Data Processing Agreement (DPA)

Main Agreement and date ("Agreement")	
Customer Name and Address for Notices	
Service Provider legal entity and Address for Notices	
Data Processing Agreement Effective Date	

Service Provider and Customer hereinafter collectively referred to as the "Parties" or separately, "Party".

This Data Processing Agreement ("DPA") forms part of the Agreement between the Customer and Service Provider. In consideration of the mutual obligations set out in this DPA, the Parties hereby agree that the terms and conditions set forth below shall be added as an addendum to the Agreement. Except as modified below, the Agreement shall remain in full force and effect.

Any capitalized terms not otherwise defined in this DPA will have the meaning assigned to them in the Agreement or in the applicable Data Protection Law.

1 Interpretation

1.1 In this DPA, the following terms shall have the following meanings:

"Controller", "Processor", "Data Subject", "Data Subject Request", "Personal Data", "Personal Information", "Process", "Processing", "Supervisory Authority", "Third Country" shall have the meaning given to them in the applicable Data Protection Law.

"Data Protection Law" means any Law that applies from time to time to the processing of Personal Data by either Party under this DPA and to include all relevant national implementing legislation and subordinate legislation and any applicable decisions and guidance made under them. **Annex 4** to this DPA outlines the Data Protection Requirements per relevant countries, that shall supplement this DPA whenever applicable. In case of conflict or inconsistency between the terms of this DPA and Annex 4, the terms and requirements under **Annex 4** shall prevail.

"Customer Data" means any Personal Data relating to an identified or identifiable natural person disclosed to Service Provider by or on behalf of the Customer pursuant to the Agreement. The processing Purpose, the types of Customer Data and Categories of Data Subjects, Approved Sub-processors are further specified in **Annex 1** (Details of Processing) to this DPA.

"**EU Standard Contractual Clauses**" means the standard contractual clauses forming part of Decision (EU) 2021/914/EC (as amended or replaced from time to time), including their appendices and with the relevant Modules and Options.

"Service Provider Personal Data" means the Personal Data of Service Provider employees or personnel that Service Provider may disclose to the Customer, and/or the Customer may otherwise obtain, in connection with provision of Services under the Agreement.

"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, as maybe amended, updated, replaced or superseded from time to time.

"Law" means any statute, directive, other legislation, law or regulation in whatever form, delegated act (under any of the foregoing), rule or other binding restriction, decision, or guidance in force from time to time.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Data.

"Services" means the activities and services required to be rendered or performed by Service Provider under the Agreement or as may be set out in the applicable Customer Service Order Form or Statement of Work;

"Standard Contractual Clauses" means the EU Standard Contractual Clauses and the UK Addendum, as applicable.

"Sub-processor" means a Processor engaged by Service Provider to process Customer Data.

"TOMs Schedule" means Annex 3 *(Technical and Organizational Measures)* which describes the technical and organizational measures which Service Provider is required to maintain and which the Parties expressly agree shall apply to the data protection terms of this DPA.

"**UK Addendum**" means the Addendum to the EU Standard Contractual Clauses issued by the UK Information Commissioner's Office in accordance with S119A of the UK Data Protection Act 2018 and as amended or superseded by the UK data protection framework established under the Data (Use and Access) Act 2025 (DUAA 2025).

1.2 Where any expressions in this DPA are defined by reference to a particular Data Protection Law and such Data Protection Law is amended, extended, applied, consolidated or re-enacted such that the relevant expression is no longer used, the expressions in this DPA shall be interpreted to refer to the terms used within the Data Protection Law as amended, extended, applied, consolidated or re-enacted as most closely relate to the meaning of those expressions prior to the amendment, extension, application, consolidated or re-enacted of such Data Protection Law.

1.3 This DPA is subject to the terms of the Agreement and is incorporated into the Agreement. This DPA shall remain in full force and effect so long as the Agreement remains in effect. In case of conflict between this DPA and the Agreement, the terms of this DPA shall prevail.

1.4 With regard to the processing of Customer Data, Customer is the Controller and Service Provider is the Processor, except when the Customer acts as Processor of such Customer Data on behalf of a third-party Controller, in which case Service Provider is a Sub-processor.

