# MCPEmails Data Processing Agreement

Version 2026-11-01. Effective 1 November 2026. https://mcpemails.com/dpa

## 1. Parties, scope and acceptance

This Data Processing Agreement ("DPA") sets the terms on which MCPEmails processes personal data for a customer. It meets Article 28 of the EU General Data Protection Regulation ("GDPR") as it applies in Norway through the EEA Agreement, and Annex A extends it to customers under other laws, including South Africa's Protection of Personal Information Act ("POPIA").

| Role | Party |
|---|---|
| Processor | Albretsen AS, a Norwegian private limited company (aksjeselskap), org. no. 938 702 373, Håsteins gate 9, 5160 Laksevåg, Norway, trading as "MCPEmails" ("MCPEmails") |
| Controller | The customer that holds the MCPEmails account or workspace ("Customer") |

1. **Part of the Terms.** This DPA forms part of the MCPEmails Terms of Service (the "Terms"). It applies automatically to every Customer that accepts the Terms; no signature is needed. If the Terms and this DPA conflict on personal data, this DPA prevails.
2. **Countersigned copy.** A Customer that needs a signed copy can ask at privacy@mcpemails.com. MCPEmails will send this same text signed by Albretsen AS. A signed copy does not change the terms.
3. **Scope.** This DPA covers personal data in email content and mailbox metadata that MCPEmails processes on the Customer's behalf through the service at mcpemails.com, its MCP server, its API and its web client.
4. **Outside scope.** For account, billing, support and website usage data, MCPEmails is an independent controller under its Privacy Policy. This DPA does not cover copies of the MCPEmails server code that a Customer or anyone else hosts on its own infrastructure.
5. **Duration.** This DPA runs as long as MCPEmails processes personal data for the Customer. Section 8 survives it.

## 2. Details of processing

MCPEmails reads and acts on the Customer's connected mailboxes when the Customer's AI client, API key or automation calls a tool. It does not keep a copy of the email content it reads.

| Item | Description |
|---|---|
| Subject matter | Connecting the Customer's mailboxes to AI clients the Customer chooses (for example Claude or ChatGPT) over the Model Context Protocol, and running the automations, reminders and scheduled sends the Customer sets up |
| Duration | For the life of the Customer's account, then deletion under section 8 |
| Nature | Retrieving, searching, sending, drafting, organising and deleting email over IMAP, SMTP, the Gmail API or Microsoft Graph, each on a request from the Customer's client, key or automation |
| Purpose | Providing the service the Customer has asked for. No profiling, advertising, sale of data or AI training |
| Data subjects | The Customer's users, and the people they correspond with |

| Item | Description |
|---|---|
| Personal data | Email headers, addresses, names, subjects, bodies and attachments; contact details found in mail; mailbox credentials (app passwords or OAuth tokens); connection data (IP address and client name of the calling AI client) |
| Special categories | Mail may contain any category of personal data, including special categories such as health data. MCPEmails stores no email content it reads, so none of it is stored. The only content MCPEmails stores is what the Customer asks it to hold, listed in section 8 |

