TEJMA

Data Processing Agreement

TEJMA LLC · TEJMA DISPATCHER · DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") forms part of the Terms of Service between Tejma LLC ("Tejma", the "Processor") and the customer organization using **Tejma Dispatcher** (the "Customer", the "Controller"). It applies whenever Tejma processes personal data contained in Customer Content on the Customer's behalf and is subject to data protection law such as the GDPR, the UK GDPR, or the California Consumer Privacy Act. It is incorporated into the Terms of Service; no signature is required, though Tejma will countersign a copy on request.

Effective August 31, 2026 · Last updated August 31, 2026 · Reno, Nevada

1. Roles and Scope

Customer is the controller; Tejma is the processor. The Customer decides which channels to connect, which agents to run, and what those agents do; Tejma processes the resulting Customer Content only to provide the service. Where the CCPA applies, Tejma is the Customer's "service provider" and does not sell or share personal information, retain it except to provide the service, or combine it across customers.

Precedence. For personal data processing, this DPA prevails over any conflicting term of the Terms of Service. Everything else — including the limitation of liability, which applies to this DPA in aggregate with the Terms — remains governed by the Terms of Service.

2. Details of the Processing

Subject matter and nature. Ingestion, storage, task extraction, task routing, AI-assisted task execution, and Customer-directed outbound messaging of communications flowing through channels the Customer connects (email mailboxes, Slack channels, Discord channels) and content submitted through the Customer's MCP clients and API calls.

Duration. The term of the Customer's subscription, plus the post-termination export and deletion window in Section 9.

Categories of data subjects. The Customer's personnel (organization members), and the people who correspond with the Customer through connected channels — email senders and recipients, chat-workspace participants, and persons referenced in messages, attachments, and tasks.

Categories of personal data. Names, email addresses, and chat handles; message and thread content and any personal data those messages, attachments, and files happen to contain (which the Customer, not Tejma, determines); task content derived from them; and organization-member account and billing data. The service is not designed for, and the Customer agrees not to direct to it, special-category data or data subject to sector rules (such as HIPAA or PCI card data) absent a separate written agreement.

3. Processing on Documented Instructions

Tejma processes Customer Content only on the Customer's documented instructions: this DPA, the Terms of Service, the Customer's configuration of the service (connected channels, agents, skills, connectors, approvals), and the Customer's use of its API — unless processing is required by law, in which case Tejma will inform the Customer before processing where the law allows. Tejma will inform the Customer if, in its opinion, an instruction infringes data protection law.

4. Confidentiality and Personnel

Persons Tejma authorizes to process Customer Content are bound by confidentiality obligations and access Customer Content only as needed to operate, secure, and support the service.

5. Security Measures

Tejma implements technical and organizational measures appropriate to the risk, including:

- **Tenant isolation.** Every message, task, document, connector, and channel record belongs to exactly one user; requests for another tenant's identifiers behave as if the record does not exist, and stored files are keyed per user.
- **Encryption.** TLS for data in transit; AES-256-GCM encryption at rest for stored secrets (channel and connector authorization tokens, Anthropic API keys), which are write-only and decrypted solely at the moment of use.
- **Authenticated ingress.** OAuth 2.0 bearer tokens verified as JWTs against the identity provider on every API and MCP request; cryptographic signature verification on every inbound webhook (Nylas, Slack, Stripe) before any processing.
- **Access control.** Role-gated administration: billing, member management, and credential rotation are restricted to organization admin roles; the operator's billing controls sit behind a separate, dedicated identity tenant.
- **Payment isolation.** Card data is entered only on Stripe's hosted pages and never reaches Tejma's systems.
- **Operational integrity.** Idempotent, at-least-once ingestion with verified redelivery; billing events journaled in append-only ledgers within the same transaction as the balance they change.