1.5 Each Party represents and warrants that it shall always comply with this DPA and Data Protection Law. Both Parties shall implement appropriate technical and organisational measures against unauthorized or unlawful processing, and against accidental loss or destruction of or damage to the Personal Data, to ensure compliance with Data Protection Law.

1.6 The Annexes (as amended or updated from time to time) to this DPA and all documents delivered pursuant to this DPA shall form an integral part of this DPA. In the event of any express conflict or inconsistency between the provisions of an Annex and the provisions of this DPA, the provisions of such Annex will govern or prevail with respect to the interpretation of such Annex; provided, however, that the provisions of such Annex will be construed to give effect to the applicable provisions of this DPA to the fullest extent possible.

2 Servicer Provider Responsibilities

2.1 Service Provider will only process Customer Data to the extent, and in such a manner, as is necessary for the provision of Services, and in accordance with Customer's documented instructions. If Service Provider considers that any instruction from Customer contravenes the Data Protection Law, it shall immediately notify Customer, giving reasonable details.

2.2 Service Provider will promptly comply with any Customer request or instruction requiring Service Provider to update, amend, transfer, delete or otherwise process the Customer Data.

2.3 Service Provider will ensure that all its employees and representatives who process Customer Data are: (i) bound by appropriate obligations of confidentiality in respect of the Customer Data and understand that the Customer Data is confidential in nature; (ii) have undertaken training in the laws relating to processing of Personal Data and how it applies to their particular duties; and (iii) are aware both of Service Provider's obligations and their personal obligations under such Data Protection Law and this DPA, whether under contract or otherwise.

2.4 Service Provider will ensure that access to Customer Data is limited to: (i) those employees and representatives of Service Provider and of its Sub-processor who need access to Customer Data; and (ii) such disclosure of Customer Data is strictly necessary for performance of that employee's duties.

2.5 Service Provider will reasonably assist Customer with meeting Customer's compliance obligations under Data Protection Law in relation to the processing of the Customer Data, including in relation to data protection impact assessments and/or prior consultation, having regard to the nature of the processing and the information available to Service Provider.

2.6 Service Provider, using commercially reasonable efforts, will implement appropriate technical and organizational measures against unauthorised or unlawful processing of Customer Data, and against accidental loss or destruction of or damage to Customer Data, to ensure compliance with Data Protection Law. For the avoidance of doubt, Service Provider will implement the agreed technical and organizational measures as set forth in **Annex 3**.

2.7 Service Provider must promptly on termination or expiry of the Agreement, or otherwise at the written instruction of the Customer, return or permanently delete all Customer Data, including any copies thereof, in its possession or control, except to the extent Service Provider is required by the applicable Law to retain such Customer Data. Service Provider will, upon Customer's written request, issue a signed certificate confirming deletion or return of Customer Data.

3 Customer responsibilities

3.1 Customer undertakes to comply with all obligations laid down in applicable Data Protection Law, for Controllers, including, but not limited to, ensure the lawfulness of the processing of Personal Data, provide information to Data Subjects and secure their consent pursuant to applicable Data Protection Law, and maintain a record of processing activities under its responsibility.

3.2 Customer shall provide Service Provider with all necessary information and assistance to enable Service Provider to process the personal data in accordance with this DPA, including but not limited to obtaining all necessary consents and authorizations required under applicable Data Protection Law, to allow the processing of Personal Data pursuant to the Agreement.

4 Audits

4.1 Service Provider will make available to Customer, upon written request, all relevant information necessary to demonstrate compliance with the obligations laid down in this DPA and Data Protection Law.

4.2 Customer shall have the right to perform audits on Service Provider's processing of Customer Data to verify Service Provider's compliance with this DPA. Such audits shall be subject to reasonable written notice by Customer of no less than 10 business days and will be limited to no more than once every 12 months, unless Customer has reasonable grounds to believe Service Provider is not in compliance with Data Protection Law. Each Party shall bear its own costs in relation to such audits.

5 Data Subject Requests

5.1 Service Provider will provide reasonable assistance, and in accordance with Customer's instruction, in responding to any Data Subject Request which is received by Customer or Service Provider. Service Provider will not acknowledge or respond to any such Data Subject Request, nor disclose any of the Customer Data to any Data Subject or to any third party, other than upon and in accordance with Customer's instructions.

