DATA PROCESSING AGREEMENT (DPA)

Version 6 (International)

Effective December 2026

This data processing agreement forms part of the 'WhatConverts Terms of Use' ("Principal Contract") available at https://www.whatconverts.com/terms and is made effective from _____ between the undersigned parties:

Icon Digital LLC (DBA WhatConverts) ("Processor") By: _____ Name: _____ Title: _____ Signature Date: _____ **Address:** 3540 Toringdon Way Suite 200 #1045 Charlotte, NC 28277 United States of America	**Customer Name (Required)** ("Controller") (Full legal entity name) By: _____ Name: _____ Title: _____ Signature Date: _____ **Customer Address (Required):** _____ _____ _____

Instructions

This Agreement has been pre-signed on behalf of Icon Digital LLC (DBA WhatConverts). To enter into this Agreement, Customer must:

- Complete the table above by signing and providing the Customer's full legal entity name, address and signatory information.
- Submit the completed and signed DPA to WhatConverts via email to support@whatconverts.com.
- Customer signatory represents to Icon Digital LLC that he or she has the legal authority to bind the Customer.
- This DPA will terminate automatically upon termination of the Principal Contract.

1. Terms of Agreement

1.1. This agreement supplements the Principal Contract and makes legally binding provisions for compliance with the Data Protection Laws as set forth in this agreement. As per the requirements of relevant Data Protection Law, all processing of personal data by a processor on behalf of a controller shall be governed by a contract. The terms, obligations and rights set forth in this agreement relate directly to the data processing activities and conditions laid out in Appendix I.

1.2. The terms used in this agreement have the meanings as set out in the ‘Definitions’ part of the document.

2. Definitions

2.1. In this Agreement, unless the text specifically notes otherwise, the below words shall have the following meanings:

2.2. “Consent” of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

2.3. “Data Protection Laws” means all data protection and privacy laws applicable to the personal data processed under this DPA in any jurisdiction, including the laws specified in the Country Schedules.

2.4. “EEA” means the European Economic Area.

2.5. “Effective Date” means the date that this agreement comes into force.

2.6. “Personal Data” means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.7. “GDPR” means the General Data Protection Regulation (EU) 2016/679.

2.8. “Principal Contract” means the WhatConverts Terms of Use available at https://www.whatconverts.com/terms.

2.9. “Processing” means 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 or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.10. “Recipient” means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with applicable law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

2.11. “Third-party” means a natural or legal person, public authority, agency or body other than the data subject, Controller, Processor and persons who, under the direct authority of the Controller or Processor, are authorized to process personal data.

2.12. “Sub Processor” means any person or entity appointed by or on behalf of the Processor to process personal data on behalf of the Controller.

2.13. “Supervisory Authority” means an independent public authority with jurisdiction over the processing of personal data under applicable Data Protection Laws.

2.14. “Services” means the services provided by the Processor pursuant to the Principal Contract.

2.15. “Third Country” means a country other than the country in which the personal data was originally collected.

3. Obligations and Rights of the Processor

3.1. The Processor shall comply with the relevant Data Protection Laws as well as the following:

A. only act on the documented instructions of the Controller, unless required by applicable law to which the Processor is subject, in which case, the Processor shall to the extent permitted by such law inform the Controller of that legal requirement before the relevant Processing of that Personal Data;

B. assist the Controller in ensuring compliance with obligations regarding security of processing, notifications of personal data breaches to the corresponding supervisory authority and to the affected data subjects, data protection impact assessments and prior consultations pursuant to applicable Data Protection Laws, taking into account the nature of processing and the information available to the Processor;

C. ensure that each of its employees, agents, subcontractors or vendors authorized to process personal data is bound by a duty of confidentiality and is made aware of their obligations regarding the security and protection of the personal data and the terms set out in this agreement;