## 3. Processor duties (GDPR Article 28(3))

1. **Instructions (a).** MCPEmails processes personal data only on the Customer's documented instructions, including for transfers outside the EEA. The instructions are the Terms, this DPA, the Customer's settings, and the tool calls made by the Customer's AI clients, API keys and automations. If law requires other processing, MCPEmails will tell the Customer first unless the law forbids it.
2. **Unlawful instructions (h, last paragraph).** If MCPEmails believes an instruction breaks data protection law, it will tell the Customer and may refuse it.
3. **Confidentiality (b).** MCPEmails is run by one person, Asgeir Albretsen, who is bound by confidentiality. No one else has production access. Anyone given access later will be bound by confidentiality first.
4. **Security (c).** MCPEmails applies the measures in section 4 and keeps them at least as strong for the life of this DPA.
5. **Subprocessors (d).** MCPEmails uses only the subprocessors in section 5, on the terms set out there.
6. **Data subject requests (e).** Email stays in the Customer's mailbox, so most requests are answered there. MCPEmails will pass on any request it receives about the Customer's data without answering it itself, and will help the Customer answer the rest without undue delay.
7. **Assistance (f).** MCPEmails will give reasonable help with the Customer's duties under GDPR Articles 32 to 36 (security, breach notices, impact assessments and prior consultation), using the information available to it.
8. **Deletion at the end (g).** When the service ends, MCPEmails deletes personal data as set out in section 8. There is no stored email content to return; the mail stays with the Customer's mail provider.
9. **Information and audits (h).** MCPEmails will make available the information needed to show it meets this DPA, and allows audits under section 9.

## 4. Security measures (GDPR Article 32)

The main safeguard is that email content is fetched live and not stored.

| Area | Measure |
|---|---|
| Email content | Not written to the database, cache or logs. Only messages the Customer schedules for later or holds for approval are stored, encrypted (section 8) |
| Credentials at rest | App passwords and OAuth tokens are encrypted with AES-256-GCM. The key is a server secret kept apart from the database |
| Data in transit | TLS 1.2 or higher. Mail servers that do not support TLS are refused |
| Database location | One database for all customers, in the EU (Stockholm, Sweden) |
| Backups | Daily encrypted database backups, kept 7 days by Supabase |

| Area | Measure |
|---|---|
| API keys | Only a SHA-256 hash is stored. The raw key is shown once |
| Tenant isolation | Row-Level Security stops one workspace from reading another's data |
| Least privilege | Each key or AI client connection carries scopes. Sending, deleting and other changes need their own scopes and can be limited to chosen mailboxes |
| Read-only mode | A read-only connection opens IMAP folders with EXAMINE, so the mail provider also refuses changes |
| Human checks | The Customer can require approval before any send. Deleting mail needs an explicit confirmation flag |
| Abuse limits | Every key is rate limited, and sending has automatic brakes against bulk or runaway sends |
| Admin access | Production dashboards (Supabase, Vercel, GitHub) are protected by multi-factor authentication |
| Transparency | The server code is public on GitHub and can be self-hosted |

## 5. Subprocessors (GDPR Article 28(2) and (4))

The Customer gives general authorisation for the subprocessors below.

| Subprocessor | Purpose | Location |
|---|---|---|
| Supabase Pte. Ltd. (Singapore) | Database, authentication, and the edge functions that connect to mailboxes | Data stored in the EU (Stockholm, Sweden). Edge functions run in the US (East) and process email live without storing it |
| Vercel Inc. (USA) | Website, dashboard, and the server functions that pass AI client requests to the edge functions | US (East) and EU (Stockholm, Sweden); global network for requests in transit |
| Hetzner Online GmbH (Germany) | Mail relay: a TLS tunnel used for providers that refuse connections from cloud addresses, and as a one-time retry route when a provider refuses a direct connection. TLS runs end to end, so the relay cannot read mail or passwords | Germany |

1. **Not subprocessors.** The Customer's mail provider and AI client are chosen by the Customer and are not engaged by MCPEmails. Resend sends account emails (sign-in links, receipts, notices) and Stripe handles payments; both process only MCPEmails' own account and billing data, never mail content, and are covered by the Privacy Policy.
2. **Terms.** Each subprocessor is bound by a written data processing agreement with duties no weaker than this DPA. MCPEmails remains fully liable to the Customer for its subprocessors.
3. **Changes.** MCPEmails will email the account owner at least 30 days before adding or replacing a subprocessor, and will update this list. The Customer may object on reasonable data protection grounds within that period. If the objection cannot be resolved, the Customer may end the service before the change and get a pro-rata refund of prepaid fees for the unused period.