5.2 If Service Provider receives any complaint, notice or communication regarding the processing of Customer Data by Service Provider on behalf of the Customer, it will promptly notify Customer and shall in no event respond directly, unless with the Customer's prior written instruction. It shall provide reasonable co-operation and assistance in relation to any such complaint, notice or communication.

6 Personal Data Breaches

6.1 Service Provider shall promptly (and in no case later than 48 hours after becoming aware of the Personal Data Breach) inform Customer, in writing, of any Personal Data Breach directly affecting Customer Data. Such notification shall contain (at a minimum):

a) the nature of the Personal Data Breach;
b) the date and time of occurrence;
c) the extent of the Customer Data and Data Subjects affected;
d) the likely consequences of the Personal Data Breach and any measures taken or proposed to be taken by Service Provider to contain the Personal Data Breach; and
e) any other information that Customer shall require to discharge its responsibilities under Data Protection Law in relation to such Personal Data Breach.

6.2 Service Provider will thereafter promptly (i) provide Customer with all such information as Customer requests in connection with such Personal Data Breach; (ii) take such steps as Customer

reasonably requires it to take to mitigate the detrimental effects of any such Personal Data Breach on any of the Data Subjects and/or on Customer; and (iii) otherwise cooperate with Customer in investigating and dealing with such Personal Data Breach and its consequences.

7 Use of Sub-processor

7.1 Service Provider may make use of Sub-processors in accordance with Annex 2.

7.2 Service Provider shall inform the Customer, in writing, of any intended changes concerning the addition or replacement of Sub-processors at least 30 days in advance. The Customer may submit an objection within this period of time, in which case it shall endeavour to explain the reasons why it objects to said Sub-processor, without being obligated to do so. In the event of such an objection, even if Service Provider does not agree with the Customer's position, the Sub-processor shall not be engaged for processing Customer Data and the Parties will work in good faith to attempt to mutually resolve the matter.

7.3 Service Provider shall enter into a written contract with the Sub-processor that contains terms substantially the same as those set out in this DPA. If Service Provider uses cloud telephony or other cloud providers in support of the Agreement, the Customer recognizes that such services are provided on the basis of standardized agreements and the Service Provider's obligations with respect to Sub-processors contained in this DPA shall apply to the extent they are compatible with the standardized agreements and as updated from time to time.

7.4 Service Provider shall be responsible for the acts and omissions of any such Sub-processor.

8 International Data Transfers

8.1 Service Provider will comply with the EU Standard Contractual Clauses adopted by the European Commission, together with the UK Addendum where applicable, as a lawful mechanism for international transfers of Personal Data. The applicable EU Standard Contractual Clauses and UK Addendum are set out in Annex 6 of this DPA .

9 Analytics Solutions (optional)

9.1 Service Provider will provide analytics services to the Customer on a non-exclusive basis, in accordance with the terms and conditions set forth in the Agreement.

9.2 In connection with the analytics services provided by Service Provider to the Customer, Service Provider may collect, process, and analyse Personal Data on behalf of the Customer. Service

Provider will ensure that all Personal Data processed is done in compliance with applicable Data Protection Law and this DPA.

9.3 Service Provider will not use the Personal Data for any purposes other than for the purpose of providing the analytics services to the Customer and will not disclose the Personal Data to any third party without the Customer's prior written consent, except as required by Law.

9.4 Customer represents and warrants that it has obtained all relevant consents or has a legal basis for the analytic processing of the Personal Data.

10 AI Solutions (optional)

10.1 Service Provider will provide services to the Customer that include AI features on a non-exclusive basis, in accordance with the terms and conditions set forth in the Agreement. The AI services shall be performed using reasonable care and skill in accordance with industry standards.

10.2 The Customer acknowledges that the AI services provided by Service Provider are subject to change based on industry developments, technological advances, and other factors beyond Service Provider's control.

10.3 Service Provider shall process Customer Personal Data for the purpose of providing the AI services to the Customer. The Customer shall provide Service Provider with all necessary information and assistance to enable Service Provider to process the data in accordance with the Agreement and this DPA.