D. implement the technical and organizational security measures in accordance with applicable Data Protection Laws, for which purposes the Processor undertakes to assess potential risks arising from the data processing activities that it carries out, taking into account the means that are used to provide the services (technology, resources, etc.) and other circumstances which may have a security impact;

E. promptly notify the Controller if it receives any communication from a Data Subject or Supervisory Authority under any Data Protection Laws in respect of the Personal Data, including requests by a Data Subject to exercise rights under applicable Data Protection Laws, and assist the Controller in the Controller’s obligation to respond to these communications. The Processor shall be given reasonable time to assist the Controller with such requests in accordance with applicable law. To the extent permitted by law, the Processor reserves the right to charge the Controller a reasonable fee based on standard professional services hourly rates for time spent fulfilling custom compliance assistance or data extraction requests; provided, however, that the Processor shall not charge any fee for assistance to the extent that applicable Data Protection Laws require such assistance to be provided in connection with routine data subject or consumer requests;

F. following expiration or termination of the Principal Contract, delete or return to the Controller all Personal Data in its possession as provided in the Principal Contract (or, if sooner, the service to which it relates) except to the extent the Processor is required by applicable law to retain some or all of the personal data (in which case the Processor will implement reasonable measures to prevent the personal data from any further processing). The terms of this DPA will continue to apply to such Personal Data;

G. make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in the relevant Data Protection Laws and allow for, and contribute to,

audits, including inspections, conducted by the Controller or another auditor mandated by the Controller. Any audit conducted by the Controller shall be at the Controller's sole expense. The Controller must provide at least 30 days' prior written notice, ensure the audit takes place during standard business hours, and take all reasonable steps to minimize disruption to the Processor's daily operations. The auditor must be an independent third party that is not a competitor of the Processor and is bound by a strict non-disclosure agreement. Audits shall be limited to no more than once in any twelve (12) month period, except where an audit is required by a Supervisory Authority or follows a personal data breach affecting the Controller's Personal Data. The Processor may first satisfy an audit request by providing its most recent third-party certification and attestation reports in accordance with Appendix III, and an on-site inspection shall be required only where such reports are reasonably insufficient to demonstrate compliance;

H. inform the Controller without undue delay if the instructions received are infringing applicable Data Protection Laws;

I. in the event that the Processor becomes aware of any personal data breach involving data that the Controller has disclosed to the Processor, notify the Controller without undue delay after becoming aware of the said personal data breach. Taking into account the nature of the processing and the information available to the Processor, the Processor shall assist the Controller in ensuring compliance with the Controller's personal data breach notification obligations to the supervisory authority and data subjects under Data Protection Law;

J. where applicable, employ a Data Protection Officer if required.

3.2. Nothing within this agreement relieves the Processor of its own direct responsibilities, obligations and liabilities under applicable Data Protection Laws.

3.3. The parties acknowledge that in providing the services under this Agreement, the Processor may transfer Personal Data to a sub-processor located in a Third Country ("International Transfers"). The Customer consents to such International Transfers, provided that the Processor has ensured appropriate safeguards for the Personal Data are in place as required by applicable Data Protection Laws.

3.4. Outsourcing

3.4.1. The Controller grants general authorization to the Processor to engage other data processors for the processing of the Personal Data. Moreover, it also grants general authorization in order for such Sub Processors to also subcontract to other Sub Processors.

3.4.2. The Sub Processor(s) currently engaged in the processing of Personal Data are listed in Appendix II. When the Processor engages other companies, the Processor shall inform the Controller of any intended changes at least 30 days in advance, and such Sub Processors shall be deemed automatically included in such Appendix as of such notification, without the need to update such Appendix. If the Controller objects to a newly appointed sub-processor on reasonable data protection grounds within the 30-day notice period, the Processor will attempt to provide an alternative solution. If no alternative is commercially viable, either party may terminate the affected Services upon written notice, in which case the Processor shall refund to the Controller any prepaid fees attributable to the terminated Services for the period following the effective date of termination, and neither party shall have any further liability except for fees accrued prior to the effective date of termination.

