer’s prospective customers, Customer’s suppliers, and Customer’s business contacts. |

### **ANNEX**

**STANDARD CONTRACTUAL CLAUSES**

### **SECTION I**

#### ***Clause 1***

#### **Purpose and scope**

1. 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 (General Data Protection Regulation)1 for the transfer of personal data to a third country.
2. The Parties:
	1. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
	2. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)
3. have agreed to these standard contractual clauses (hereinafter: “Clauses”).
4. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
5. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

####

####

####

#### ***Clause 2***

#### **Effect and invariability of the Clauses**

1. 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, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
2. 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**

1. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
	1. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
	2. Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
	3. Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
	4. Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
	5. Clause 13;
	6. Clause 15.1(c), (d) and (e);
	7. Clause 16(e);
	8. Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.
2. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

#### ***Clause 4***

#### **Interpretation**

1. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
2. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
3. 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 I.B.

#### ***Clause 7 - Optional***

#### **Docking clause**

(*omitted*)

### **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**

1. 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.
2. 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 I.B, 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 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. 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 I.B. 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**

1. 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.
2. 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.
3. 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.
4. 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 I.B.

**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 Union4 (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:

1. the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
2. 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;
3. 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
4. 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**

1. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
2. 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.
3. 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.
4. 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.
5. 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**

1. OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub- contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter’s prior specific written authorisation. The data importer shall submit the request for specific authorisation at least 30 days prior to the engagement of the sub- processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.
2. 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.8 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.
3. 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.
4. 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.
5. 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**

1. 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.
2. 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.
3. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

#### ***Clause 11***

#### **Redress**

1. 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.
2. 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.
3. 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:
	1. 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;
	2. refer the dispute to the competent courts within the meaning of Clause 18.
4. 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.
5. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
6. 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**

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

#### ***Clause 13***

#### **Supervision**

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**

1. 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.
2. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
	1. 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;
	2. 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 safeguards12;
	3. 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.
3. 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.
4. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
5. 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).
6. 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**

1. 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:
	1. 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
	2. 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.
2. 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.
3. 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.).
4. 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.
5. 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**

1. 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).
2. 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.
3. 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**

1. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
2. 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).
3. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
	1. 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;
	2. the data importer is in substantial or persistent breach of these Clauses; or
	3. 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.

1. [For Modules One, Two and Three: 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.
2. 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 one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

[OPTION 2 INTENTIONALLY OMITTED]

#### ***Clause 18***

#### **Choice of forum and jurisdiction**

1. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
2. The Parties agree that those shall be the courts of Germany.
3. 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.
4. The Parties agree to submit themselves to the jurisdiction of such courts.

Signed



for and on behalf of the Data Processor

Name: Samuel Hoult

Title: Founder

Date: Apr 5, 2022

Signed

for and on behalf of the Data Controller

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### **ANNEX I to the Standard Contractual Clauses**

**A. LIST OF PARTIES**

MODULE TWO: Transfer controller to processor

**Data exporter(s):** [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: …
Address: …
Contact person’s name, position and contact details: …
Activities relevant to the data transferred under these Clauses: …
Signature and date: …
Role (controller/processor): …
2. …

**Data importer(s):** [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: Dataimporter Limited

Address: 12 Puriri Street, Takapuna, New Zealand, 0622

Contact person’s name, position and contact details:

Samuel Hoult, sam@dataimporter.io

Activities relevant to the data transferred under these Clauses:

Dataimporter provides an open-source data integration platform that provides software and services for data integration, data management, data quality, and data integration for Salesforce customers.

Signature and date: …

Role: Processor

**B. DESCRIPTION OF TRANSFER**

MODULE TWO: Transfer controller to processor

*Categories of data subjects whose personal data is transferred*

The extent of which Personal Data is provided to Dataimporter is determined by the Dataimporter Customer. Personal Data categories disclosed to Dataimporter by Dataimporter Customers may include (i) data regarding potential customers, customers, partners and other vendors of Customer, (ii) Customer personnel, agents, advisors, and freelancers, or (iii) Customer's personnel, agents, advisors, and freelancers.

*Categories of personal data transferred*

Dataimporter Services provide data integration tools to Dataimporter customers; therefore, the categories of Personal Data Dataimporter Customers provide Dataimporter include non-sensitive and sensitive data from all industries. To the extent Dataimporter operates as a Processor on behalf of Dataimporter Customers, Dataimporter Customers may submit Personal Data to the Services, or provide Personal Data to Vendor, which may include, but is not limited to the following categories of Personal Data:

* First and last name
* Employment information
* Contact information (company, email, phone, physical business address) Identification information (drivers ID, passport, other government issued ID) Professional life information
* Personal life information
* Connection information including internet or electronic network activity
* Location information
* Commercial information
* Device information
* Audio/visual information

*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.*

None.

