MINDWIRE DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms part of, and is subject to, the services agreement or other written or electronic terms of service or subscription agreement between MindWire, Inc. ("**MindWire**") and the legal entity defined as 'Client' thereunder together with all Client Affiliates who are signatories to an Order Form, SOW, or similar written agreement for their own Account (as defined in Section 1 below) pursuant to such agreement (collectively, for purposes of this DPA, "**Client**", and together with MindWire, the "**parties**") (such agreement, the "**Agreement**"). This DPA shall be effective on the effective date of the Agreement, unless this DPA is separately executed in which case it is effective on the date of the last signature ("**DPA Effective Date**"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

1. Definitions.

"**Account**" means Client's account in the Services in which Client stores and processes Client Data.

"**Affiliate**" has the meaning set forth in the Agreement.

"**Authorized Affiliate**" shall mean a Client Affiliate who has not signed an Order Form pursuant to the Agreement, but is either a Data Controller or Data Processor for the Client Personal Data processed by MindWire pursuant to the Agreement, for so long as such entity remains a Client Affiliate.

"**California Consumer Privacy Act**" or "**CCPA**" means the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020, and all implementing regulations, as the foregoing may be amended from time to time.

"CPA" means the Colorado Privacy Act, and its implementing regulations, Col. Rev. Statutes, Part 13, et seq. as the same may be amended from time to time;

"CTDPA" means the Connecticut Data Protection Act, Conn. Gen. Stat. Section 743d, et seq. and its implementing regulations, as the same may be amended from time to time;

"**Client Data**" has the meaning set forth in the Agreement (including any references to "customer data," "customer information," or any similar terms).

"**Client Personal Data**" means any Client Data that is Personal Data.

"**Data Controller**" means an entity that determines the purposes and means of the Processing of Personal Data.

"**Data Processor**" means an entity that Processes Personal Data on behalf of a Data Controller.

"**Data Protection Laws**" means all data protection and privacy laws applicable to the respective party in its role in the Processing of Personal Data under the Agreement, including, where applicable, EU & UK Data Protection Law, the CCPA, CPA, CTDPA, UCPA, and VCDPA.

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

"**EU & UK Data Protection Law**" means (i) Regulation 2016/679 of the European Parliament and of the Council 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) ("**GDPR**"); and (ii) the GDPR as it forms part of United Kingdom law pursuant to Section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**") and the Data Protection Act 2018.

"**Personal Data**" means any information or data relating to an identified or identifiable natural person and includes similarly defined terms in Data Protection Laws, including, but not limited to, the definition of "personal information" in the CCPA.

"**Processing**" shall mean any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination and "Process‟, "Processes" and "Processed" will be interpreted accordingly.

"**Purposes**" shall mean (i) MindWire's provision of the Services as described in the Agreement, including Processing initiated by End Users in their use of the Services; and (ii) further documented, reasonable instructions from Client agreed upon by the parties.

"**Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Client Personal Data.

"**Services**" means the MindWire services provided by MindWire to Client as described under the Agreement, including but not limited to support and technical services.

"**SCCs**" means together (i) "EU SCCs" means the standard contractual clauses for the transfer of personal data to third countries approved pursuant to Commission Decision (EU) 2021/914 of 4 June 2021, currently found at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en and (ii) "UK Addendum" means the International Data Transfer Addendum issued by the Information Commissioner's Office under s.119(A) of the UK Data Protection Act 2018, currently found at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf ("**UK Addendum**").

"**Sub-Processor**" means any other Data Processors engaged by MindWire to Process Client Personal Data.

"UCPA" means the Utah Consumer Privacy Act, Utah Code, Chapter 61, and its implementing regulations as the same may be amended from time to time; and

"VCDPA" means the Virginia Consumer Data Protection Act, Va. Code § 59.1-575 et. seq.

2. Scope and Applicability of this DPA. This DPA applies where and only to the extent that MindWire Processes Client Personal Data on behalf of Client as Data Processor in the course of providing the Services.

