Data Processing Addendum

This Data Processing Addendum ("**DPA**") is between:

Initus Technologies Inc. ("**Processor**" or "**Initus,**" "us," "our," and "we") and "you" or the entity you represent (our "**Customer**" and the "**Controller**" of Personal Data) and specifies the Parties' obligations with regard to data protection which result from the Personal Data Processing on behalf of the Controller as described in this DPA and its Annexes, which shall form part of the DPA.

This DPA forms an integral part of the main agreement between the parties agreed to by the Controller in connection with the performance of the Services, which includes without limitation the Master Services Agreement, as may be amended from time to time (the "**MSA**"), the Statement of Work (the "**SOW**"), and any Change Order effected pursuant to the SOW (collectively, the "**Principal Agreement**"). By executing the SOW the parties agree that they are also executing this DPA, which forms an integral part of the Principal Agreement.

In connection with the Services, Initus may Process certain Personal Data for which you as the Customer are the Controller ("**Customer Data**" or **Controller Data**"). When you agree to the terms of the Principal Agreement, you also agree to this DPA.

Controller and Processor are hereinafter collectively referred to as the "**Parties**" and individually as the "**Party**."

References in this DPA to specific requirements contained in the GDPR shall only apply to the extent that GDPR applies to such processing activities.

1. DEFINITIONS

1.1 "Affiliate" means, for the sole purpose of this DPA and without prejudice to any applicable use or license restrictions, limitations in service scope or other limitations provided under the Principal Agreement, any consolidated group entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity (and "control", for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity), or any entity otherwise expressly designated as an "Affiliate" in the Principal Agreement.

1.2 "Applicable Data Protection Law" means the PIPEDA, the GDPR, and the CCPA, and any other laws and regulations of the EEA, Canada and its provinces, and the United States of America and its states, insofar as they may be applicable to the Processing of Controller Data under the Principal Agreement.

1.3 "Annexes" has the meaning given to the term in the first Recital of this DPA.

1.4 "Audits" has the meaning given to the term in Section 3.1g) of this DPA.

1.5 "Authorized Third Party" has the meaning given to the term in Section 3.1g) of this DPA.

1.6 "CCPA" means the California Consumer Privacy Act Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.

1.7 "Controller" has the meaning given to this term under the Applicable Data Protection Law and is as described in the first Recital of this DPA. For the purpose hereof "Controller" includes the Customer and as applicable, its Affiliates, end-customers, suppliers, contractors and/or partners in their capacity as Controllers and whose Personal Data at any time is Processed by Initus or its Sub-processors under this DPA (the "Other Controllers").

1.8 “Customer Data” or “Controller Data” has the meaning given to the term in the Principal Agreement or, if not defined, means all data and all content submitted by Customer using the software licensed or made available by Initus or provided by Customer to Initus in the course of Initus providing the Services pursuant to the Principal Agreement.

1.9 “Data Processing Addendum” or “DPA” means this data processing addendum including its Appendices.

1.10 “Data Subject” means the identified or identifiable person to whom Personal Data relates.

1.11 “Data Transfer Agreement” has the meaning given to the term in Section 6.3 of this DPA.

1.12 “EEA” means, for the purposes of this DPA and the Principal Agreement, the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom.

1.13 “EU Personal Data” means the Processing of Personal Data to which Data Protection Law of the EEA was applicable prior to its Processing by Initus.

1.14 “GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

1.15 “MSA” has the meaning given to the term in the second Recital of this DPA.

1.16 “Personal Data” means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under Applicable Data Protection Laws), where for each (i) or (ii), such data is Customer Data.

1.17 “Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

1.18 “Principal Agreement” has the meaning given to the term in the second Recital of this DPA.

1.19 “Processing” means any operation or set of operations which is performed upon Customer Data, including Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

1.20 “Processor” means the entity which processes Personal Data on behalf of the Controller including as applicable any "service provider" as that term is defined by the CCPA, and for the purposes of this DPA the Processor is Initus or an Affiliate of Initus.

