emellow

Security & Data Handling Whitepaper

Version 1.0 | March 2026

This document is intended for emellow users and prospective customers.

Introduction

At emellow, we believe you should know exactly what happens to your email data when you use our service. This document explains, in plain terms, how your email is accessed, what we process, what we store, and how we protect your information.

emellow connects to your Gmail inbox to automatically identify actionable items — tasks, follow-ups, commitments — and surfaces them as todos. We do this by reading incoming email on your behalf, running it through an AI model to extract relevant action items, and then presenting those todos to you in the emellow interface.

The short version: We read your email to find your todos. We never store your email. No human at emellow ever sees your email content. Ever.

Email Access

emellow connects to your Gmail account using Google's official OAuth 2.0 authorization flow. When you connect your inbox, Google presents you with a permissions screen showing exactly what access you are granting.

Read-Only Access

emellow requests read-only Gmail access — enforced at the Google API level, not just our policy. This means we cannot send email, delete email, move email, or modify your inbox in any way. If you are ever uncertain about what emellow can access, you can review and revoke permissions directly from your Google Account security settings at any time.

OAuth Token Security

The OAuth tokens that allow us to read your inbox are protected as follows:

- Encrypted at rest using AES-256 before being stored in our systems
- Transmitted exclusively over TLS 1.2 or higher — never sent in plaintext

- Scoped strictly to read-only Gmail access at the Google API level
- Revocable at any time from your Google Account at myaccount.google.com/permissions, independent of your emellow account

emellow is not affiliated with or endorsed by Google. Google's own privacy policy governs how Google handles your data on their infrastructure.

No Human Ever Reads Your Email

No emellow employee, contractor, or affiliate reads your email. Ever.

When a message arrives, it is fetched programmatically and passed directly to an AI model for processing. The email exists in memory only for the duration of that processing — it is never written to disk, never logged, never stored in a database, and never seen by a person.

Once the AI extracts your todos, the email content is gone. The only thing that ever "sees" your email is the AI model — and it has no memory, no curiosity, and no agenda beyond completing the extraction task it was given.

Infrastructure Access Controls

Access to emellow's production infrastructure is tightly controlled:

- All production access is conducted exclusively through AWS Systems Manager (SSM) Session Manager — no direct SSH access is permitted and no SSH keys are distributed
- SSM sessions are fully logged and audited, including session start/end times and command transcripts, shipped to CloudWatch
- All AWS API activity is recorded via AWS CloudTrail, providing a complete audit trail of infrastructure changes
- Access is restricted to authorized personnel only

In practical terms, this means there is no mechanism by which a person could casually or accidentally read your email — access to the systems that process it requires deliberate, logged, audited action.

The Data Lifecycle: What We Read vs. What We Keep

Here is exactly what happens when an email arrives in your connected inbox:

1	Email is fetched from your Gmail inbox via the Gmail API (read-only)

2	Email content is passed to our AI model (Claude, by Anthropic) for todo extraction
3	Extracted todos are saved to your emellow account
4	The original email content is discarded — not stored, not logged, not retained

What We Store

- Extracted todo items and their metadata (title, due date, priority, source inbox)
- Your account information (email address, display name, preferences)
- Inbox configuration and connection settings
- Encrypted OAuth tokens for Gmail access
- Processing and error logs (7-day rolling window, no email body content)

What We Do Not Store

- Email bodies or subjects
- Email attachments
- A copy or mirror of your inbox
- Sender or recipient contact information beyond what appears in an extracted todo
- Any email metadata not captured in your extracted todos

AI Processing: How Claude Handles Your Email

emellow uses Claude, developed by Anthropic, as the AI model that reads your emails and extracts todos. We access Claude exclusively through Anthropic's commercial API.

What Gets Sent to Claude

When an email arrives, its text content (subject and body) is sent to Claude for processing. Claude returns the extracted todos and the email content is not retained by emellow or Anthropic.

Anthropic Does Not Train on Your Data

This is important, and it is worth being explicit:

> Because emellow uses the Anthropic commercial API, your email content is **categorically excluded** from AI model training — by Anthropic's own API terms.

The training policy changes Anthropic announced for consumer Claude accounts in 2025 do **not apply** to API usage. We are governed by separate commercial terms that explicitly prohibit data training on API inputs.

Additionally, Anthropic's API retains request data for only 7 days before automatic deletion — meaning even the transient processing window is short. Your email content is not persisted on Anthropic's infrastructure beyond what is needed to fulfill the immediate request.

We selected Anthropic specifically because of these commitments. We do not use any AI provider that trains on customer data submitted through their API.

You can review Anthropic's API data usage policy at anthropic.com/legal/privacy.

Infrastructure & Security

emellow is hosted on Amazon Web Services (AWS) infrastructure in the United States.

Encryption

- All data in transit is encrypted via TLS 1.2 or higher
- All data at rest is encrypted using AES-256
- OAuth tokens are encrypted before storage using AES-256
- Encryption keys are managed and rotated following AWS best practices

Infrastructure Components

- Application servers: AWS EC2 / AWS Fargate (container-based)
- Database: MongoDB Atlas — encrypted at rest, network-isolated, access-controlled
- Queue processing: Redis + BullMQ for reliable, async email processing
- All components operate within private AWS network boundaries
- No public-facing database or queue endpoints

Data Retention Summary

Data Type	Retention Period

Email content (body, subject, attachments)	Not retained — discarded after AI processing
Extracted todo items	Until you delete them or close your account
Account & inbox configuration	Retained for the life of your account
OAuth access tokens	Encrypted at rest; revoked on disconnect
Processing / error logs	7 days rolling
Billing records	As required by law (typically 7 years)

Your Rights & Controls

You are in control of your data at all times.

- Delete todos at any time from within the emellow app
- Disconnect your Gmail inbox at any time — this immediately revokes our API access and we will delete your stored OAuth token
- Request account deletion by contacting us — we will delete all stored account data within 30 days
- Request a copy of your data — we will provide an export of all data associated with your account
- GDPR / CCPA: If you are located in the EU or California, you have additional rights regarding your personal data. Contact hello@emellow.io to exercise these rights.

What We Will Never Do

- Sell your data or email content to any third party
- Use your email content to train AI models
- Read your email for any purpose other than extracting the todos you asked us to find
- Share your data with advertisers
- Allow any employee or contractor to read your email
- Store your email content beyond the duration of a single processing request

Contact & Transparency

We are a small, focused team and we take data handling seriously. If you have questions about how your data is handled, want to report a security concern, or need to exercise any privacy rights, reach out to us at:

hello@emellow.io

We commit to responding to security reports within 48 hours and privacy requests within 30 days.

Last updated: March 2026. This document will be updated when our data handling practices change in any material way. Significant changes will be communicated to active users via email.