DATA PROCESSING ADDENDUM

PIPEDA-Compliant Data Processing Framework | Effective: February 9, 2026 | Version 3.0

1. PURPOSE AND SCOPE

This Data Processing Addendum ("DPA") supplements the Authentic Journey Service Agreement and Privacy Policy. It provides detailed information about how Authentic Journey processes personal information on behalf of its clients in compliance with the Personal Information Protection and Electronic Documents Act (PIPEDA) and other applicable Canadian privacy laws.

Data Controller: The Client (business subscribing to Authentic Journey services)

Data Processor: 17635966 Canada Inc. (operating as Authentic Journey)

This DPA applies to all personal information processed by Authentic Journey when providing AI receptionist services, including call recordings, caller contact information, and transcripts.

2. DEFINITIONS

Personal Information: Any information about an identifiable individual as defined under PIPEDA, including caller names, phone numbers, email addresses, call recordings, call transcripts, and any other data that directly or indirectly identifies a natural person.

Anonymized Data: Personal Information that has been irreversibly processed in accordance with the Office of the Privacy Commissioner of Canada's de-identification standards, such that there is no reasonable basis to believe it could be used to identify an individual.

Processing: Any operation or set of operations performed on Personal Information, including collection, recording, storage, retrieval, use, disclosure, or destruction.

Sub-Processor: Any third party engaged by Authentic Journey to process Personal Information on behalf of a Client.

Data Subject: The natural person to whom Personal Information relates — including callers, client contact persons, and website visitors.

Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information.

3. TYPES OF PERSONAL INFORMATION PROCESSED

3.1 Caller Identity Information

- Full name (as provided during the call)
- Phone number (Caller ID)
- Email address (if provided)
- Business name or company affiliation (if provided)
- City/province (derived from phone number or disclosed by caller)

3.2 Call Content

- Audio recordings of phone conversations
- Transcripts (text versions of conversations)
- Information voluntarily disclosed during calls (contact preferences, service inquiries, appointment requests)

3.3 Call Metadata

- Date, time, and duration of call
- Phone number called (client's business line)
- Call routing information and outcome

> **Note on Sensitive Information**
>
> Callers may voluntarily disclose sensitive personal information during calls, including health information, financial information, family information, and employment information. Clients are responsible for ensuring appropriate consents and safeguards are in place where their business involves the collection of sensitive personal information.

4. PURPOSES OF PROCESSING

4.1 Primary Purpose — Service Delivery

- Answer incoming calls to client's business phone number
- Collect caller contact and intake information
- Schedule callback appointments on behalf of clients
- Route calls to appropriate contacts

4.2 Secondary Purposes

- Quality Assurance — monitor AI agent performance and accuracy
- Service Improvement — identify areas for AI training and enhancement
- Client Reporting — provide call summaries, analytics, and performance metrics
- Compliance — meet legal and regulatory obligations

4.3 AI Model Training

Anonymized data may be used to improve AI models. Authentic Journey applies Office of the Privacy Commissioner of Canada de-identification standards before any data is used for this purpose. General clients may opt out by emailing support@authentic-journey.com.

> **Insurance Clients — Absolute Prohibition**
>
> For clients who have executed the Insurance Industry Client Addendum, no data from their AI deployments — whether personally identifiable or anonymized — will be used for AI model training under any circumstances. This prohibition applies without requiring an opt-out request.

5. SUB-PROCESSORS

5.1 Current Sub-Processors

- GrowthHub365 (United States) — AI platform and phone system infrastructure
- OpenAI / Anthropic (United States) — AI language processing
- Zoho Mail (India / United States) — email services
- Stripe / Square (United States) — payment processing

5.2 Sub-Processor Obligations

All sub-processors must: comply with PIPEDA and applicable data protection laws; implement security measures equivalent to those described in this DPA; use personal information only to provide services to Authentic Journey; delete or return data upon termination; and notify Authentic Journey of any data breaches within 24 hours of discovery.

5.3 Sub-Processor Changes

Authentic Journey will notify clients at least 30 days in advance of engaging new sub-processors or making material changes to existing arrangements. Clients may object within 30 days of notice. If Authentic Journey cannot accommodate the objection, either party may terminate the Service Agreement without penalty.

6. SECURITY MEASURES

6.1 Technical Safeguards

- Encryption in transit (TLS 1.2 or higher) for all data transmitted over networks
- Encryption at rest (AES-256) for all stored call recordings and transcripts
- Encrypted backups stored in geographically separate locations
- Multi-Factor Authentication (MFA) required for all administrative access
- Role-Based Access Control (RBAC) limiting access to data necessary for each role
- Audit logs of all access to personal information
- Firewalls, intrusion detection systems, and secure API endpoints
- Regular vulnerability scanning and penetration testing

6.2 Organizational Safeguards

- Privacy and security training for all employees upon hiring and annually thereafter
- Confidentiality agreements signed by all employees, contractors, and sub-processors
- Need-to-know access principle with regular permission reviews
- Documented and tested incident response procedures

6.3 Physical Safeguards

Personal information is stored in SOC 2 certified data centres with 24/7 physical security monitoring, restricted access, biometric controls, and environmental controls.

