Data Processing Agreement (DPA)

Between Customer ("Controller") and MailMCP ("Processor")

Version : 1.2 **Effective from :** 2026-10-17 (v1.1 : 2026-10-14, v1.0 : 2026-05-26) **Reference :** GDPR Articles 28, 32, 33

---

1. Parties

Processor : STAY WEB (SASU, operating MailMCP) 59 rue de Ponthieu, bureau 326, 75008 Paris, France DPO contact : privacy@mailmcp.io

Controller : The natural or legal person who has created a MailMCP account or signed this DPA. Identified by the email address and company name registered on the MailMCP account.

By creating a MailMCP account and accepting our Terms of Service, the Controller agrees to this DPA. A PDF copy signed by the Processor can be downloaded at https://mailmcp.io/legal/dpa.

---

2. Subject matter and duration

Element	Detail
Subject matter	The provision of the MailMCP SaaS — connecting IMAP/SMTP mailboxes to AI assistants via the Model Context Protocol (MCP).
Duration	This DPA applies for the entire duration of the Controller's MailMCP account, plus a 30-day grace period after termination.
Termination	Automatic upon account deletion. The Controller may terminate this DPA at any time by deleting their account from the dashboard.
Post-termination	Within 30 days of termination, the Processor deletes all personal data of the Controller's data subjects (see §10).

---

3. Nature and purpose of processing

The Processor processes personal data **only on documented instructions from the Controller** (GDPR Art. 28.3.a), namely:

- Storing the Controller's mailbox credentials (IMAP/SMTP user, password — encrypted at rest with AES-256) to allow authorized AI agents to access the mailbox.
- Forwarding requests from AI clients (Claude, ChatGPT, Cursor, etc.) to the Controller's IMAP/SMTP server via the MCP protocol.
- Logging metadata about MCP calls (tool name, IP address, timestamp) for security, abuse prevention, and quota enforcement.

- Optionally invoking generative AI models on behalf of the Controller for : outreach pitch generation and the email signature generator.

The Processor does **not** :

- Read, store, copy, index, or analyze email content beyond what is strictly required to forward an MCP tool call to the Controller's IMAP/SMTP server.
- Use Controller's data for marketing, profiling, advertising, or model training (own or third-party).
- Sell, rent, lend, or otherwise transfer personal data to any third party except documented subprocessors (see §7 and Annex 2).

---

4. Types of personal data

Category	Examples	Storage
Identification data	Name, email, account creation date, locale, plan	Encrypted at rest on Processor servers
Authentication data	Hashed password, 2FA secret (if enabled)	Bcrypt / encrypted
Mailbox credentials	IMAP/SMTP host, port, username, password	AES-256 encrypted, never logged in plaintext
MCP usage metadata	Tool name, IP, timestamp, success/failure	90-day retention, then auto-purged
AI call metadata	Preset, model, provider, tokens, cost, latency, status	90-day retention, then auto-purged. **Prompt and response content are NOT stored.**
Webhook/audit logs	Connection events, failed-auth attempts	12 months (legal retention)

---

5. Categories of data subjects

- The Controller themselves (account holder).
- The Controller's recipients/correspondents (email addresses, names, content of messages that pass through MailMCP via MCP calls — these are in **transit only**, never stored beyond the connection).

Support requests sent to MailMCP (contact@mailmcp.io, contact form, website chat) are processed by STAY WEB as an independent controller under its Privacy Policy, not under this DPA.

---

6. Technical and organisational security measures (TOMs)

The Processor implements the following measures (GDPR Art. 32) :

6.1 Encryption

- TLS 1.2+ enforced for all customer-facing endpoints (HTTPS only, HSTS enabled).

- IMAP : port 993 SSL or 587 STARTTLS only — no plaintext IMAP.
- SMTP : port 465 SSL or 587 STARTTLS only — no plaintext SMTP.
- Mailbox credentials encrypted at rest with AES-256 (Laravel `Crypt` facade).
- Database files protected by filesystem permissions (`0600`) on the VPS.

6.2 Access control

- Multi-factor authentication (TOTP) available for all accounts and required for admin.
- Role-based access : Controller can only access their own data ; admin access logged and IP-restricted via diag whitelist.
- API tokens for MCP scoped to a single mailbox.

6.3 Network

- Production VPS in France (LWS datacenters, ISO 27001).
- No public database port. All admin operations via SSH.
- Diagnostics endpoint `/x/diag/logs` IP-whitelisted to authorised IPs only.

6.4 AI-specific measures

- MailMCP never sends the content of the Controller's mailboxes to an AI model. Mailbox data is only read by the AI assistant the Controller connects itself (Claude, ChatGPT, etc.), under the Controller's own agreement with that provider.
- AI calls are routed through OpenRouter. Every feature that processes customer personal data on behalf of the Controller (email signature generator, outreach) is pinned to an EU region, with fallback to any other region refused (`allow_fallbacks=false`).
- The public website chat and its documentation search run on models hosted outside the EU (see §8).
- Data collection by providers for training disabled (`data_collection=deny`).

6.5 Operational

- Automated daily backup of database, 7-day retention.
- Migration to MySQL planned with at-rest encryption.
- Vulnerability scanning of dependencies (Composer audit).
- Incident response plan documented internally.