3.4.3. When the Processor engages another data processor for carrying out specific processing activities on behalf of the Controller, the Processor is obliged to sign a sub-processing agreement subject to the terms set forth in this DPA.

3.4.4. The Sub Processor is considered a data processor and shall not process Personal Data except on instructions from the Controller and the Clauses of this DPA. The Processor shall regulate the new contractual relationship so that the same data protection obligations (instructions, security measures, duties, etc.) and the same formal requirements regarding data processing and rights and freedoms of data subjects are fulfilled by the Sub Processor.

3.5. The Processor shall maintain a record of all categories of processing activities carried out on behalf of the Controller, containing:

- the name and contact details of the Processor;
- the categories of processing carried out on behalf of each Controller;
- transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and the documentation of suitable safeguards;
- a general description of the technical and organizational security measures implemented by the Processor.

3.6. The Processor shall maintain records of processing activities in writing and electronic form and shall make the record available to the supervisory authority on request.

3.7. When assessing the appropriate level of security and the subsequent technical and organizational measures, the Processor shall consider the risks presented by any processing activities, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

3.8. The parties acknowledge that the Processor maintains an internal identity resolution index for the purpose of performing the Services, including accurate attribution and deduplication of lead records within each Controller's account. The Processor may use pseudonymized identifiers derived from Personal Data to determine whether records within the Controller's account relate to the same individual. This processing is carried out on behalf of each Controller to provide the Services and does not involve the disclosure of Personal Data originating from one Controller to any other Controller. The Processor shall not display, export, or otherwise make available to a Controller any Personal Data that did not originate from that Controller's own account. In accordance with the Principal Contract, the Controller may disable the use of its account data in the identity resolution index at any time in its account settings, and the Controller is solely responsible for determining whether its compliance obligations under applicable Data Protection Laws require disabling this feature.

4. Controller Obligations

4.1. The Customer represents, undertakes and warrants that all personal data processed by WhatConverts has been and shall be collected and processed by the Customer in accordance with Data Protection Laws and, without limitation to the foregoing, the Customer shall take all steps necessary, including without limitation providing appropriate fair collection notices and ensuring that there is a lawful basis for the Customer to process the personal data, to ensure that the processing of the personal data by WhatConverts

in accordance with this Agreement is in accordance with Data Protection Laws. Without limiting the foregoing, where required by applicable Data Protection Laws or telecommunications or wiretapping laws, the Controller is solely responsible for (a) implementing a technically effective consent mechanism that prevents the Processor's tracking technology from loading or transmitting Personal Data until required affirmative consent is obtained, and (b) providing all legally required call recording and monitoring notices and obtaining all required consents from End Users and personnel, as further set forth in the Principal Contract.

4.2. The Controller shall indemnify, defend, and hold harmless the Processor against any and all claims, liabilities, regulatory fines, and legal expenses arising directly from the Controller's failure to secure appropriate end-user consents, provide necessary privacy notices, or establish a valid lawful basis for processing personal data via the platform. The Processor shall provide the Controller with prompt written notice of any claim subject to this indemnity, permit the Controller to control the defense and settlement of such claim (provided that any settlement fully and unconditionally releases the Processor without any admission of fault or liability by the Processor), and provide reasonable cooperation in the defense at the Controller's expense.

5. Relationship with the Principal Contract

5.1. Except for the changes made by this DPA, the Principal Contract remains unchanged and in full force and effect. If there is any conflict between this DPA and the Principal Contract, this DPA shall prevail to the extent of that conflict.

5.2. Any claims brought under or in connection with this DPA shall be subject to the Terms of Use, including but not limited to, the exclusions and limitations set forth in the Principal Contract. For the avoidance of doubt, the Processor's aggregate liability arising out of or related to this DPA is subject to the limitations of liability set forth in the Principal Contract, and nothing in this DPA extends or increases those limitations. The Controller's indemnification obligations under clause 4.2 of this DPA are not subject to those limitations.