10.4 Service Provider ensures that Customer personal data used in the development of the AI services, including training, validation, and testing, has been and shall be subject to data governance appropriate for the context of use as well as the intended purpose of the AI solution. Those measures shall concern in particular:

a) Transparency regarding the original purpose of data collection;
b) The relevant design processes;
c) Data collection processed;
d) Data preparation for processing operations, such as annotation, labelling, cleaning, enrichment, and aggregation;
e) The formulation of relevant assumption, notably with respect to the information that the data are supposed to measure and represent;
f) Examination in view of possible biases that are likely to affect health and safety of natural persons or lead to discrimination prohibited by the applicable laws;
g) Appropriate measures to detect, prevent, and mitigation possible biases;
h) The identification of relevant data gaps or shortcomings that prevent compliance with this DPA and how those gaps and shortcomings can be addressed.

10.5 Service Provider ensures that the AI solution has been and shall be designed and developed in such a way, including with appropriate human-machine interface tools, that it can be effectively overseen by natural persons as proportionate to the risks associated to the AI solution.

10.6 Customer represents and warrants that it has obtained all relevant consents or has a legal basis for AI processing of the Personal Data.

11 Liability

11.1 Service Provider will not incur liability or responsibility to Customer or any third party for any claims, damages or causes of action under this DPA or a relevant statement of work, including but not limited to, any data breaches to the extent resulting from Customer's failure to implement and maintain reasonable security controls within Customer's systems and networks, failure to comply with its data protection obligations, including but not limited to failure to obtain necessary consents, failure to ensure the lawfulness of processing, or failure to implement appropriate technical and organizational measures to protect Personal Data.

11.2 The Parties agree that in the event a Party identifies and notifies the other party of a vulnerability in its systems, procedures or methodologies, the other party shall promptly assess and take commercially reasonable steps to correct such vulnerability to prevent the vulnerability or loss from occurring again, or in the event the Party fails to correct such vulnerability, the other Party shall not be liable for any future exploitation of such un-remedied vulnerability.

11.3 Any liability arising from any losses, costs, damages, awards of compensation, any monetary penalty notices or administrative fines for breach of Data Protection Law and/or expenses (including legal fees and expenses) suffered, incurred, or awarded, levied or imposed against either Party, as a direct result of any breach under this DPA shall be subject to the limitations of liability and indemnity provisions set forth in the Agreement.

11.4 Nothing in this DPA relieves either Party of its own direct responsibilities and liabilities under the applicable Data Protection Law.

12 Service Provider Personal Data

12.1 During the provision of the Services, it is acknowledged that Service Provider may disclose to Customer, and/or the Customer may otherwise obtain, Service Provider Personnel Data. The Parties acknowledge that they each act as independent Controllers in relation to such Service Provider Personal Data with respect to the Purpose.

12.2 In relation to Service Provider Personal Data in this clause, "Purpose" means the limited use of the Service Provider Personal Data to manage and provide access to systems and tools controlled by the Customer, restricted use to verify compliance with legal requirements or to enable the development, compliance and control of the agreed provision of Services, the limited use for internal technical operations to enable Service Provider to provide Services under the Agreement.

12.3 Customer shall:

a) comply with its obligations as a Controller under applicable Data Protection Law in respect of Service Provider Personal Data;

b) process Service Provider Personal Data only for the Purpose;
c) comply with the information duties set forth in applicable Data Protection Law and make available an applicable Privacy Notice to Service Provider, if required;
d) immediately notify Service Provider in writing, within 48 hours of any Personal Data Breach affecting Service Provider Personal Data;
e) not use the Service Provider Personal Data to generate any performance evaluations or reports in respect of any Service Provider personnel on an individual or named basis, without the prior written agreement of Service Provider;
f) process Service Provider Personal Data within the Customer system with pseudonymized logins and/or IDs whenever possible; and
g) provide Service Provider with access to raw data and reports to the extent required for that Service Provider to manage its employees and assess the quality of the Services.

13. Governing law and jurisdiction

13.1 This DPA and other obligations arising out of or in connection with this DPA are subject to the governing law and jurisdiction of the Agreement.

The Parties' authorized signatories have duly executed this DPA.