3. Roles and Scope of Processing.

3.1. **Role of the Parties**. As between MindWire and Client, MindWire shall Process Client Personal Data only as a Data Processor (or sub-processor) acting on behalf of Client and, with respect to CCPA, as a "service provider" as defined therein, in each case regardless of whether Client acts as a Data Controller or as a Data Processor on behalf of a third-party Data Controller ("**Third-Party Controller**") with respect to Client Personal Data.

3.2. **Client Instructions**. MindWire will Process Client Personal Data only for the Purposes. Client shall ensure its Processing instructions are lawful and that the Processing of Client Personal Data in accordance with such instructions will not violate applicable Data Protection Laws. The parties agree that the Agreement (including this DPA) sets out the exclusive and final instructions to MindWire for all Processing of Client

Personal Data, and (if applicable) include and are consistent with all instructions from Third-Party Controllers. Any additional requested instructions requires the prior written agreement of MindWire. MindWire shall promptly notify Client if, in MindWire's opinion, such an instruction violates EU & UK Data Protection Law. Where applicable, Client shall be responsible for any communications, notifications, assistance and/or authorizations that may be required in connection with a Third-Party Controller.

3.3. **Client Affiliates**. MindWire's obligations set forth in this DPA shall also extend to Authorized Affiliates, subject to the following conditions:

(a) Client must exclusively communicate any additional Processing instructions requested pursuant to 3.2 directly to MindWire, including instructions from its Authorized Affiliates;

(b) Client shall be responsible for Authorized Affiliates' compliance with this DPA and all acts and/or omissions by an Authorized Affiliate with respect to Client's obligations in this DPA shall be considered the acts and/or omissions of Client; and

(c) Authorized Affiliates shall not bring a claim directly against MindWire. If an Authorized Affiliate seeks to assert a legal demand, action, suit, claim, proceeding or otherwise against MindWire ("**Authorized Affiliate Claim**"): (i) Client must bring such Authorized Affiliate Claim directly against MindWire on behalf of such Authorized Affiliate, unless Data Protection Laws require the Authorized Affiliate be a party to such claim; and (ii) all Authorized Affiliate Claims shall be considered claims made by Client and shall be subject to any liability restrictions set forth in the Agreement, including any aggregate limitation of liability.

3.4. **Client Processing of Personal Data**. Client agrees that it: (i) will comply with its obligations under Data Protection Laws with respect to its Processing of Client Personal Data; (ii) will make appropriate use of the Services to ensure a level of security appropriate to the particular content of the Client Personal Data, such as pseudonymizing and backing-up Client Personal Data; and (iii) has obtained all consents, permissions and rights necessary under Data Protection Laws for MindWire to lawfully Process Client Personal Data for the Purposes, including, without limitation, Client's sharing and/or receiving of Client Personal Data with third parties via the Services.

3.5. **Details of Data Processing**.

(a) Subject Matter: The subject matter of the Processing under this DPA is the Client Personal Data.

(b) Frequency and duration: Notwithstanding expiry or termination of the Agreement, MindWire will Process the Client Personal Data continuously and until deletion of all Client Personal Data as described in this DPA.

(c) Purpose: MindWire will Process the Client Personal Data for the Purposes, as described in this DPA.

(d) Nature of the Processing: MindWire will perform Processing as needed for the Purposes, and to comply with Client's Processing instructions as provided in accordance with the Agreement and this DPA.

(e) Return or Deletion of Client Personal Data. Upon Client's request following expiration or termination of the Agreement, MindWire shall return to Client or destroy any Client Personal Data in MindWire's possession or control. This requirement shall not apply: (i) to the extent that Mindwire is required by applicable law to retain Client Personal Data; and/or (ii) Client Personal Data stored on MindWire's or any Sub-Processor's automatic electronic backup or disaster recovery systems until deleted in the ordinary course thereof; provided that Mindwire (and any Sub-Processor, as applicable) refrain from further Processing the Client Personal Data in performance of the Agreement, and comply with this DPA until Client Personal Data is returned or destroyed.

(f) Categories of Data Subjects: The categories of Data Subjects to which Client Personal Data relate are determined and controlled by Client in its sole discretion, and may include, but are not limited to:

- Employees (prospective or current), temporary workers and contractors of Client (who are natural persons);

(g) Categories of Personal Data: The types of Client Personal Data are determined and controlled by Client in its sole discretion, and may include, but are not limited to:

- Names and contact information
- Professional and employment information
- Additional data categories as may be outlined the Agreement.

