Data processing agreement

The e-mails your applications send to mavimail can contain personal data. mavimail processes them on your behalf; a data processing agreement governs this processing.

The agreement is concluded when you accept the terms of service at registration; it forms part of the terms and applies to all inboxes of your organization. If you want a signed copy for your records, download the template below as PDF, sign it and send it to datenschutz@mavimail.dev; we countersign and return it. Deviating contracts are only possible in text form.

What the template covers

Subject matter and duration, nature and purpose of the processing, type of data and categories of data subjects, your instructions, our obligations (confidentiality, security, assistance with data subject requests, reporting personal data breaches), the use of sub-processors, audit rights, deletion during and after the end of the contract (e-mails you delete stay in the trash of your inbox for up to 7 days and are then deleted automatically and permanently; before that you can restore them or delete them permanently right away; when the retention period of your plan ends and when an inbox, project or organization is deleted, we delete without a trash, without delay and permanently; backups expire within 12 months at most) and the technical and organizational measures (TOMs). The measures include transport encryption: web interface and API over HTTPS, the SMTP entry point with TLS, the IMAP access exclusively over implicit TLS (TLS 1.2 or higher, no unencrypted access).

IMAP access and copies on your devices

On paid plans you can fetch the e-mails of an inbox with a mail client over IMAP. This is an instruction given by you: we transmit the e-mails in their original form to the mail client you set up with the inbox's credentials. From the transmission on, the copy is within your sphere of responsibility as controller; we are not a processor for storage, backup, onward transfer or deletion on your devices and in your mail client. Mail clients usually store e-mails locally and can load external images from third-party servers. A deletion at mavimail (also after the retention period ends or at the end of the contract) does not delete these copies; we cannot retrieve them. You are responsible for processing, protecting and deleting the copies lawfully, including towards data subjects. The IMAP credentials must be kept secret; pass them only to authorized members of your team. With "New IMAP password" in the app you can block the access immediately.

Instruction on the content of push notifications

The mobile apps can send push notifications about new e-mails. Whether content from your e-mails goes to Apple or Google is determined by the organization setting "Allow content in push" (Owners and Admins only; default: **off**). This is your instruction within the meaning of Art. 28(3)(a) GDPR:

- **Setting off (default):** The server does not send sender and subject to Apple or Google. A notification contains only the name of the inbox and of the project and technical identifiers (organization, project, inbox, e-mail).
- **Setting on:** You instruct us to hand the sender (name and address) and the subject (shortened to 120 characters) of every new e-mail to Apple or Google in the notification so that they are displayed on your members' devices. Each member can additionally switch the content off on their device; they can switch it on only as far as the organization allows it.
- In no case do we transmit the e-mail body, attachments or recipient addresses.

You are responsible for choosing the setting according to the data in your test e-mails, for informing your members, and for keeping names of projects and inboxes free of personal data, because these names appear in every notification. Depending on the device settings, notifications appear on the lock screen; we have no influence on that. Apple and Google process the notifications only to deliver them (Apple holds undeliverable notifications for 24 hours at most). Every change of the setting applies to all devices of the organization from the next notification.

Apps and cache on devices

The mobile apps cache recently retrieved lists and e-mails on the member's device, protected by device encryption and excluded from cloud and device backups. We delete this cache when the member signs out in the app and as soon as the app learns that the session has ended (for example by signing out under "Signed-in devices", a password change, suspension or account deletion); we cannot delete it remotely. Management, locking and loss of your members' devices are within your sphere of responsibility.

Sub-processors

As of 19 November 2026

Company	Service	Location / processing
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	server hosting of the application and all data	Germany (Falkenstein data center park)
Hetzner Online GmbH (Storage Box)	encrypted offsite backups of the database	Germany
Apple Inc., One Apple Park Way, Cupertino, CA 95014, USA	delivery of push notifications to iOS devices (Apple Push Notification service). Data: device token, inbox and project name, technical identifiers (organization, project, inbox, e-mail); only if push content is allowed, also sender and subject (shortened). Used with the iOS app	USA. Safeguard: EU-US Data Privacy Framework where certified, otherwise standard contractual clauses
Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	delivery of push notifications to Android devices (Firebase Cloud Messaging), with the same data as for Apple. Used only with the Android app; until then no data is transmitted to Google	USA. Safeguard: EU-US Data Privacy Framework where certified, otherwise standard contractual clauses
Forwarding delivery provider: not yet named, added here at least 30 days before forwarding is enabled	delivery of forwarded e-mails; only once forwarding is enabled	EU

No content from your inboxes goes to: Alfahosting GmbH, Halle (Saale) (sending system e-mails to accounts such as confirmation and invitation) and Stripe (payment through the service Link, independent controller). We announce changes to the list by e-mail at least 30 days in advance; you may object for an important data protection reason. For Apple and Google: we announce their addition to the list before the iOS app launches; Google is used only with the Android app.