1.21 “Services” means any services which Initus provides to the Customer pursuant to the Principal Agreement.

1.22 “SOW” has the meaning given to the term in the second Recital of this DPA.

1.23 “Sub-processor” means any processor engaged by Initus, by an Affiliate of Initus or by another Sub-processor, including Affiliates of Initus acting as Processors.

1.24 “Standard Contractual Clauses” means:

a) for UK Personal Data, the International Data Transfer Addendum to the EU SCCs, issued by the Information Commissioner in accordance with s.119A of the UK Data Protection Act 2018 but, as permitted by clause 17 of such addendum, the Parties agree to change the format of the information set out in the addendum so that (i) the details of the parties in table 1 shall be as set out in Annex 1 of the EU SCCs (with no requirement for further signature); (ii) for the purposes of table 2, the addendum shall be appended to the EU SCCs (including the modules and optional clauses noted below) and clause 6.5(b) below selects the option and timescales for clause 9; and (iii) the appendix information listed in table 3 shall be as set out in the Annexes to the EU SCCs (“UK SCCs”); for the purposes of table 4, the Parties agree that neither Party may terminate the International Data Transfer Addendum;

b) for EU Personal Data, the standard contractual clauses adopted by the European Commission under Commission Implementing Decision (EU) 2021/914 including the text from Module 2 of such clauses, not including any clauses marked as optional, and as further described in Section 6.5 of this DPA (“EU SCCs”); and

c) for Swiss Personal Data, the EU SCCs.

1.25 “Swiss Personal Data” means the processing of Personal Data to which the Swiss Federal Acts on Data Protection were applicable prior to its processing by Initus.

1.26 “Transfer” means and includes disclosure, transmission and/ or any other form of transfer of Controller Data and further has the meaning given to the term in Section 6.2 of this DPA.

1.27 “UK Personal Data” means the processing of Personal Data to which data protection laws of the United Kingdom were applicable prior to its processing by Initus.

2. RIGHTS AND OBLIGATIONS OF THE CONTROLLER

2.1 The Controller (i) shall ensure that the Controller when Processing Controller Data, complies with Applicable Data Protection Law; (ii) is at all times entitled to provide new or amended instructions regarding the Processing of the Controller Data, whereby the Processor shall be given reasonable time for implementation; (iii) shall without undue delay inform the Processor of any circumstances that may require modifications to the Processor’s Processing of the Controller Data; (iv) is at all times entitled to, by written notification to the Processor, terminate the Processor's Processing of the Controller Data if the Controller has reasonable grounds to believe that the Processor is unable, or has failed, to comply with the provisions of the DPA or Applicable Data Protection Law; and (v) provides a general authorisation to the Processor to engage Sub-processors, provided however that the Controller’s authorisation is subject to such Sub-processor‘s compliance with all the provisions set out in this DPA.

2.2 This DPA shall apply to all Processing of the Controller Data performed by the Processor on behalf of the Controller; in no event shall the Parties Process any Personal Data as joint controllers, as such term is defined in the GDPR.

3. OBLIGATIONS OF THE PROCESSOR

3.1 The Processor shall Process the Controller Data only on behalf of the Controller, as specified in this Section and **Annex I**, and solely for the purposes specified by the Controller; however, nothing in the Principal Agreement (including this DPA) shall limit or prevent Processor from collecting or using data that Processor would otherwise

collect and process independently of Controller's use of the Services. The Processor shall:

a) Process the Controller Data only in accordance with (i) this DPA; (ii) the instructions regarding processing of Controller Data provided by the Controller; and (iii) Applicable Data Protection Law. If the Processor, in order to comply with Applicable Data Protection Law, is obliged to deviate from the provisions of this DPA and/or the Controller's instructions, the Processor shall, without undue delay and before further processing of the Controller Data, inform the Controller of such mandatory requirements, unless providing such information violates mandatory law.