(h) Special Categories of Personal Data: None.

3.6. **CCPA Terms.**

(a) Client is the "Business" and MindWire is the "Service Provider," for purposes of CCPA.

(b) Client discloses Client Personal Data to MindWire solely for the Purposes.

(c) Client is entitled, to the extent required under CCPA, to: (i) take reasonable and appropriate steps to ensure that MindWire uses Client Personal Data in a manner consistent with Client's obligations under CCPA; (ii) monitor MindWire's compliance to the extent required by CCPA; and (iii) take, upon notice, reasonable and appropriate steps to stop and remediate unauthorized use of Client Personal Data by MindWire to the extent required by CCPA.

(d) MindWire shall: (i) not "Sell" or "Share" Client Personal Data; (ii) not retain, use, or disclose the Client Personal Data: (A) outside the direct business relationship between MindWire and Client; or (B) for any purpose other than for the Purposes, unless otherwise permitted by the CCPA; (iii) upon instruction by Client, stop using Sensitive Personal Information for any purpose other than the Purposes to the extent Mindwire has actual knowledge that the Client Personal Data is Sensitive Personal Information; (iv) not combine Client Personal Data with other personal data that MindWire receives from, or on behalf of, other Clients, unless permitted by CCPA; (v) refrain from attempting to re-identify any de-identified information disclosed by Client to MindWire under the Agreement; (vi) only subcontract any Processing of Client Personal Data pursuant to Section 4 of this DPA ("Sub-Processing"); (viii) reasonably assist Client in responding to Data Subject Requests pursuant to Section 9 of this DPA ("Cooperation"); (ix) promptly notify Client if MindWire determines that MindWire can no longer meet its obligations under CCPA or under this Section; and (x) remain liable for MindWire's own violations of CCPA. "Business," "Selling," "Sensitive Personal Information" and "Service Provider" as used in this Section shall have the meaning set forth in CCPA.

4. Sub-Processing.

4.1. **Authorized Sub-Processors**. Client provides MindWire with a general authorization to engage Sub-processors, subject to Section 4.3 (Changes to Sub-processors), as well as MindWire's current Sub-processors provided to Client by MindWire upon request ("**Current Sub-processors**") as of the DPA Effective Date.

4.2. **Sub-Processor Obligations**. MindWire shall: (i) enter into a written agreement with each Sub-processor imposing data protection obligations materially no less protective of Client Personal Data as MindWire's obligations under this DPA to the extent applicable to the nature of the services provided by such Sub-processor; and (ii) remain liable for each Sub-processor's compliance with the obligations under this DPA. Upon written request, and subject to any confidentiality restrictions, MindWire shall use reasonable efforts to provide Client all relevant information it reasonably can in connection with its applicable Sub-processor agreements where required to satisfy Client's obligations under Data Protection Laws.

4.3. **Changes to Sub-Processors**. MindWire shall provide notice to Client of the addition of any new Sub-Processors. MindWire shall provide such notification at least fourteen (14) days in advance of allowing the new Sub-processor to Process Client Personal Data (the "**Objection Period**"). During the Objection Period, objections (if any) to MindWire's appointment of the new Sub-processor must be provided to MindWire in writing and based on reasonable grounds relating to data protection. In such event, the parties will discuss those objections in good faith with a view to achieving resolution. If it can be reasonably demonstrated to MindWire that the new Sub-processor is unable to Process Client Personal Data in compliance with the terms of this DPA and MindWire cannot provide an alternative Sub-processor, or the parties are not otherwise able to achieve resolution as provided in the preceding sentence, Client, as its sole and exclusive remedy, may provide written notice to MindWire terminating the Order Form(s) with respect only to those aspects of the Services which cannot be provided by MindWire without the use of the new Sub-processor. MindWire will refund Client any prepaid unused fees of such Order Form(s) following the effective date of termination with respect to such terminated Services.

5. Security.

5.1. **Security Measures**. MindWire shall implement and maintain appropriate technical and organizational security measures designed to protect Client Personal Data from Security Incidents and to preserve the security and confidentiality of the Client Personal Data in accordance with the measures set forth in Appendix 1 ("**Security Addendum**"). MindWire may review and update its Security Addendum from time to time, provided that any such updates shall not materially diminish the overall security of the Services or Client Personal Data.