Customer	**Service Provider**
Signature:	Signature:
Name:	Name:
Title:	Title:
Date:	Date:

Annex 1

Details of Processing (Customer Data)

1. Processing Purpose

Service Provider will process Customer Data as necessary to perform the Services pursuant to the Agreement and as further instructed by the Customer in its use of the Services.

2. Categories of Data Subjects

Service Provider will process the Personal Data of the following categories of Data Subjects *(select all that apply)*:

- ☐ Current, former or prospective Customer customers
- ☐ Current, or former Customer employees, contractors, temporary workers, or beneficiary/dependents, or other related Data Subjects
- ☐ Current, or former Customer supplier or other business partners
- ☐ Children or other vulnerable Data Subjects
- ☐ Other (Service Provider to insert details):

3. Categories of Personal Data

Service Provider will process the following categories of Customer *(select all that apply)*:

- ☐ Contact information (e.g., name, address, email address, phone number, etc.)
- ☐ Financial information (such as credit card numbers, bank information, salary and/or financial benefits details, credit score etc.)
- ☐ Professional and employment information (e.g., occupation, title, income, salary, etc.)
- ☐ Purchasing/transactional information
- ☐ Account information (e.g., username, password, account metadata)
- ☐ Communications Content
- ☐ Location information
- ☐ Online identifiers (e.g., IP address, cookies, beacons)
- ☐ Device information (e.g., operating system, language preferences)
- ☐ Internet or other Online Data (e.g., browsing or search history, usage data, in-app tracking, etc.)
- ☐ Other (Service Provider to insert details):

- ☐ Special Category Data (Service Provider to insert details and specific categories of special category data):

Annex 2

Sub-processors

Service Provider is authorized by the Customer to engage the following Sub-processors with respect to this DPA.

Name of Sub-Processor	Registered address	Purpose and description of processing

Annex 3

Technical and Organizational Measures

This Section describes the technical and organizational security measures and procedures that Service Provider shall, as a minimum, maintain to protect the security of Personal Data created, collected, received, or otherwise obtained. Service Provider will keep documentation of technical and organizational security measures identified below to facilitate audits and for the conservation of evidence. Service Provider will, at any time, comply with the specific statutory requirements for technical and organizational security measures.

All controls listed below for systems or applications are applicable only to the extent of those systems or applications within the scope of control to manage/modify of Service Provider and also their applicability to the data being processed and the service being provided under the Agreement to which this document is attached.

Access Control to Processing Areas

Service Provider implements suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment where the Personal Data is processed or used. This is accomplished by:

- establishing security areas; protection and restriction of access paths;
- securing the decentralized data processing equipment and personal computers;
- establishing access authorizations for staff and third parties, including the respective documentation;
- regulations on card-keys;
- restriction on card-keys;
- all access to the data center where Personal Data is hosted is logged, monitored, and tracked; and
- the data center where Personal Data is hosted is secured by restricted access controls, and other appropriate security measures.

Access Control to Data Processing Systems

Service Provider implements suitable measures to prevent its data processing systems from being used by unauthorized persons. This is accomplished by:

- identification of the terminal and/or the terminal user to the data exporter systems;
- automatic time-out of user terminal if left idle, with user identification and password required to reopen;
- automatic temporary disabling of the user identification when several erroneous passwords are entered, along with log file of events (monitoring of break-in-attempts);
- issuing and safeguarding of unique user identification; and
- dedication of individual terminals and/or terminal users, identification characteristics exclusive to specific functions.

Access Control to Use Specific Areas of Data Processing Systems

Service Provider commits that the persons entitled to use its data processing system are only able to access the data within the scope and to the extent covered by its access permission (authorization) and that Personal Data cannot be read, copied or modified or removed without authorization. This shall be accomplished by:

- employee policies and training with respect to each employee's access rights to the Personal Data;
- allocation of individual terminals and/or terminal users, and identification characteristics exclusive to specific functions;
- monitoring capability with respect to individuals who delete, add, or modify the Personal Data;
- effective and measured disciplinary action against individuals who access Personal Data without authorization;
- release of data only to authorized persons;
- control of files, and controlled and documented destruction of data; and
- policies controlling the retention of back-up copies.

Transmission Control

Service Provider implements suitable measures to prevent Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by:

- use of state-of-the-art firewall and encryption technologies to protect the gateways and pipelines through which the data travels;
- monitoring of the completeness and correctness of the transfer of data (end-to-end check).