6. General Information

6.1. This DPA applies wherever the Processor processes personal data on behalf of the Customer in the course of providing the Services, where that data is subject to Data Protection Laws, regardless of the country in which the data originates.

6.2. The Controller agrees that (i) it shall comply with its obligations as a Controller under Data Protection Laws in respect of its processing of personal data and any processing instructions it issues to the Processor; and (ii) it has provided notice and obtained (or shall obtain) all consents and rights necessary under Data Protection Laws for the Processor to process personal data and provide the services pursuant to the Principal Contract and this DPA.

6.3. Both parties assume their responsibilities respectively for the use of personal data in accordance with all applicable Data Protection Laws with regard to the obligations of the Controller and the Processor.

6.4. In the fulfillment of its obligations under this DPA, the Processor shall be liable where it has failed to comply with the Controller's documented instructions or with its obligations under this DPA and applicable Data Protection Laws, subject in each case to the exclusions and limitations set forth in the Principal Contract.

6.5. No one other than a party to this DPA, its successors and permitted assignees shall have any right to enforce any of its terms.

7. International Transfers and Data Location

7.1. The Controller acknowledges that personal data is stored and processed in the United States, and by the Sub Processors listed in Appendix II in the locations listed there.

7.2. The Processor shall ensure that any onward transfer to a Sub Processor is protected by a written agreement with protections no less than those in this DPA.

7.3. If a Data Protection Law requires a specific transfer mechanism or contract terms, the parties shall cooperate in good faith to put them in place.

8. Country Schedules

8.1. Where personal data is subject to the Data Protection Laws of a country listed in Appendix IV, the terms in the relevant schedule apply in addition to this DPA and prevail in case of conflict for that data.

8.2. Where personal data is subject to the Data Protection Laws of a country that is not listed in Appendix IV, this DPA applies to that data without a country schedule. If the Controller requires additional terms to meet specific requirements of such laws, the parties shall cooperate in good faith to agree them in accordance with clause 7.3.

Appendix I – Processing Details

a. The Controller named in this agreement has appointed the Processor with regard to specific processing activity requirements. These requirements relate to provision of the Processor's platform and services.

b. The duration of the data processing under this DPA is until the termination of the Principal Contract in accordance with its terms.

c. The purpose of the data processing under this DPA is the provision of the 'WhatConverts' Services and the performance of the Processor's obligations under the Principal Contract and this DPA, including the operation of an internal identity resolution index used to match lead records relating to the same individual for the purpose of accurate attribution within the Controller's account (unless disabled by the Controller in its account settings), or as otherwise agreed by the parties.

d. The requirement for the named Processor to act on behalf of the Controller is with regard to the below type(s) of personal data and categories of data subjects:

- Controller and User data, including: identification and contact data (name, date of birth, gender, occupation or other demographic information, address, title, contact details, including email address); personal interests or preferences (including purchase history, marketing preferences and publicly available social media profile information); IT information (IP addresses, usage data, cookies data, online navigation data, location data, browser data); financial information (credit card details, account details, payment information).
- Lead and end-user communications data collected via the 'WhatConverts' platform on behalf of the Controller, including: call metadata (caller and callee numbers, call time, duration, routing information and call outcomes); call recordings; voicemail messages; call and voicemail transcriptions; SMS/MMS message content; web form submissions; chat sessions and chat transcripts; and associated marketing attribution data (such as source, medium, campaign, keyword and landing page).
- Any individual accessing and/or using the 'WhatConverts' platform through the Customer's account ("Users") and whose information is stored on or collected via the 'WhatConverts' platform.
- Any individual who contacts or interacts with the Controller through tracked communication channels provided by the platform, including telephone calls, text messages, web forms and chat ("End Users").

e. The nature of the processing includes the collection, recording, organization, structuring, storage, retrieval, consultation, use, analysis (including AI-assisted analysis, summarization and transcription carried out through the authorized Sub Processors listed in Appendix II), disclosure, restriction, erasure and destruction of personal data, and the generation and storage of pseudonymized identifiers derived from contact data for record matching, as necessary to provide the Services.