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

Continuous basis depending on the use of the Services by Customer.

*Nature of the processing*

The nature of the Processing of Personal Data by Dataimporter is for the performance of the Services pursuant to the Agreement.

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

The purposes of the data transfer and further Processing by Dataimporter is the performance of the Services pursuant to the Agreement.

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

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Subject to the Deletion of Data section of the Addendum, Dataimporter will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

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

Subprocessor will Process Personal Data as necessary to perform the Services pursuant to the Agreement. Subprocessor will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

**C. COMPETENT SUPERVISORY AUTHORITY**

MODULE TWO: Transfer controller to processor

European Data Protection Supervisor, shall act as competent supervisory authority insofar as the relevant data transfer is governed by Regulation (EU) 2016/679.

The UK Information Commissioner's Office shall act as competent supervisory authority insofar as the relevant data transfer is governed by UK Data Protection Laws and Regulations.

The Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations.

### **ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

Dataimporter Limited will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services, as described in the Dataimporter Limited Security Policy documentation applicable to the Services, and accessible via <https://dataimporter.io/privacy-policy> or otherwise made reasonably available by Dataimporter Limited.

**a) Access Control**

i) Preventing Unauthorized Product Access Outsourced processing: Dataimporter.io hosts its Service with outsourced cloud infrastructure providers. Additionally, Dataimporter.io maintains contractual relationships with vendors in order to provide the Service in accordance with our Data Processing Agreement. Dataimporter.io relies on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

Physical and environmental security: Dataimporter.io hosts its product infrastructure with multitenant, outsourced infrastructure providers. The physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.

Authentication: Dataimporter.io implemented a uniform password policy for its customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data.

Authorization: Customer data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of Dataimporter.io’s products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user’s permissions against the attributes associated with each data set.

ii) Preventing Unauthorized Product Use Dataimporter.io implements industry standard access controls and detection capabilities for the internal networks that support its products. Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

Intrusion detection and prevention: Dataimporter.io implemented a Web Application Firewall (WAF) solution to protect hosted customer websites and other internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services.

Static code analysis: Security reviews of code stored in Dataimporter.io’s source code repositories is performed, checking for coding best practices and identifiable software flaws.

Penetration testing: Dataimporter.io maintains relationships with industry recognized penetration testing service providers for four annual penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

iii) Limitations of Privilege & Authorization Requirements Product access: The founder of Dataimporter.io has access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through “just in time” requests for access; all such requests are logged. Employees are granted access by role, and reviews of high risk privilege grants are initiated daily. Employee roles are reviewed at least once every six months.

Background checks: All Dataimporter.io employees undergo a third-party background check prior to being extended an employment offer, in accordance with the applicable laws. All employees are required to conduct themselves in a manner consistent with company guidelines, nondisclosure requirements, and ethical standards.

**b) Transmission Control In-transit**

Dataimporter.io makes HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces and for free on every customer site hosted on the Dataimporter.io products. Dataimporter.io’s HTTPS implementation uses industry standard algorithms and certificates. At-rest: Dataimporter.io stores user passwords following policies that follow industry standard practices for security. Dataimporter.io has implemented technologies to ensure that stored data is encrypted at rest.

**c) Input Control** **Detection**

Dataimporter.io designed its infrastructure to log extensive information about the system behaviour, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. Dataimporter.io personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: Dataimporter.io maintains a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, Dataimporter.io will take appropriate steps to minimise product and Customer damage or unauthorised disclosure.

Communication: If Dataimporter.io becomes aware of unlawful access to Customer data stored within its products, Dataimporter.io will:

1) notify the affected Customers of the incident.

2) provide a description of the steps Dataimporter.io is taking to resolve the incident; and

3) provide status updates to the Customer contact, as Dataimporter.io deems necessary. Notification(s) of incidents, if any, will be delivered to one or more of the Customer’s contacts in a form Dataimporter.io selects, which may include via email or telephone.

**d) Availability Control Infrastructure availability**

The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.95% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

Fault tolerance: Backup and replication strategies are designed to ensure redundancy and failover protections during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple availability zones.

Online replicas and backups: Where feasible, production databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases are backed up and maintained using at least industry standard methods. Dataimporter.io’s products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists Dataimporter.io operations in maintaining and updating the product applications and backend while limiting downtime.

### **ANNEX III – LIST OF SUB-PROCESSORS**

| Third-Party Sub-Processor | Purpose | US Data Center Location | EU Data Center Location |
| --- | --- | --- | --- |
| Linode | Cloud Hosting | Dallas, TX | Frankfurt, DE |
| Sendgrid | Email Deliverability | Las Vegas, NV;Chicago, IL; San Jose, CA; Herndon, VA; Washington D.C., | - |
| Hubspot | LiveChat | United States East (AWS) | Europe West (AWS) |