Input Control

Service Provider implements suitable measures to ensure that it is possible to check and establish whether and by whom Personal Data has been input into data processing systems or removed. This is accomplished by:

- an authorization policy for the input of data, as well as for the reading, alteration, and deletion of stored data;
- authentication of authorized personnel; protective measures for the data input, as well as for the reading, alteration, and deletion of stored data; utilization of user codes (passwords);
- providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) can be locked/secured;
- automatic log-off of user identifications that have not been used for a substantial period of time; and
- proof established within Service Provider’s organization of the input authorization, and electronic recording of entries.

Availability Control

Service Provider shall implement suitable measures to make sure that Personal Data is protected from accidental destruction or loss. This will be accomplished by:

- infrastructure redundancy; and
- sending real-time backup replications securely to secure offsite storage location in case of failure of infrastructure where applicable and agreed.

Job Control

Service Provider implements suitable measures to ensure that, in the case of commissioned processing of Personal Data, the Personal Data is processed strictly in

accordance with the instructions of the Customer. This is accomplished by:

- ensuring clear instructions regarding the scope of any processing of Personal Data; and
- granting regular access and control rights, on appropriate notice and accompanied by Service Provider.

Separation of processing for different purposes

Service Provider implements suitable measures to ensure that data collected for different purposes can be processed separately. This is accomplished by:

- access to data shall be separated through application security for the appropriate users;
- at the database level, data shall be stored in different normalized tables, and separated per module or function they support; and
- interfaces, batch processes, and reports shall be designed for only specific purposes and functions, so data collected for specific purposes is processed separately.

Anti-Virus Protection

Service Provider must ensure that anti-virus software is deployed on all servers, PCs and laptop computers with regular virus definition updates and scanning across all devices. Additionally, mail servers with internet mail gateways run appropriate scanning and outbreak control software which is regularly updated. The anti-virus software on all servers and endpoints is configured to pull signatures multiple times a day and perform scans of the hard drive and endpoints on a weekly basis.

Data Encryption

All requests to implement data transmission or storage processes and procedures are risk assessed to ensure Customer Data will always be appropriately encrypted both during transmission and at rest.

Service Provider standardizes on industry standard encryption protocols and algorithms. Deviations from standards require approval by the Customer and the Service Provider.

Furthermore, Service Provider shall review and continue to review its security programs and procedures to ensure that they are adequate, having regard to the risks with which Service Provider may be confronted, the nature of the data, industry good practice, and the cost of their implementation at that time.

Annex 4

Country Specific Data Protection Requirements

This Annex sets out the high-level Data Protection Requirements per relevant countries and/ or jurisdictions, that are lifted from the applicable Data Protection Law. Parties understand and agree that all other requirements from the Data Protection Law that are not explicitly stated in this Annex, are deemed incorporated into this Annex, to the extent applicable, including any amendments or modifications to the Data Protection Law.

CANADA DATA PROTECTION REQUIREMENTS -

1. **Definitions.** For the purposes of this Annex:

    a. "**Data Protection Laws**" includes (i) the *Personal Information Protection and Electronic Documents Act*, SC 2000 c. 5 ("PIPEDA"); (ii) the *Freedom of Information and Protection of Privacy Act* (Ontario) ("FIPPA"); and (iii) any other applicable law with respect to any Personal Information (as that term is defined below).
    b. **"Personal Information"** means personal information as that term is defined in PIPEDA.
    c. **"Privacy Risks"** means risks relating to privacy, including but not limited to the over-retention of Personal Information, use exceeding scope of identified purposes, collection, use, or disclosure of Personal Information for inappropriate purposes, unauthorized access, use, or disclosure of Personal Information or other privacy breaches, data breaches involving Personal Information, data and cybersecurity incidents and complaints.

2. **Requirements.** Service Provider will comply with the following when processing Personal Information in scope of this Annex:

    a. Service Provider will immediately inform Customer of any known or suspected significant Privacy Risks. Service Provider will also immediately inform Customer of any significant risks as required by FIPPA.
    b. Service Provider and Service Provider's Sub-processors will not transfer any Personal Information outside of the province of Ontario without the prior written consent of Customer, not to be unreasonably held. Any transfer outside of Ontario will not affect Service Provider's protection of Personal Information, which will at all times remain at least equivalent to those security and privacy protections as required by this DPA, the Agreement, and Data Protection Laws.