7. DATA BREACH PROCEDURES

7.1 Detection and Assessment

Upon detecting a suspected breach, Authentic Journey will assess scope, nature, and potential impact within 24 hours; implement containment measures; and conduct a detailed investigation to identify cause and affected data.

7.2 Notification Obligations

Notification to Clients: Authentic Journey will notify affected clients within 72 hours of confirming a data breach by email, including: (a) the nature of the breach; (b) categories of Personal Information affected; (c) approximate number of Data Subjects affected; (d) steps taken to address the breach; and (e) a contact for follow-up questions.

Notification to Individuals: Where a breach poses a real risk of significant harm to affected individuals under PIPEDA, Authentic Journey will notify affected Data Subjects directly as soon as reasonably practicable.

Notification to Authorities: Authentic Journey will report data breaches that pose a real risk of significant harm to the Office of the Privacy Commissioner of Canada as required by PIPEDA. Clients who are independently regulated remain responsible for any additional breach reporting obligations to their own regulators.

8. DATA SUBJECT RIGHTS

Under PIPEDA, Data Subjects have the following rights: Right to Access; Right to Correction; Right to Deletion; Right to Withdraw Consent; and Right to File Complaints with the Privacy Commissioner of Canada.

Clients (as Data Controllers) are primarily responsible for responding to data subject rights requests. Authentic Journey will forward requests received directly to the relevant client within 2 business days and provide requested personal information in usable format within 10 business days.

9. CROSS-BORDER DATA TRANSFERS

9.1 Transfer Locations

- United States — GrowthHub365, OpenAI / Anthropic, Stripe / Square
- India / United States — Zoho Mail

9.2 Consent Mechanism

To ensure meaningful consent for cross-border transfers as required by PIPEDA, the AI receptionist delivers a mandatory disclosure at the start of every call before collecting personal information, informing callers that information may be processed by service providers outside Canada, including in the United States.

9.3 Safeguards

- All international sub-processors are bound by contracts requiring PIPEDA-equivalent data protection
- Encryption in transit (TLS 1.2+) and at rest (AES-256) for all cross-border transfers
- Regular audits of sub-processors' data protection practices

10. DATA RETENTION AND DELETION

10.1 Retention Periods

- Call Recordings and Transcripts (General Clients) — 90 days default; configurable between 30 days and 12 months
- Call Recordings and Transcripts (Insurance Clients) — up to 7 years where extended retention is elected to meet regulatory requirements
- Client Account Information — duration of service agreement, then 7 years for tax and legal compliance
- Anonymized Analytics — may be retained indefinitely for service improvement

10.2 Deletion Upon Request

- Client-initiated deletion within 30 days of request
- End of Service Agreement deletion within 30 days unless export is requested or legally required retention applies

10.3 Certification of Deletion

Upon request, Authentic Journey will provide written certification that personal information has been securely deleted.

11. CLIENT OBLIGATIONS AS DATA CONTROLLER

- Ensure a lawful basis for processing personal information through Authentic Journey services
- Obtain necessary consents from callers and comply with PIPEDA and applicable privacy laws
- Provide accurate business information for the AI knowledge base
- Use caller information only for legitimate business purposes consistent with the purpose of the call
- Implement appropriate security measures to protect caller information received from Authentic Journey
- Respond to data subject rights requests within PIPEDA timelines (30 days)

12. LIABILITY AND INDEMNIFICATION

Authentic Journey is liable for:

- Breaches of this DPA caused by Authentic Journey's negligence or willful misconduct
- Failure to implement the security measures specified in Section 6
- Failure to deliver the mandatory AI disclosure
- Unauthorized disclosure of client personal information by Authentic Journey's employees or agents

Clients are liable for:

- Providing inaccurate or misleading business information for the AI knowledge base
- Unlawful or unauthorized processing instructions given to Authentic Journey
- Failure to comply with PIPEDA and applicable industry-specific privacy legislation

- Regulatory violations resulting from the client's own business practices

13. GOVERNING LAW

This DPA is governed by the laws of the Province of Ontario, Canada and is subject to PIPEDA and other applicable Canadian privacy laws.

14. PRIVACY OFFICER CONTACT

Primary Privacy Officer: Allistair Joseph, Founder & CEO

Phone: 1-888-218-5642 **|** Email: allistair@authentic-journey.com

15-75 Bayly St W, #1029, Ajax, ON L1S 7K7, Canada **|** https://authentic-journey.com