b) Implement such technical, physical, administrative and organisational security measures and appropriate to the risk that the Processing of the Controller Data may impose on the rights and freedoms of Data Subjects. In assessing the appropriate security levels, and taking appropriate measures, the Processor shall ensure that account is taken in particular of the risks for accidental or unlawful destruction, loss or alteration and of the risks of unauthorised disclosure of, or unauthorised access to, the Controller Data as well as of the risk of Personal Data Breaches.

c) Ensure that individuals authorised to Process Controller Data have committed to confidentiality or are under an appropriate statutory confidentiality obligation.

d) Ensure that individuals Processing Controller Data have undergone relevant training in relation to the Processing of the Controller Data.

e) Assist the Controller by ensuring that the Controller's obligations under Applicable Data Protection Law and the DPA are complied with, for example, but not limited to regarding the performance of data protection impact assessments or audits performed by competent supervisory authorities.

f) Assist the Controller by implementing appropriate technical and organisational measures to comply with Controller's obligations in relation to Data Subjects' requests to exercise their rights under Applicable Data Protection Law. The Processor shall immediately notify the Controller of such Data Subject requests. Unless explicitly stated in the Controller's instructions, provided for in mandatory law or a decision by a competent supervisory authority, the Processor may not respond to a Data Subject's request.

g) Without undue delay, provide the Controller with access to all information required to demonstrate that the Processor's obligations set out in this DPA have been fulfilled. The Processor shall also enable and contribute to the Controller's reviews of the Processor's processing of the Controller Data, including audits of the Processor's premises, equipment and/or systems ("**Audits**"). The aforementioned shall also apply in relation to third parties authorised by the Controller to perform such reviews and audits on the Controller's behalf ("**Authorized Third Party**"), provided however that such Authorized Third Party (i) has executed a non-disclosure agreement appropriate for the purpose; and (ii) is not conducting operations that compete with the Processor's operations. The Controller is responsible for ensuring that reviews and Audits are carried out without unreasonable disruptions of the Processor's operations, including the activities performed by the Processor's other customers and their reasonable need for protection of their operations. The Controller shall bear all Authorized Third Party costs as well as its own costs for reviews and Audits.

h) Keep a record on the Processing of the Controller Data under this DPA and allow the Controller access to such record at the Controller's request.

i) Ensure that the Controller Data is only Transferred disclosed, transmitted or otherwise made available by the Processor to Sub-processors, if any, who, by agreement with the Processor, are bound by obligations that correspond to and are no less stringent than the Processor's obligations set out in this DPA. A current list of Sub-processors is provided in **Annex III** to this DPA; and (ii) copies of agreements with the Sub-processors (to the extent necessary to evidence that Sub-processors are bound by obligations that correspond to the Processor's obligations set out in this DPA and subject to any confidentiality restrictions in place with such Sub-processors from time to time),

j) When replacing or hiring a new Sub-processor, ensure that the Controller is given the opportunity to object to such change. If the Controller reasonably and fairly objects to the replacement or hiring of a Sub-processor, the Processor shall ensure that the Sub-processor's processing of Controller Data is not initiated, or, where applicable, is terminated without unnecessary delay. The Controller acknowledges that an objection to a specific Sub-processor may result in (i) limitations in the Processor's ability to comply with its obligations under the Principal Agreement; and (ii) that the Processor may be entitled to compensation under

k) Without undue delay, inform the Controller if the Processor believes the Controller's instructions violate Applicable Data Protection Law or that Controller Data is processed or may be processed in violation of Applicable Data Protection Law. The Processor is not entitled to stop the processing of the Controller Data unless the Processor can reasonably demonstrate that continued processing would result in that the Processor would violate the DPA, the Principal Agreement and/or Applicable Data Protection Law.

l) Without undue delay, inform the Controller of a competent supervisory authority's investigation or audit of the Controller Data, unless providing such information violates mandatory law.

m) Without undue delay, notify the Controller of a suspected or confirmed Personal Data Breach related to the Processing of the Controller Data.

n) In the event of termination of this DPA, depending on what the Controller requests, delete or return all the Controller Data, including copies thereof, provided however that the Processor is not prohibited by mandatory law to comply with the Controller's request.