6. Subprocessors

General authorization. The Customer authorizes the subprocessors below. Tejma will give admins at least 30 days' notice before adding or replacing a subprocessor; the Customer may object on reasonable data-protection grounds, and if the objection cannot be resolved, may terminate the affected service with a prorated refund of prepaid, unused fees.

Current subprocessors — each engaged under a written agreement imposing data-protection obligations no less protective than this DPA

- **WorkOS, Inc.** (US) — authentication, sessions, organization and member management.
- **Anthropic, PBC** (US) — AI processing of message and task content; calls are made under the Customer's own Anthropic API key, so Anthropic also acts under its direct commercial terms with the Customer.
- **Nylas, Inc.** (US; EU region available) — email mailbox connectivity, message sync, attachment retrieval.
- **Slack Technologies / Salesforce, Inc.** (US) — receiving and sending messages in connected Slack channels.
- **Discord Inc.** (US) — receiving and sending messages in connected Discord channels.
- **Stripe, Inc.** (US) — payment processing and recurring subscription billing.
- **Railway Corp.** (US) — cloud hosting: compute and the Postgres database holding messages, tasks, and account data.
- **Cloudflare, Inc.** (US) — R2 object storage holding message documents and attachments.

MCP connector servers the Customer registers, and the channels' own providers in their capacity as the Customer's communication services, are engaged by the Customer directly and are not Tejma subprocessors.

Tejma remains responsible to the Customer for its subprocessors' performance under this DPA.

7. Assistance to the Controller

Data subject requests. Taking into account the nature of the processing, Tejma will assist the Customer with data subject requests (access, rectification, erasure, restriction, portability, objection) through the service's built-in controls — per-document and per-task deletion, channel disconnection, per-user storage keys enabling bulk deletion, and export on request — and with reasonable further assistance where the built-in controls do not suffice. Requests Tejma receives directly from data subjects about Customer Content will be forwarded to the Customer without undue delay.

DPIAs and consultations. Tejma will provide reasonable assistance with data protection impact assessments and prior consultations with supervisory authorities, insofar as they concern processing by the service.

8. Personal Data Breach

Tejma will notify the Customer's organization admins without undue delay after becoming aware of a personal data breach affecting Customer Content, and in any event within 72 hours, providing what is known at the time — the nature of the breach, categories and approximate volumes affected, likely consequences, and measures taken — and supplementing as facts develop. Tejma will not characterize the Customer's own notification obligations; notification is not an admission of fault.

9. Deletion and Return

During the term, the Customer deletes Customer Content directly through the service, and deletion of a document removes its stored bytes before its record. Upon termination of the subscription, Tejma will honor export requests for 30 days and then delete Customer Content, including stored documents and encrypted credentials, except where law requires retention (billing and tax records are retained for their statutory periods) and except for backups, which age out on a fixed schedule and are protected until they do.

10. International Transfers

Tejma processes Customer Content in the United States. Where personal data protected by the GDPR or UK GDPR is transferred to Tejma or its subprocessors outside the EEA or UK, the parties rely on the EU Standard Contractual Clauses (Module 2, controller-to-processor), which are incorporated by reference with the Customer as data exporter and Tejma as data importer, supplemented by the UK International Data Transfer Addendum where the UK GDPR applies, and on the subprocessors' own transfer safeguards. The processing details in Section 2 complete the Clauses' annexes.

11. Audits and Information

Tejma will make available the information reasonably necessary to demonstrate compliance with this DPA — security documentation, subprocessor agreements' data-protection terms, and answers to reasonable security questionnaires — and will allow audits required of the Customer by a supervisory authority, on at least 30 days' notice, at most annually absent a breach, during business hours, under confidentiality, and at the Customer's expense.

TEJMA

Contact. Privacy and data protection matters: Tejma LLC · Reno, Nevada · ai.assistants@tejmallc.com · tejmallc.com

Matej Meciar · Tejma LLC
925-963-4257 · ai.assistants@tejmallc.com · tejmallc.com