5.2. **Confidentiality of Processing**. MindWire shall ensure that any person who is authorized by MindWire to Process Client Personal Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

5.3. **No Assessment of Client Personal Data by MindWire**. MindWire shall have no obligation to assess the contents or accuracy of Client Personal Data, including to identify information subject to any specific legal, regulatory, or other requirement. Client is responsible for reviewing the information made available by MindWire relating to data security and making an independent determination as to whether the Services meet Client's requirements and legal obligations under Data Protection Laws.

6. Client Audit Rights.

6.1. Upon written request and at no additional cost to Client, MindWire may provide Client, and/or its appropriately qualified third-party representative (collectively, the "**Auditor**"), access to reasonably requested documentation evidencing MindWire's compliance with its obligations under this DPA (collectively, "**Reports**"). In the event that the Reports are not available or are not sufficient to fulfill Client's obligations under applicable Data Protection Laws, MindWire shall, to the extent required by applicant Data Protection Laws: (a) provide additional documentation and information as reasonably necessary; and (b) allow for an contribute to audits in order to assess MindWire's compliance with this DPA (such audits shall not take place more than once in any twelve (12) month period, shall not unreasonably interfere with MindWire's operations, shall require no less than sixty (60) days written notice to MindWire, and shall not require MindWire to disclose information or data relating to any other Client or that is subject to confidentiality obligations).

7. Data Transfers.

7.1. **Hosting and Processing Locations**. Client acknowledges that MindWire may transfer Client Personal Data to countries outside of the European Economic Area and its member states, United Kingdom and/or Switzerland in order to provide the Services. Client hereby consents to such transfers of Client Personal Data subject to MindWire's compliance with applicable Data Protection Laws, including the obligations set forth in this Section 7.

7.2. **Transfer Mechanisms**. For any transfers by Client of Client Personal Data from the European Economic Area and its member states, United Kingdom and/or Switzerland (collectively, "**Restricted Countries**") to MindWire in a country which does not ensure an adequate level of protection (within the meaning of and to the extent governed by the applicable Data Protection Laws of the Restricted Countries) (collectively, "**Third Country**"), such transfers shall be governed by a valid mechanism for the lawful transfer of Client Personal Data recognized under applicable Data Protection Laws, such as those directly below in 7.2.1. For clarity, for transfers from the United Kingdom and Switzerland, references in the SCCs shall be interpreted to include applicable terminology for those jurisdictions (e.g., 'Member State' shall be interpreted to mean 'United Kingdom' for transfers from the United Kingdom).

7.2.1. SCCs: Each party agrees to abide by and transfer Client Personal Data from the Restricted Countries in accordance with the EU SCCs and UK Addendum respectively and where applicable, which are incorporated into this DPA by reference. Each party is deemed to have executed the SCCs as of the Effective Date by entering into this DPA and such details shall apply for the purposes of Table 1 of the UK Addendum.

(a) The below shall apply to the SCCs, including the election of specific terms and/or optional clauses as described in more detail in (i)-(x) below, and any optional clauses not expressly selected are not incorporated (including with respect to Table 2 of the UK Addendum):

(i) The Module 2 terms apply to the extent Client is a Data Controller and the Module 3 terms apply to the extent Client is a Data Processor of the Client Personal Data. The foregoing shall apply with respect to Table 2 of the UK Addendum;

(ii) The optional Clause 7 in Section I of the SCCs is incorporated, and Authorized Affiliates may accede to this DPA and the SCCs under the same terms and conditions as Client, subject to Section 3.3 of this DPA via mutual agreement of the parties. The foregoing shall apply with respect to Table 2 of the UK Addendum;

(iii) For purposes of Clause 9 of the SCCs, Option 2 ('General written authorization') is selected and the process and time period for the addition or replacement of Sub-processors shall be as described in Section 4 (Sub-processing) of this DPA. The foregoing shall apply with respect to Table 2 of the UK Addendum;