COLOMBIA DATA PROTECTION REQUIREMENTS –

1. **Definitions.** For purposes of this Annex:
   a. "**Data Protection Laws**" means Statutory Law 1581 of 2012, Decree 1074 of 2015, and any other applicable law or decrees with respect to any Personal Data (as that term is defined below).
   b. **"Personal Data**" means personal data as that term is defined in Law 1581 of 2012.
   c. **"Transfer"** shall be understood for all purposes as "Transmission" according to the definition of Law 1581 of 2012 (Controller to Processor).

2. **Requirements.** Service Provider agrees that the following apply when processing Personal Data under this Annex:
   a. **Cross-Border Transfer.** Pursuant to the DPA, Service Provider and Service Provider's Sub-processors will not transfer any Personal Data outside of Colombia without the prior written consent of Customer. If Customer consents, and if Service Provider is collecting Personal Data directly from Data Subjects, Service Provider will ensure it has provided all legally required notices and obtained all legally required consents under Data Protection Laws for such transfer.

MEXICO DATA PROTECTION REQUIREMENTS –

1. **Definitions.** For purposes of this Annex:
   a. "**Data Protection Laws**" includes Ley Federal De Protección De Datos Personales En Posesión De Los Particulares, Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, and any other applicable law with respect to any Personal Data (as that term is defined below).
   b. **"Personal Data**" means personal data as that term is defined in Ley Federal De Protección De Datos Personales En Posesión De Los Particulares.

2. **Requirements.** Service Provider will comply with the following when processing Personal Data in scope of this Annex:
   a. In addition to its obligations under Exhibit B of the DPA, Service Provider's security measures for Personal Data will at all times comply with the recommendations set out in the Recomendaciones en materia de seguridad de datos personales, approved by the Federal Institute of Access to Information and Data Protection (IFAI) (the "IFAI Requirements). Service Provider will provide evidence of its compliance with this section.

PERU DATA PROTECTION REQUIREMENTS –

1. **Definitions.** For purposes of this Annex:

    a. **"Data Protection Laws**" means Law No. 29733 on the Protection of Personal Data (*Ley No. 29733 de Protección de Datos Personales*), its Regulation approved by Supreme Decree No. 003-2013-JUS (*Decreto Supremo No. 003-2013-JUS*), and any other laws with respect to Personal Data under this Annex.

    b. **"Personal Data"** means personal data as that term is defined in Peru Data Protection Laws.

    c. **"Personal Data Database"** means an organized set of Personal Data, automated or not, regardless of medium, and regardless of the database's form or its creation, formation, storage, organization, and access of or to Personal Data.

2. **Requirements.** Service Provider will comply with the following when processing Personal Data in scope of this Annex:

    a. **Database Registration.** Service Provider will register any Personal Data Database with the National Authority for Personal Data Protection if required by Data Protection Laws.

    b. **Data Accuracy.** If the Service Provider becomes aware that the Personal Data that it has received is inaccurate or outdated, it shall inform the Customer of this without undue delay. In this case, the Service Provider shall cooperate with the Customer to delete or rectify the data.

    c. **Securities Measures.** In addition to its obligations under the DPA, the Service Provider's security measures for Personal Data will consider as good practice the recommendations set out in the "Directiva de Seguridad" approved by the National Authority for the Protection of Personal Data.

CALIFORNIA DATA PROTECTION REQUIREMENTS -

1. **Definitions.** For purposes of this Annex:

    a. "**Data Protection Laws**" means the California Consumer Privacy Act of 2018, Cal. Civil Code § 1798.100 et seq., as amended, including by the California Privacy Rights Act of 2020, and related regulations, as may be further amended from time to time (collectively, the "CCPA"), and any other applicable law with respect to any Personal Information (as that term is defined below).
    b. **"Personal Information**" means personal information as that term is defined in the CCPA.