Appendix II – Authorized Sub Processors List

The Controller authorizes the engagement of the following Sub Processors in connection with the provision of the Services as of the Effective Date of this DPA. The Processor shall notify the Controller of any intended changes to this list in accordance with clause 3.4.2 of this DPA.

Sub Processor	Service / Purpose of Processing	Location
Amazon Web Services, Inc.	Cloud infrastructure, hosting and data storage	United States
Twilio Inc.	Telephony and messaging services: call tracking, call routing, call recording and SMS/MMS delivery	United States
Bandwidth Inc.	Telecommunications carrier services: phone number provisioning, voice and messaging services	United States
AssemblyAI, Inc.	Speech-to-text transcription of call recordings and voicemail messages, and AI-based analysis and summarization of lead data through AssemblyAI's LLM Gateway	United States
Anthropic, PBC	AI model provider for lead analysis and summarization, accessed through AssemblyAI's LLM Gateway; AI-assisted responses in WhatConverts support chat	United States
Datadog, Inc.	Infrastructure monitoring, log management, application performance monitoring and real user monitoring (RUM)	United States
Google LLC (Google Workspace)	Email infrastructure for support and service communications, which may contain customer platform data	United States
Zoho Corporation Pvt. Ltd. (Zoho SalesIQ and Zoho Desk)	Website live chat, visitor engagement and storage of chat transcripts; customer support ticketing	United States / India

Each Sub Processor engagement is governed by a written agreement imposing data protection obligations consistent with those set out in this DPA, in accordance with clause 3.4.3.

Appendix III

Technical and Organizational Measures Including Technical and Organizational Measures to Ensure the Security of the Data

Description of the technical and organizational security measures implemented by the Processor:

The Processor utilizes third-party data centers that maintain current ISO 27001 certifications and/or SSAE 18 SOC 1 Type II or SOC 2 Attestation Reports. The Processor will not utilize third-party data centers that do not maintain the aforementioned certifications and/or attestations, or other substantially similar or equivalent certifications and/or attestations.

Upon the Controller's written request (no more than once in any 12 month period), the Processor shall provide within a reasonable time, a copy of the most recently completed certification and/or attestation reports (to the extent that to do so does not prejudice the overall security of the Software and Services). Any audit report submitted to the Controller shall be treated as Confidential Information and subject to the confidentiality provisions of the Agreement between the parties.

The following descriptions provide an overview of the technical and organizational security measures implemented. It should be noted however that, in some circumstances, in order to protect the integrity of the security measures and in the context of data security, detailed descriptions may not be available; however additional information regarding technical and organizational measures may be found in the Security Policy. It is acknowledged and agreed that the Security Policy and the technical and organizational measures described therein will be updated and amended from time to time, at the sole discretion of the Processor. Notwithstanding the foregoing, the technical and organizational measures will not fall short of those measures described in the Security Policy in any material, detrimental way.

Entrance Control

Technical or organizational measures regarding access control, especially regarding legitimation of authorized persons: The aim of the entrance control is to prevent unauthorized people from physically accessing such data processing equipment which processes or uses Personal Data. Due to their respective security requirements, business premises and facilities are subdivided into different security zones with different access authorizations. Access to the data center is monitored by security personnel. Access for employees is only possible with an encoded ID with a photo on it. All other persons have access only after having registered before (e.g. at the main entrance). Access to special security areas for remote maintenance is additionally protected by a separate access area. The constructional and substantive security standards comply with the security requirements for data centers.

System Access Control

Technical and organizational measures regarding the user ID and authentication: The aim of the system access control is to prevent unauthorized use of data processing systems that are used for the processing of Customer Data. Authorization is executed by providing a unique username and password to a centralized directory service. All access attempts, successful and unsuccessful, are logged and monitored. Additional technical protections are in place using firewalls and proxy servers and state of the art encryption technology that is applied where appropriate to meet the protective purpose based on risk.