(iv) For purposes of Clause 13 and Annex 1.C of the EU SCCs, Client shall maintain accurate records of the applicable Member State(s) and competent supervisory authority, which shall be made available to MindWire on request;

(v) For purposes of Clause 14(c), Client may request from MindWire notifications regarding updates to MindWire's overview of relevant laws and practices of Third Countries;

(vi) For purposes of Clause 17 and Clause 18 of the EU SCCs, the Member State for purposes of governing law and jurisdiction shall be the Netherlands. Part 2, Section 15(m) and Part 2, Section 15(n) of the UK Addendum regarding Clause 17 and Clause 18 of the EU SCCs shall apply;

(vii) For purposes of Annex 1.A, the 'data importer' shall be MindWire and the 'data exporter' shall be Client and any Authorized Affiliates that have acceded to the SCCs pursuant to this DPA. The foregoing shall apply with respect to Table 3 of the UK Addendum;

(viii) For purposes of Annex 1.B, the description of the transfer is as described in Section 3.5 (Details of Data Processing) of this DPA. The foregoing shall apply with respect to Table 3 of the UK Addendum;

(ix) For purposes of Annex 2, the technical and organization measures are as follows: (i) Those measures implemented by MindWire shall be as described in Section 5.1 (Security Measures) of this DPA; and (ii) Those measures that can be selected or configured by Client, including appropriate controls for 'special categories of data', shall be as further described in MindWire's Documentation. The foregoing shall apply with respect to Table 3 of the UK Addendum; and

(x) The Sub-processors for Annex III shall be as described in Section 4.1 (Authorized Sub-processors) of this DPA. The foregoing shall apply with respect to Table 3 of the UK Addendum; and

(xi) With respect to Table 4 of the UK Addendum, Client may suspend or terminate the Processing of the Client Personal Data by MindWire that is subject to UK GDPR at any time by deleting all such Client Personal Data in the Service. Additionally, either party may terminate the UK Addendum pursuant to Section 19 of the UK Addendum if, after a good faith effort by the parties to amend this DPA to account for the approved changes and any reasonable clarifications to the UK Addendum, the parties are unable to come to a mutual agreement

8. Security Incident Response.

8.1. **Security Incident Reporting**. If MindWire becomes aware of a Security Incident, MindWire shall notify Client without undue delay, and in any case, where feasible, notify Client within seventy-two (72) hours after becoming aware. MindWire's notification shall be sent to the email registered by Client within the Service for such purposes, and where no such email is registered, Client acknowledges that the means of notification shall be at MindWire's reasonable discretion and MindWire's ability to timely notify shall be negatively impacted. MindWire shall promptly take commercially reasonable steps to assist Client in its efforts to contain, investigate, and mitigate any Security Incident.

8.2. **Security Incident Communications**. MindWire shall provide Client timely information about the Security Incident, including, but not limited to, to the extent known, the nature and consequences of the Security Incident, the measures taken and/or proposed by MindWire to mitigate or contain the Security Incident, the status of MindWire's investigation, a contact point from which additional information may be obtained, and the categories and approximate number of data records concerned. Notwithstanding the foregoing, Client acknowledges that because MindWire personnel do not have visibility to the content of Client Personal Data, it will be unlikely that MindWire can provide information as to the particular nature of the Client Personal Data, or where applicable, the identities, number or categories of affected Data Subjects. Communications by or on behalf of MindWire with Client in connection with a Security Incident shall not be construed as an acknowledgment by MindWire of any fault or liability with respect to the Security Incident.

9. **Cooperation.**

9.1. **Data Subject Requests**. In the event MindWire receives a request from a Data Subject that identifies Client Personal Data or otherwise identifies Client, including where the Data Subject seeks to exercise any of its rights under applicable Data Protection Laws (collectively, "**Data Subject Request**"), MindWire shall (unless prohibited by law) direct the Data Subject to Client in the first instance. The Service provides Client with a number of controls that Client may use to assist it in responding to Data Subject Requests and Client will be responsible for responding to any such Data Subject Requests. To the extent Client is unable to access the relevant Client Personal Data within the Services using such controls or otherwise, MindWire shall (upon Client's written request and taking into account the nature of the Processing) provide commercially reasonable cooperation to assist Client in responding to Data Subject Requests.