## 6. International transfers (GDPR Chapter V)

Stored data stays in the EU. Email is processed live in the United States, and Supabase's contracting entity is in Singapore.

1. **Mechanism.** Transfers to Supabase Pte. Ltd. and Vercel Inc. are covered by the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914 (Module Three, processor to processor), incorporated in each subprocessor's data processing agreement. Where a recipient is certified under the EU-US Data Privacy Framework, that also applies.
2. **Supplementary measures.** Mail content is not stored in the US. Credentials are decrypted there only in memory for the length of a request, and the key is kept apart from the database.
3. **Customer outside the EEA.** For a Customer outside the EEA, MCPEmails (in Norway) receives data from the Customer. Annex A sets out the terms for that.

## 7. Personal data breaches (GDPR Article 33(2))

1. MCPEmails will notify the Customer of a personal data breach without undue delay, and no later than 48 hours after becoming aware of it.
2. The notice goes to the account owner's email address and says what happened, the data and people likely affected, the likely consequences, and the steps taken or proposed. Details that are not yet known will follow as soon as they are.
3. MCPEmails will help the Customer notify authorities and data subjects. Notifying the Customer is not an admission of fault.

## 8. Retention and deletion

| Data | How it is stored | How long |
|---|---|---|
| Email content read, searched or sent immediately | Not stored. Passed to the Customer's client in the same response | Not kept |
| Mailbox credentials | Encrypted with AES-256-GCM | Erased the moment the mailbox is disconnected or the account is deleted. They remain inside encrypted daily database backups until those expire, up to 8 days later |
| Mailbox settings (address, display name, server settings, signature) | Database | Erased 30 days after the mailbox is disconnected or the account is deleted |
| Messages scheduled to send later | Full message encrypted with AES-256-GCM | The message is erased 7 days after it is sent, fails or is cancelled. Only the time and status are kept as send history, and that is erased 30 days after account deletion |
| Sends held for approval | Message, recipients and subject encrypted with AES-256-GCM | Held for at most 24 hours waiting for a decision. The message is erased 7 days after the send is decided or expires, and the approval record is deleted after 90 days |
| Activity log | Tool name, mailbox, time, status, duration and error code. No message bodies | Deleted after 90 days on Free and Personal, and after 2 years on Pro and Business. The Free dashboard shows only the last 30 days |
| AI client connection log | Sign-ins and token refreshes of AI clients, with IP address and user agent | IP address and user agent erased after 30 days |

| Data | How it is stored | How long |
|---|---|---|
| Automation run records | Subject and sender of each message an automation acted on, cut to 120 characters, and the outcome | Deleted after 90 days |
| Reminders and follow-ups | Encrypted reference to the message (subject, sender, recipients) | Deleted 90 days after the reminder completes (180 days if it failed) |
| Unsubscribe tools | Sender list from a scan, encrypted; requests the Customer sends, with the sender's name and address | Scan results deleted after 1 day. Sent requests erased 30 days after account deletion |
| Send safety records | One-way hashes of recipients and content, used to stop bulk sends | Deleted after 2 days |
| Account deletion | API keys revoked, mailboxes disconnected, credentials erased, workspace closed at once | Everything above is erased within 30 days of account deletion, and leaves the encrypted backups up to 8 days after that |

1. **Return.** MCPEmails stores no email content the Customer could need back. The Customer's mail stays with its mail provider throughout.
2. **Revocation.** The Customer can cut MCPEmails off at any time without asking, by revoking the app password or OAuth grant at its mail provider, or by disconnecting the mailbox in the dashboard.
3. **Earlier deletion.** On written request, MCPEmails will erase a Customer's remaining records sooner than the table above, unless law requires it to keep them.

