

Customer Data Processing Addendum - JamayaAI

Customer Data Processing Addendum (DPA) - JamayaAI

This Customer Data Processing Addendum ("Addendum"), including its Exhibits and Appendices, is entered into between MetasSV SAS de CV, an El Salvador corporation doing business as JamayaAI.com ("JamayaAI" or "Processor"), and the business entity utilizing the services ("Client" or "Controller").

This Addendum is incorporated by reference into, and forms part of, the JamayaAI.com Terms of Service (effective May 1, 2026). In the event of any conflict or inconsistency between this Addendum and the Terms of Service regarding the processing of Personal Data, the terms of this Addendum shall take precedence. For the avoidance of doubt, the Standard Contractual Clauses (SCCs) shall prevail over any other terms of this Addendum in the context of Restricted Transfers.

1. Definitions

- **Applicable Data Protection Laws:** Means all laws and regulations applicable to the Processing of Customer Personal Data, including but not limited to the GDPR (EU and UK), the Australian Privacy Act, the Brazilian LGPD, the Canadian PIPEDA, and United States Data Protection Laws (including CCPA/CPRA and various state privacy acts), and the laws of El Salvador.
- **Contracted Processor:** Means any third party appointed by or on behalf of JamayaAI to process Customer Personal Data in connection with the Services (this includes "Sub-processors").
- **Customer Personal Data:** Means Personal Data contained within data that JamayaAI processes on behalf of the Client to provide the Services. Customer Personal Data does not include the Client's Account Information (such as billing details, account credentials, or administrative contact info).
- **Personal Data Breach:** Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data.
- **Services:** Means the "AI Employee Team" tech stack and automated software infrastructure provided by JamayaAI, including automated marketing, sales, and administrative software, as described in the Agreement.
- **Controller, Processor, Data Subject, and Processing:** Shall have the meanings assigned to them under the GDPR and other Applicable Data Protection Laws.

2. Scope and Role of Parties

The parties acknowledge and agree that MetasSV SAS de CV acts as the Processor (or Sub-processor, where Client acts as a Processor for its own customers) and the Client acts as the Controller.

- **Duration:** The processing shall continue concurrently for the duration that Personal Data is processed by JamayaAI pursuant to the Terms of Service, subject to the retention provisions in Section 9.
- **Instructions:** JamayaAI shall only process Customer Personal Data on the documented instructions of the Client. These instructions specifically include the provision of AI-driven marketing, sales, and administrative automation. JamayaAI shall immediately inform the Client if an instruction, in its opinion, infringes Applicable Data Protection Laws.

3. Processor Obligations and Personnel

JamayaAI shall:

- Comply with all Applicable Data Protection Laws in the processing of Customer Personal Data.
- Ensure that all personnel authorized to process Customer Personal Data are subject to formal confidentiality undertakings or professional/statutory obligations of confidentiality.
- Limit access to Customer Personal Data to those individuals who require such access to fulfill the instructions of the Client or to comply with legal obligations.

4. Contracted Processors (Sub-processing)

The Client grants general authorization for JamayaAI to engage Contracted Processors.

- Authorized Processors: The Client acknowledges and authorizes the use of Amazon Web Services (AWS) and GoogleCloud as existing contracted processors.
- Notification of Changes: JamayaAI shall notify the Client of any new Contracted Processors via its website or direct notification.
- Right to Object: The Client may object to the appointment of a new Contracted Processor within thirty (30) days of notification. If an objection is raised, the parties will work in good faith to reach a resolution. If no resolution is found, the Client may terminate the Agreement without further fees other than those accrued to the date of termination.

5. Data Subject Rights and Cooperation

Taking into account the nature of the processing, JamayaAI shall implement appropriate technical and organizational measures to assist the Client in responding to requests from Data Subjects exercising their rights (e.g., access, deletion, portability).

- If JamayaAI receives a request directly from a Data Subject, it shall notify the Client within a reasonable timeframe and shall not respond to the request except on the documented instructions of the Client or as required by law.

6. Personal Data Breach Notification

JamayaAI shall notify the Client without undue delay, and in any event within 72 hours, after becoming aware of a Personal Data Breach. The notification shall include:

- The nature of the breach and affected categories/numbers of data and Data Subjects.
- The measures taken or proposed to address the breach and mitigate its effects.
- Supplemental notifications as additional information becomes available.

7. Security of Processing

JamayaAI has implemented and shall maintain appropriate technical and organizational measures (TOMs) as detailed in Exhibit B. These include, but are not limited to:

- Encryption: Use of AES-256 CBC for data at rest and TLS 1.2+ for data in transit.
- Certifications: JamayaAI maintains a HIPAA Seal of Compliance Certificate issued by The Compliancy Group.