9.2. **Data Protection Impact Assessments**. MindWire shall provide reasonably requested information regarding the Services to enable Client to carry out data protection impact assessments or prior consultations with data protection authorities as required by Data Protection Laws, so long as Client does not otherwise have access to the relevant information.

9.3. **Government, Law Enforcement, and/or Third-Party Inquiries**. If MindWire receives a demand to retain, disclose, or otherwise Process Client Personal Data for any third party, including, but not limited to law enforcement or a government authority ("**Third-Party Demand**"), then MindWire shall attempt to redirect the Third-Party Demand to Client. Client agrees that MindWire can provide information to such third-party as reasonably necessary to redirect the Third-Party Demand. If MindWire cannot redirect the Third-Party Demand to Client, then MindWire shall, to the extent legally permitted to do so, provide Client reasonable notice of the Third-Party Demand as promptly as feasible under the circumstances to allow Client to seek a protective order or other appropriate remedy. This section does not diminish MindWire's obligations under the SCCs with respect to access by public authorities.

10. Relationship with the Agreement.

10.1. The parties agree that this DPA shall replace and supersede any existing data processing addendum, attachment, exhibit or standard contractual clauses that MindWire and Client may have previously entered into in connection with the Services. MindWire may update this DPA from time to time, with such updated version provided by MindWire to Client by email notice; provided, however, that no such update shall materially diminish the privacy or security of Client Personal Data.

10.2. Except as provided by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict in connection with the Processing of Client Personal Data.

10.3. Notwithstanding anything to the contrary in the Agreement or this DPA, each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or relating to this DPA, the SCCs, and any other data protection agreements in connection with the Agreement (if any), shall be subject to any aggregate limitations on liability set out in the Agreement. Without limiting the parties' obligations under the Agreement, each party agrees that any regulatory penalties incurred by one party (the "**Incurring Party**") in relation to the Client Personal Data that arise as a result of, or in connection with, the other party's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce the Incurring Party's liability under the Agreement as if it were liability to the other party under the Agreement.

10.4. In no event shall this DPA benefit or create any right or cause of action on behalf of a third party (including a Third-Party Controller), but without prejudice to the rights or remedies available to Data Subjects under Data Protection Laws or this DPA (including the SCCs).

10.5. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement.

MindWire, Inc.,	**[CLIENT NAME]**
Name	Name
Signature	Signature
Title	Title
Date	Date

Appendix 1

Security Measures

The following details MindWires' administrative, physical, technical and organizational security measures with respect to the Processing of Personal Data. If applicable, this Appendix forms part of the Standard Contractual Clauses and is deemed signed by the parties upon signature to the Services Agreement.

1. Physical Access Controls: data importer shall take reasonable measures to prevent physical access, such as security personnel and secured buildings and factory premises, to prevent unauthorized persons from gaining access to Client Personal Data.

2. System Access Controls: data importer shall take reasonable measures to prevent Client Personal Data from being used without authorization. These controls shall vary based on the nature of the processing undertaken and may include, among other controls, authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes and/or, logging of access on several levels.

3. Data Access Controls: data importer shall take reasonable measures to provide that Client Personal Data is accessible and manageable only by properly authorized staff, direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the personal data to which they have privilege of access; and, that Client Personal Data cannot be read, copied, modified or removed without authorization in the course of processing. In addition to the access control rules set forth in Sections 1- 3 above, data importer implements an access policy under which access to its system environment, to personal data and other data by authorized personnel only.

4. Transmission Controls: data importer shall take reasonable measures to ensure that it is possible to check and establish to which entities the transfer of personal data by means of data transmission facilities is envisaged so Client Personal Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport.

5. Input Controls: data importer shall take reasonable measures to provide that it is possible to check and establish whether and by whom Client Personal Data has been entered into data processing systems, modified or removed. Data importer shall take reasonable measures to ensure that (i) the Client Personal Data source is under the control of data exporter; and (ii) personal data integrated into data importer's systems is managed by secured file transfer from the data importer and data subject.

6. Data Backup: data importer shall ensure that back-ups are taken on a regular basis, are secured, and encrypted when storing Client Personal Data to protect against accidental destruction or loss when hosted by data importer.