3.2 If a review or an Audit of the Processor requested by the Controller (according to Section 3.1g) relates to a matter that is covered by an audit report made in accordance with SSAE 16/ISAE 3402 Type II, ISO, NIST or similar, the Controller shall accept the results of that report instead of having the requested review or Audit being performed. The aforementioned shall apply only if (i) the audit report has been performed by an independent third party that can reasonably be assumed to possess relevant competencies; (ii) the Processor confirms that the reviewed functions, processes and measures have not changed after the completion of the audit report; (iii) the audit report has been completed no more than 12 months prior to the date on which the Controller has made his request for review or Audit; and (iv) both Parties consider that the procedure is consistent with Applicable Data Protection Law.

4. COMPENSATION

4.1 Unless otherwise agreed in writing between the Parties, the Processor shall not receive any compensation for the fulfilment of its obligations under this DPA, including compliance with the Controller's instructions regarding the processing of the Controller Data, besides to the compensation received pursuant to the Principal Agreement.

4.2 Notwithstanding Section 4.1 above, the Processor is entitled to compensation for actual and proven additional costs incurred by the Processor as a result of:

a) the Processor's assistance with data protection impact assessments initiated by the Controller;

b) the Processor's assistance on a review or an Audit of the Processor and/or its Sub-Processors initiated by the Controller, however no compensation will be paid for assistance on reviews or Audits that are performed in accordance with Section 3.2;

c) that the Controller, after the DPA has entered into force, notifies the Processor of new or changed instructions regarding the Processor's processing of the Controller Data;

d) that the Sub-Processor's processing of the Controller Data has been terminated at the Controller's request in accordance with Section 3.1j); and

e) that the extent of the Processor's assistance with regards to the Controller's compliance with Applicable Data Protection Law substantially exceeds what the Processor could reasonably have foreseen at the time of the execution of the DPA.

5. LIABILITY

Without prejudice to any express right or remedy available to Data Subjects provided under Applicable Data Protection Law, any liability arising out of or in connection with this DPA is, as between the Parties, limited to direct damages (excluding any indirect, consequential, special or incidental cost, loss or damage of any kind) and subject to the applicable provisions on limitation of liability of the Principal Agreement, and such liability limitations shall include Customer's and any other data controller's claims in the aggregate.

6. EEA SPECIFIC TERMS

6.1 If as part of the Services, and as may indicated in the SOW, Initus Processes EU Personal Data, UK Personal Data or Swiss Personal Data, Initus will assist Customer in complying with its obligations as Controller under Articles 32-36 of the GDPR or equivalent provisions in Data Protection Law of EEA countries taking into account the nature of processing and the information available to Initus.

6.2 It is acknowledged that Initus, either itself or using permitted Sub-processors, as part of its regular business, performs Services from locations in countries and territories outside the EEA. Where applicable, this Section 6 sets forth the provisions on how Personal Data Processed under this DPA may be Transferred from a country or territory within the EEA to, or accessed from, a country or territory outside the EEA, either directly or via onward transfer (each a "**Transfer**") by Initus, acting itself and/or through permitted Sub-processors, and Customer (for its own part and on behalf of the Other Controllers, if any) hereby gives its specific written mandate, authorization and instruction to Initus for the purposes of conducting such Transfers when providing the services from locations outside the EEA, as set forth below.

6.3 For the purposes of Transfers of Personal Data under this DPA, Customer and Initus incorporate the relevant Standard Contractual Clauses as if they were set out in full in this DPA (the "**Data Transfer Agreement**") and under which Customer, for its own part and on behalf of each Other Controller, if any, acts as the "data exporter" and Initus, itself and/or through any permitted Sub-processor outside of the EEA, acts as the "data importer" (as those terms are defined in the Standard Contractual Clauses). The Parties' execution of the SOW shall be deemed to be the signature of the Data Transfer Agreement on the same date as the execution of the SOW (with the Customer

signing as the data exporter and Initus signing as the data importer). The terms of the relevant Data Transfer Agreements, if applicable, will prevail over conflicting or inconsistent terms in this DPA to the extent of the conflict or inconsistency.