2. **Requirements.**

a. Service Provider shall not: (a) sell or share the Personal Information (as those terms are defined in the CCPA); (b) retain, use, or disclose the Personal Information for any purpose other than the specific purpose of providing the services specified in the Agreement, including retaining, using, or disclosing the Personal Information for a commercial purpose other than providing the services specified in the Agreement, except as explicitly permitted by the CCPA; (c) retain, use, or disclose the Personal Information outside of the direct business relationship between Service Provider and Customer; and/or (d) combine the Personal Information Service Provider receives pursuant to the Agreement with Personal Information which Service Provider receives from or on behalf of another person or persons, or that Service Provider may collect from its own interaction with the consumer unrelated to this Agreement, provided that Service Provider may combine Personal Information solely if required to perform any business purpose as described in CCPA § 1798.140.
b. Service Provider certifies that it understands and will comply with its obligations under the CCPA, including without limitation by providing the same level of privacy protection as required by the CCPA.

Annex 5
Processing Details (Service Provider Personal Data)

1. Processing Purpose

Customer will only process Service Provider Personal Data only to the extent, and in such a manner, as is necessary for the Purpose as stated in Clause 12 of the DPA.

2. Categories of Data Subjects

Customer will process the Personal Data of Service Provider's potential (applicants), current, or former employees.

3. Categories of Personal Data

Customer will process the following categories of Service Provider Personal Data *(select all that apply below)*:

- ☐ Contact information (e.g., name, address, email address, phone number, etc.)
- ☐ Professional and employment information (e.g., occupation, title, income, salary, etc.)
- ☐ Account information (e.g., username, password, account metadata)
- ☐ Communications Content
- ☐ Location information
- ☐ Online identifiers (e.g., IP address, cookies, beacons)
- ☐ Device information (e.g., operating system, language preferences)
- ☐ Internet or other Online Data (e.g., browsing or search history, usage data, in-app tracking, etc.)
- ☐ Performance data (e.g., call handling statistics, quality monitoring results, etc.)
- ☐ Image and voice (e.g., recording of Data Subject's voice, image (excluding when used for biometric processing in which case this should be indicated under special category data.)
- ☐ Other (Customer to insert details):

- ☐ Special Category Data (Customer to insert details and specific categories of special category data):

Annex 6

Content of the Standard Contractual Clauses

The EU Standard Contractual Clauses (Module Two – Controller to Processor) and the UK International Data Transfer Addendum or UK Addendum are hereby incorporated into this DPA. The Parties shall abide by the terms of the EU Standard Contractual Clauses' Sections I, II, III and IV (as applicable) and the UK Addendum in the manner described in this Annex 6. The EU Standard Contractual Clauses and the UK Addendum shall apply to Service Provider in its role as "Data Importer" and to the Customer in its role as "Data Exporter" and, to the extent legally required, all of the Parties' authorized affiliates established within the European Economic Area or the UK.

The EU Standard Contractual Clauses Module 2, as set out in the DPA, will be the applicable Standard Contractual Clauses, and the following shall apply:

Clause 7 (*Docking clause*)	Clause 7 shall be incorporated
Clause 9 (*Use of sub-processors*)	General written authorization for sub-processors with 30 days' notification
Clause 11 (*Redress*)	Clause 11 shall be incorporated
Clause 13 (*Supervision: Parties to specify)*	
Clause 17 (*Governing law: Parties to specify*)	
Clause 18 (*Choice of forum and jurisdiction: Parties to specify*)	
Annex 1 A	Customer is the Data Exporter and Service Provider is the Data Importer
Annex 1B	As per Annex 1 to the DPA
Annex I C *(Competent Supervisory Authority: Parties to specify)*	
Annex II *(TOMs)*	As per Annex 3 to the DPA
Annex III *(Approved Sub-processors)*	As per Annex 2 to the DPA

The UK International Data Transfer Addendum to the EU SCCS shall apply as follows:

a. The information relevant for Table 1 is included in Annex I to the EU SCCs, Customer being the "Exporter" and Service Provider being the "Importer" of Module Two;
b. The information relevant for Table 2 is included in the applicable module of the EU SCCs;
c. The information relevant for Table 3 is included in Annex I & II to the EU SCCs; and
d. In Table 4, the Parties agree that the Exporter and the Importer may each end the UK Clauses as set out in Section 19.