## 9. Audits, liability and general terms

1. **Audits.** MCPEmails will answer reasonable written questions about its compliance within 30 days. If that is not enough, the Customer may audit once a year at its own cost, on 30 days' notice, during business hours and under a confidentiality agreement. A supervisory authority may audit at any time.
2. **Liability.** Liability under this DPA follows the limits in the Terms, except where data protection law does not allow them.
3. **Governing law.** This DPA is governed by Norwegian law, and disputes go to the courts of Bergen, Norway, as in the Terms. The Standard Contractual Clauses follow their own governing law clause.
4. **Changes.** MCPEmails may update this DPA to reflect changes in law or the service, by email to the account owner at least 30 days before the change takes effect. A change will not reduce the protection given to personal data.
5. **Contact.** Data protection: privacy@mcpemails.com. Security reports: security@mcpemails.com.

## Annex A. Customers under other data protection laws, including POPIA

This annex applies when the Customer is subject to a data protection law outside the EEA. MCPEmails gives the same protection under that law as under the GDPR, and terms in this DPA are read with the nearest equivalent in that law.

### A.1 South Africa (POPIA)

For POPIA, the Customer is the "responsible party", MCPEmails is the "operator", and this DPA is the written contract required by section 21(1).

1. **Authorisation and confidentiality (section 20).** MCPEmails processes the Customer's personal information only with the Customer's knowledge or authorisation, as set out in section 3.1. It treats that information as confidential and does not disclose it, unless law requires it or it is needed to perform this DPA.
2. **Security measures (sections 19 and 21(1)).** MCPEmails establishes and maintains the security measures in section 4. They are designed to secure the integrity and confidentiality of personal information and to prevent its loss, damage, or unlawful access or processing, as section 19 requires.
3. **Notice of unauthorised access (section 21(2)).** MCPEmails will notify the Customer immediately when there are reasonable grounds to believe that the Customer's personal information has been accessed or acquired by an unauthorised person. The 48-hour limit in section 7 is an outer limit and does not delay this notice.
4. **Data subject and Regulator matters.** MCPEmails will help the Customer meet its duties to data subjects and to the Information Regulator, including notices under section 22.

### A.2 Transfers out of South Africa (POPIA section 72(1)(a))

Personal information flows from the Customer in South Africa to MCPEmails in Norway, and from there to the subprocessors in section 5. The parties agree that this DPA is a binding agreement giving the information a level of protection substantially similar to the conditions for lawful processing in POPIA, as follows:

1. **Conditions upheld.** MCPEmails processes the information only for the purpose in section 2, keeps it no longer than section 8 allows, secures it under section 4, and helps data subjects exercise their rights through the Customer.
2. **Same law at the recipient.** MCPEmails is subject to the GDPR in Norway, which itself gives protection substantially similar to POPIA.
3. **Onward transfers.** MCPEmails transfers the information onward only to the subprocessors in section 5, under written terms no weaker than this DPA, and to recipients outside the EEA only under the safeguards in section 6. It does not transfer the information to any other third party except where law requires it, and then only after telling the Customer if the law allows.

### A.3 Other laws

1. **United Kingdom.** For a Customer subject to the UK GDPR, MCPEmails will, on request, sign the UK Information Commissioner's International Data Transfer Addendum (version B1.0) to the Standard Contractual Clauses.
2. **Switzerland.** For a Customer subject to the Swiss Federal Act on Data Protection, references to the GDPR include that Act, and the Standard Contractual Clauses apply with the changes the Swiss Federal Data Protection and Information Commissioner requires.
3. **Any other law.** Where another law needs a specific notice period, contract term or transfer document, the Customer can ask at privacy@mcpemails.com and MCPEmails will agree reasonable additions that do not change the service.

## Signatures (optional, for a countersigned copy)

| | **Processor** | **Controller** |
|---|---|---|
| Company | Albretsen AS (MCPEmails) | |
| Org. no. | 938 702 373 | |
| Name | Asgeir Albretsen | |

| | **Processor** | **Controller** |
|---|---|---|
| Title | Chair of the board | |
| Date | | |
| Signature | | |