6.4 Transfers of Personal Data shall only be permitted if:

a) the Transfer is performed under and pursuant to the terms of the Data Transfer Agreement; or

b) the Transfer is to a country which has been found to ensure an adequate level of protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data; or

c) the Transfer is pursuant to a framework which has been determined by the European Commission or other appropriate competent authority as ensuring an adequate level of protection for the rights and freedoms of Data Subjects and subject to the scope restrictions of any such determination, e.g. Binding Corporate Rules; or

d) the Transfer is subject to a separate data transfer agreement with Initus or any Initus Affiliate incorporating the Standard Contractual Clauses applicable at the time of the relevant Transfer; or

e) the Transfer is otherwise covered by a suitable framework recognized by the relevant supervisory authorities or courts as providing an adequate level of protection for Personal Data, including without limitation any Initus Group intra-company arrangement requiring all Transfers of Personal Data to be made in compliance with the Standard Contractual Clauses.

6.5 Without prejudice to Section 6.3 of this DPA, the following provisions will be used to assist in the interpretation of the Standard Contractual Clauses incorporated as part of this DPA:

a) Annexes to the EU SCCs and the UK SCCs are as set out in **Annex I**;

b) for the purposes of the EU SCCs: (i) the Parties choose to include the optional docking clause in Clause 7, (ii) Clause 9 Option 2 shall apply (general written authorisation) and the Parties agree that the time period for submitting notice of changes shall be 10 business days, (iii) the Parties choose not to include the optional language relating to the use an independent dispute resolution body in Clause 11 (iv) Clause 17 Option 1 (governing law) shall apply and shall be governed by the laws of Ireland, (v) Clause 18 (choice of forum and jurisdiction) the courts of Ireland shall have jurisdiction;(vi) the terms contained in Annex IV shall supplement the Standard Contractual Clauses.

c) for the purposes of the UK SCCs, the Parties incorporate and adopt the EU SCCs in exactly the same manner as set forth in this DPA, with the following distinctions: (Clause 13 (Annex 1.C): the competent authority shall be the UK ICO; (ii) for Clause 17, the UK SCCs shall be governed by the laws of England and Wales; (iii) for Clause 18, the Parties agree that any dispute arising from the Standard Contractual Clauses, or the incorporated UK Transfer Addendum shall be resolved by the courts of England and Wales. A Data Subject may also bring legal proceeding against the Data Exporter and/or Data Importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.

d) information and documentation to be provided by the data importer to the data exporter under the Standard Contractual Clauses will be provided only upon Customer's

reasonable request, taking into account the nature of the Processing and the information available to Initus;

e) audits under the Standard Contractual Clauses will be carried out in accordance with Section 3.1g) of this DPA;

f) any certification of deletion of Personal Data that is required under the Standard Contractual Clauses will be provided by the data importer to the data exporter only upon Customer's request;

g) Initus will only accept to Transfer and Process any sensitive data as expressly agreed and set forth in **Annex I** to this DPA; and

h) for the purpose of Clause 9(a) of the EU SCCs and subject to Section 3.1i) of this DPA, Customer (also on behalf of the Other Controllers, if any) hereby gives its general written consent, authorization and mandate to Initus to use Sub-processors for Processing of Personal Data solely for the purposes set forth in this DPA; and

i) for Swiss Personal Data, the Data Transfer Agreement shall be deemed modified such that any reference to the GDPR shall refer to the Swiss Federal Acts on Data Protection 1992 and 2020, and the term 'Member State' shall not be interpreted in a way as to exclude Data Subjects in Switzerland from the possibility of enforcing their rights in their place of habitual residence in accordance with clause 18(c) of the Standard Contractual Clauses.

7. TERM AND TERMINATION

7.1 This DPA shall enter into force upon signature by both Parties and shall remain in force until terminated in accordance with the provisions of this Section 7.