Data Access Control

Technical and organizational measures regarding the on-demand structure of the authorization concept, data access rights and monitoring and recording of the same: Access to data necessary for the performance of the particular task is ensured within the systems and applications by a corresponding role and authorization concept. In accordance with the “least privilege” and “need-to-know” principles, each role has only those rights which are necessary for the fulfillment of the task to be performed by the individual person. To maintain data access control, state of the art encryption technology is applied to the Personal Data itself where deemed appropriate to protect sensitive data based on risk.

Transmission Control

Technical and organizational measures regarding the transport, transfer, transmission, storage and subsequent review of Personal Data on data media (manually or electronically): Transmission control is implemented so that Personal Data cannot be read, copied, changed or deleted without authorization, during transfer or while stored on data media, and so that it can be monitored and determined as to which recipients a transfer of Personal Data is intended. The measures necessary to ensure data security during transport, transfer and transmission of Personal Data as well as any other company or Customer Data are detailed in the Security Policy. This standard includes a description of the protection required during the processing of data, from the creation of such data to deletion, including the protection of such data in accordance with the data classification level. For the purpose of transfer control, an encryption technology is used (e.g. remote access to the company network via two factor VPN tunnel and full disk encryption). The suitability of an encryption technology is measured against the protective purpose. The transfer of Personal Data to a third party (e.g. customers, sub-contractors, service providers) is only made if a corresponding contract exists, and only for the specific purposes. If Personal Data is transferred to companies located in other jurisdictions, the Processor provides that an adequate level of data protection exists at the target location or organization in accordance with applicable Data Protection Laws, e.g. by employing appropriate contractual safeguards.

Data Entry Control

Technical and organizational measures regarding recording and monitoring of the circumstances of data entry to enable retroactive review: System inputs are recorded in the form of log files, therefore it is possible to review retroactively whether and by whom Personal Data was entered, altered or deleted.

Data Processing Control

Technical and organizational measures to differentiate between the competences of principal and contractor: The aim of the data processing control is to provide that Personal Data is processed by a commissioned data processor in accordance with the instructions of the principal. Details regarding data processing control are set forth in the Agreement and DPA.

Availability Control

Technical and organizational measures regarding data backup (physical/logical): Data is stored across multiple centers in geographically different locations. The data centers can be switched in the event of flooding, earthquake, fire or other physical destruction or power outage, protecting Personal Data against accidental destruction and loss. If Personal Data is no longer required for the purposes for which it was processed, it is deleted promptly. It should be noted that with each deletion, the Personal Data is only locked in the first instance and is then deleted for good with a certain delay. This is done in order to prevent accidental deletions or possible intentional damage.

Separation Control

Technical and organizational measures regarding purposes of collection and separated processing: Personal Data used for internal purposes only, e.g. as part of the respective customer relationship, may be transferred to a third party such as a subcontractor, solely under consideration of contractual arrangements and appropriate data protection regulatory requirements. Employees are instructed to collect, process and use Personal Data only within the framework and for the purposes of their duties (e.g. service provision). At a technical level, multi-client capability includes separation of functions as well as appropriate separation of testing and production systems. Customer Data is stored in a way that logically separates it from other customer data. The Processor maintains an identity resolution index containing pseudonymized identifiers used solely for record matching. Each identity attribute within this index records the originating account, and the index does not expose any Personal Data to an account other than the one from which it originated. Where a Controller deletes a record or the Processor processes a consumer request on a Controller's behalf, the corresponding link between that account and the index is removed, and any attribute sourced solely from that account is deleted.