8. Data Retention and Deletion

- Retention Period: Customer Personal Data shall be retained for 90 days post-termination of the Services.
- Deletion: Following the 90-day period, JamayaAI shall permanently delete all Customer Personal Data (including copies and those held by Contracted Processors) unless applicable law requires further storage. Data in back-up systems shall be securely isolated and protected from further processing.

9. Regulatory Compliance and International Transfers

- TCPA and CAN-SPAM: The Client is the sole designated sender and "advertiser" for all legal purposes under the Telephone Consumer Protection Act (TCPA) and the CAN-SPAM Act. The Client is responsible for obtaining "one-to-one" express written consent.
- International Transfers: JamayaAI transfers data internationally to provide its Services.
 - Data Privacy Framework (DPF): JamayaAI relies on infrastructure providers certified under the EU-U.S. Data Privacy Framework (DPF), the UK Extension, and the Swiss-U.S. DPF as the primary mechanism for transfers from the EEA, UK, and Switzerland.
 - SCCs: Where the DPF does not apply, the parties incorporate the Standard Contractual Clauses (Module Two: Controller-to-Processor or Module Three: Processor-to-Processor, as applicable) as a fallback mechanism.
- Jurisdictional Specifics: The processing will comply with jurisdictional annexes (Australia, Brazil, Canada, and US State Laws) as specified in Exhibit B of the HighLevel template.

10. Limitation of Liability

The total aggregate liability of JamayaAI for any claim arising out of data processing activities under this Addendum is subject to the liability cap defined in the Terms of Service, limited to the amount paid by the Client in the single month in which the incident occurred.

11. Governing Law and Jurisdiction

This Addendum is governed by the laws of El Salvador. Any disputes arising herefrom shall be resolved exclusively via binding international arbitration under the rules of the International Chamber of Commerce (ICC) held in El Salvador.

Exhibit A: Details of Processing

AI Employee Team Processing Roles

AI Employee Role	Data Processing Activity
AI Online Super Manager	Overseeing all digital activities; managing data coordination across integrated systems.
AI Chatbox / Avatar	Interacting with leads to demonstrate products; capturing lead identifiers via chat.
AI Viral Idea Finder	Searching public web data for content trends; processing external viral metadata.
AI Video Creator	Designing marketing assets/videos based on specific content and lead profiles.
Social Media Poster	Automating the posting of marketing content to social networks.
AI Scrape Manager	Scraping leads from external websites or directories every day to generate new data sets.
AI Google Sheet Manager	Extracting lead data from forms and tracking it in Google Sheets for CRM management.
AI Calendar Manager	Managing appointment cycles: booking, confirming, and rescheduling.
AI Online Sales Assistant	Processing orders, managing payments, invoices, and client onboarding.
AI Email Manager	Classifying, summarizing, drafting, sending, and forwarding business emails.
AI Telephone Super Agent	Coordination and processing of all voice-based data activities.
AI Phone Salesperson	Calling leads tracked on Google Sheets in under 60 seconds; processing automated sales audio.
AI Phone Receptionist	Answering inquiries via voice; managing FAQs and location-based data.
AI Phone Sales Assistant	Voice-based order processing, payment management, and client onboarding.
AI Documents Manager	Managing files, sales documents, and RAG (Retrieval-Augmented Generation) system databases.
AI Admin Assistant	Generating company financial reports, statistical reports, and business analysis.

- Categories of Data Subjects: Leads, Customers, and Client Employees.
- Categories of Personal Data: Names, Email Addresses, Phone Numbers, Voice/Audio Recordings, Professional/Business Information, and IP Addresses.

Exhibit B: Technical and Organizational Security Measures (TOMs)

JamayaAI maintains the following security measures to safeguard Customer Personal Data:

- Data Encryption: All personal data at rest is encrypted using AES-256 CBC. All personal data in transit is encrypted using TLS 1.2+ and HTTPS with valid SSL certificates.
- Assurance and Certification: JamayaAI has been issued a HIPAA Seal of Compliance Certificate by The Compliancy Group, ensuring healthcare-grade administrative and technical safeguards.
- Access Control: Strict implementation of Role-Based Access Control (RBAC) and subaccount-based authentication. Use of encrypted signed tokens for session management.

- Availability and Resilience: Data is backed up via AWS and GoogleCloud with five-minute granularity, allowing for rapid restoration and ensuring high availability.
- Audit and Testing: Annual third-party penetration testing and continuous third-party vulnerability scans of all externally facing infrastructure. Maintenance of a standard patch management process.
- Physical Security: Reliance on Tier-1 managed services (AWS and GoogleCloud) for the physical security of data centers, including biometric access and environmental controls.
- Logging and Monitoring: Comprehensive logging of all user actions and audit trails. Infrastructure and application monitoring is conducted via GoogleCloud Ops and AWS Cloudwatch.
- Governance: Maintenance of an in-house IT Security team supplemented by a third-party Managed Security Service Provider (MSSP) for 24/7 SOC monitoring.