7.2 This DPA will terminate at the later date of (i) the date of termination of the Principal Agreement; and (ii) the date on which the Processor ceases to process the Controller Data.

7.3 Notwithstanding Section 7.2, each Party is entitled to terminate the DPA with immediate effect if the other Party commits a material breach of this DPA or the Principal Agreement, which is not rectified within 30 days of receiving notice of the breach.

8. NOTICES

All notices and other communications herein shall be in writing and shall be deemed to have been given (a) when delivered by hand (with written confirmation of receipt); (b) when received by the addressee if sent by a nationally recognized overnight courier (receipt requested); (c) on the date sent by facsimile or e-mail of a PDF document (with confirmation of transmission) if sent during normal business hours of the recipient, and on the next business day if sent after normal business hours of the recipient or (d) on the third day after the date mailed, by certified or registered mail, return receipt requested, postage prepaid. Such communications must be sent to the respective parties at their registered address or at such other address for a party as shall be specified in a notice given in accordance with this Section 8:

9. FURTHER ASSURANCES

Each of the Parties will from time to time execute and deliver all such further documents and instruments and do all acts and things as the other Party may, either before or after this DPA is entered into, reasonably require to effectively carry out or better evidence or perfect the full intent and meaning of this DPA.

10. CHANGES AND AMENDMENTS

Any changes to or amendments to this DPA shall be in writing and signed by both Parties. No waiver by either Party of any of the provisions hereof shall be effective unless explicitly set forth in writing and signed by the Party so waiving. No waiver by either Party shall operate or be construed as a waiver in respect of any failure, breach or default not expressly identified by such written waiver, whether of a similar or different character, and whether occurring before or after that waiver. No failure to exercise, or delay in exercising, any right, remedy, power or privilege arising from this DPA shall operate or be construed as a waiver thereof; nor shall any single or partial exercise of any right, remedy, power or privilege hereunder preclude any other or further exercise thereof or the exercise of any other right, remedy, power or privilege.

11. SEVERABILITY

If any term or provision of this DPA is invalid, illegal or unenforceable in any jurisdiction, such invalidity, illegality or unenforceability shall not affect any other term or provision of this DPA or the Principal Agreement, or invalidate or render unenforceable such term or provision in any other jurisdiction.

12. GOVERNING LAW

If Customer engages with Initus in Canada, this DPA shall be governed by the law of the province of Ontario and the Canadian federal laws applicable therein, without regard to conflict of law rules.

If Customer engages with Initus in the United States of America or anywhere else in the world, this DPA shall be governed by the law of the state of New York and the United States of America federal laws applicable therein, without regard to conflict of law rules.

13. ENTIRE AGREEMENT

(i) This DPA (including its Annexes) and any agreements entered into by either of the Parties arising from or in relation to the DPA; (ii) the Principal Agreement; and (iii) the Standard Contractual Clauses collectively constitute the sole and entire agreement of the Parties with respect to the subject matter contained herein and therein, and supersede all prior and contemporaneous understandings and agreements, both written and oral, with respect to such subject matter. In the event of any conflict or inconsistency between the statements in the DPA and those in the Principal Agreement (other than an exception expressly set forth in either agreement), the statements in the DPA will prevail to the extent of such conflict or inconsistency, and in the event of any conflict or inconsistency between the statements in the DPA and those in the Standard Contractual Clauses (other than an exception expressly set forth in either agreement), the statements in the Standard Contractual Clauses will prevail to the extent of such conflict or inconsistency.