The Controller is assigned a unique encryption key, generated using a FIPS 140-2 compliant crypto library, which is used to encrypt and decrypt all of the Controller's archived data. In addition to the unique encryption keys, all data being written to the storage grid includes the Controller's unique account code. The Processor's systems that write data to the storage grid retrieve the encryption key from one system and the customer code from another, which serves as a cross check against two independent systems. The Controller's encryption key is further encrypted with a Processor key stored within a centralized and restricted key management system. In order for the Processor to access Customer Data via the master key, the key management system provisions individual keys following a strict process of approval that includes multiple levels of executive authorization. Use of these master encryption keys is limited to senior production engineers and all access is logged, monitored, and configured for alerting by security via a centralized Security Incident and Event Management ("SIEM") system. The Controller's archived data is encrypted at rest using AES 256 bit encryption and data in transit is protected by Transport Layer Security ("TLS").

Appendix IV – Country Schedules

Schedule A – Australia

A.1. This Schedule applies to personal information subject to the Privacy Act 1988 (Cth), including the Australian Privacy Principles ("APPs") and the Notifiable Data Breaches scheme.

A.2. The Processor shall handle such personal information in a manner consistent with the APPs, including APP 11 (security of personal information), and shall not use or disclose it except to provide the Services under the Controller's documented instructions.

A.3. On any actual or suspected unauthorized access to, disclosure of, or loss of such personal information, the Processor shall notify the Controller within the period set out in clause 3.1.I. The Processor shall provide the information reasonably needed for the Controller to assess whether an eligible data breach has occurred and to notify the Office of the Australian Information Commissioner and affected individuals.

A.4. Deletion or de-identification of such personal information follows clause 3.1.F.

Schedule B – Canada

B.1. This Schedule applies to personal information subject to the Personal Information Protection and Electronic Documents Act ("PIPEDA") or to substantially similar provincial private-sector privacy laws, including Quebec's Act respecting the protection of personal information in the private sector, Alberta's Personal Information Protection Act and British Columbia's Personal Information Protection Act.

B.2. The Processor shall use such personal information only to provide the Services under the Controller's documented instructions and shall protect it with security safeguards appropriate to its sensitivity. The parties acknowledge that the Controller remains accountable for personal information it transfers to the Processor for processing, and that this DPA constitutes the contractual means by which the Controller ensures a comparable level of protection while the information is being processed by the Processor.

B.3. On any breach of security safeguards involving such personal information, the Processor shall notify the Controller within the period set out in clause 3.1.I. The Processor shall provide the information reasonably needed for the Controller to determine whether the breach creates a real risk of significant harm, to keep the required breach records, and to notify the Office of the Privacy Commissioner of Canada, any applicable provincial regulator (including Quebec's Commission d'accès à l'information) and affected individuals.

B.4. Where such personal information is subject to Quebec law, the Controller acknowledges that it is stored and processed outside Quebec as described in clause 7.1. The Processor shall provide the information reasonably needed for the Controller to conduct any privacy impact assessment required before communicating personal information outside Quebec, and the parties agree that this DPA constitutes the written agreement required for that communication.

B.5. Deletion or de-identification of such personal information follows clause 3.1.F.

Schedule C – New Zealand

C.1. This Schedule applies to personal information subject to the Privacy Act 2020 (New Zealand), including the Information Privacy Principles ("IPPs") and the notifiable privacy breach scheme.

C.2. The parties acknowledge that the Processor holds such personal information solely as an agent of the Controller for the purpose of providing the Services, within the meaning of section 11 of the Privacy Act 2020. The Processor shall not use or disclose such personal information for its own purposes, shall act only on the Controller's documented instructions, and shall protect it with security safeguards consistent with IPP 5. Onward transfers to Sub Processors are governed by clause 7.2.

C.3. On any actual or suspected privacy breach involving such personal information, the Processor shall notify the Controller within the period set out in clause 3.1.I. The Processor shall provide the information reasonably needed for the Controller to assess whether a notifiable privacy breach has occurred and to notify the Office of the Privacy Commissioner and affected individuals.

C.4. Deletion of such personal information follows clause 3.1.F.