6.6 Pseudonymisation / minimisation

- AI call metadata stores only foreign key `user_id`, never the prompt/response.
- Log files rotate daily and purge after 90 days.
- The Processor never duplicates email content to its own storage.

---

7. Subprocessors

The Processor uses the subprocessors listed at **https://mailmcp.io/subprocessors** (the "Subprocessor List"), reproduced as **Annex 2** of this DPA.

- The Controller hereby gives general authorisation for the Processor to use these subprocessors (GDPR Art. 28.2).
- The Processor will notify the Controller in writing (email to the account email) at least **30 days** before adding a new subprocessor or replacing an existing one. The Controller may object within the notification period ; in case of unresolved objection, the Controller may terminate the contract without penalty.
- Each subprocessor is bound by data protection obligations no less protective than those of this DPA.

8. International transfers

Hosting, database and mailbox processing take place **in France** (LWS).

The following transfers to the United States are covered by Standard Contractual Clauses (SCCs, Commission Decision 2021/914) :

- **OpenRouter** (AI gateway) : routes the AI calls listed in Annex 2 and does not retain prompts or responses.
- **Polar** (Merchant of Record) : billing and invoicing data for paid plans.
- **Public website chat** (Microsoft Azure OpenAI, region outside the EU) and its documentation search (OpenAI embeddings) : only the text a visitor types into the chat.

AI features that process customer personal data on behalf of the Controller (email signature generator, outreach) are pinned to EU regions.

9. Data subject rights

The Processor will assist the Controller (GDPR Art. 28.3.e) in responding to data subject requests :

Right	Processor action
Access (Art. 15)	Within 30 days, provide a JSON/CSV export of all data linked to the data subject's email.
Rectification (Art. 16)	Update fields via the dashboard ; for fields the Controller cannot self-edit, email privacy@mailmcp.io.
Erasure (Art. 17)	Account deletion from dashboard triggers cascade delete within 30 days.
Portability (Art. 20)	Same as access — JSON/CSV export.
Restriction (Art. 18)	On request, mark account as suspended (no AI calls, no support replies).
Objection (Art. 21)	Disable any optional AI feature on request.

10. Breach notification

In case of a personal data breach (GDPR Art. 33), the Processor will **notify the Controller without undue delay and at the latest within 72 hours** of becoming aware of the breach, by email to the Controller's account address. The notification will include :

- Nature of the breach, categories and approximate number of data subjects/records.
- Likely consequences.
- Measures taken or proposed.
- Contact point for further information (privacy@mailmcp.io).

---

11. Audit

The Controller may, with reasonable advance notice (at least 30 days), and at the Controller's expense :

- Request a copy of the Processor's most recent third-party security audit report (if available).
- Submit a written questionnaire ; the Processor will respond within 30 days.
- For high-risk processing, request an on-site audit at the Processor's premises ; conducted under reasonable confidentiality conditions, max once per 12 months.

---

12. Liability

Each party's liability under this DPA is subject to and limited by the Master Services Agreement / Terms of Service. Nothing in this DPA limits a data subject's rights under the GDPR.

---

13. Governing law and jurisdiction

This DPA is governed by **French law**. Any dispute will be submitted to the competent courts of Paris (Tribunal Judiciaire de Paris).

---

14. Signature

This DPA enters into force upon the Controller creating a MailMCP account or upon counter-signature, whichever is earlier.

See the signature block at the end of this document.

Annex 1 — Description of the processing

See sections §3 (nature and purpose), §4 (types of data), §5 (data subjects).

Annex 2 — List of subprocessors

The authoritative list is published at **https://mailmcp.io/subprocessors** and updated as needed (with 30-day prior notice for material changes).

As of **2026-10-17**, the list is :

- **LWS — Ligne Web Services SAS** — Web hosting, database, support email. France. ISO 27001, HDS.
- **OpenRouter, Inc.** — AI inference gateway. USA, zero-retention, SCCs in place.

- **Microsoft Azure OpenAI** (GPT-4o-mini) — email signature generator, outreach pitch generation. Sweden (Sweden Central). ISO 27001, SOC 2.
- **Microsoft Azure OpenAI** (GPT-5.4-mini) — public website chat. Outside the EU, SCCs in place.
- **OpenAI** (text-embedding-3-small) — documentation search for the public website chat. USA, SCCs in place.
- **Polar Software, Inc.** — payments, recurring billing and invoicing (Merchant of Record). USA, SCCs in place. Card numbers are never seen nor stored by MailMCP.

Annex 3 — Technical and organisational measures

Detailed in §6 of this DPA.

Template version 1.0 — based on the EU Commission's Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914) and CNIL guidelines. A PDF copy signed by the Processor is available at https://mailmcp.io/legal/dpa.

Signatures

Processor	**Controller**
STAY WEB (SASU), publisher of MailMCP 59 rue de Ponthieu, bureau 326, 75008 Paris, France Nicolas Depredurand, CEO Nicolas Depredurand Signed electronically on 2026-10-16 21:41 UTC	Company name Name and position of the signatory Date Signature

The Processor's signature is a simple electronic signature (Regulation (EU) No 910/2014, art. 25). Text fingerprint (SHA-256) of this version: fe28591acf9add31bc989709cc2f66fa8257c5abee35e53401f54e4911afe572. This DPA also applies without countersignature from the creation of a MailMCP account (§1 and §14).