ANNEX I – PARTIES, SCOPE AND OTHER DETAILS PERTAINING TO THE PROCESSING OF PERSONAL DATA

A. List of Parties

1. Data Exporter(s):

Name: **Customer**

Address: See Principal Agreement

Contact person's name, position, and contact details: See Principal Agreement

Activities relevant to the data transferred under these Clauses:

See Section B below

Role: Controller (on its own behalf and acting on behalf of each Other Controller, if any, being established in the EEA)

2. Data importer(s):

Name: **Initus**

Address: See Principal Agreement

Contact person's name, position, and contact details: See Principal Agreement

Activities relevant to the data transferred under these Clauses:

See Section B below

Role: Processor (for and on behalf of those Initus Affiliates being non-EEA entities, for the purpose of providing the services under the terms of the Principal Agreement)

B. Scope and Manner of Processing of Personal Data

1. Scope and manner of Processing of Personal Data (including potential onward Transfers):

1.1 The Parties hereby agree that the scope and manner of Personal Data Processing may include some or all of the following:

- Entering, viewing, and manipulating Personal Data of Controller

2. Purpose of Processing of Personal Data

2.1 The Parties hereby agree that the purpose of Processing of Personal Data shall be the following:

- Provision of the Services as described in the Principal Agreement

3. Categories of Personal Data and Data Subjects

3.1 The Parties hereby agree that the groups of Data Subjects whose Personal Data may be Transferred and Processed under the Principal Agreement:

- Employees or contact persons of Controller's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Controller (who are natural persons)

3.2 The Parties hereby agree that no special categories of Personal Data will be Transferred or Processed by the data importer.

3.3 The Parties hereby agree that the Personal Data Processed under the Principal Agreement may contain some or all of the following categories of Personal Data:

Name, email, phone #, title, (business contact details) and salary information relating to Controller's employees.

4. Frequency of the Transfer

4.1 The Parties hereby agree that the Personal Data will be regular and repeated for as long as necessary for data importer to perform the Services under the Principal Agreement.

5. Retention of the Personal Data.

5.1 Generally, retention of Personal Data should not be required. The only processing that is anticipated to take place is data access. In case Personal Data should be retained, any retention period will be limited to the duration necessary to perform the services under the Principal Agreement.

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

Initus will maintain physical, administrative and technical safeguards for the protection of the security, confidentiality, and integrity of Personal Data processed, as described below.

The technical and organizational measures will be subject to technical progress, development and improvements for the protection of Personal Data and any such measures shall automatically apply hereto. Initus will not materially decrease the overall security of any services with respect to Processing of Personal Data.

1. Access, input, and transmission controls, including the following:

- Establishing and maintaining staggered access authorisations for employees and third parties;
- Regulating and restricting physical access authorities;
- Reviewing and updating the keys and card keys regularly;
- Identifying and reviewing all persons having access authority;
- Using time recording equipment;
- Recording all visitors.
- Running central data processing equipment (servers) only in specially protected areas to which only selected employees (administrators) and Processors, who are committed to diligence and secrecy, have access;
- Compliance rules for the use of mobile devices
- Logical and physical protection of all data media
- Authorising and enforcing a usage policy for the reading, alteration and deletion of stored data
- Password controls such as using secure passwords; changing the passwords regularly;
- Separation of test and production systems.
- Maintaining policies that regulate the transmission and transport of data;
- Using the data processing equipment only after identifying and authenticating the user;
- Employing data encryption in transit
- Establishing documentation for all programs which encrypt, send or receive data;

2. Data Separation, including the following:

- Logical separation of data of the Processor and/or the Processor's clients and other data;
- Using encryption for safety-critical files and files with Personal Data with different data keys depending on the files' owner;

ANNEX III – LIST OF APPROVED SUB-PROCESSORS

The Controller has authorised the use of the following Sub-processors:

1. Processor and Processor Affiliates:

- Trajectory Global Services Inc. (USA),
- Trajectory Group Inc. (Canada),
- Trajectory Inc. Chile SPA (Chile), and
- Trajectory Inc. Colombia SAS (Colombia)

2. Technology Providers:

- Google LLC, and
- Anthropic, PBC

ANNEX IV – SUPPLEMENTARY CLAUSES (ADDITIONAL SAFEGUARDS) TO THE STANDARD CONTRACTUAL CLAUSES

Initus will implement additional safeguards as and if required to ensure the protection of personal data in accordance with the Standard Contractual Clauses and this DPA.

The contemplated processing of personal data consists of data access in Customer's systems. The safeguards described in Annex II are deemed sufficiently protective of personal data.