
Clafk

Data Processing Agreement

How Clafk processes personal data on behalf of its business customers

Service	Clafk
Provided by	FITIONLED Oy, Business ID 3462861-3, Finland
Version	1.0
Last updated	3 August 2026
Contact	security@clafk.com

1. About this Agreement

This Data Processing Agreement (the “DPA”) sets out how FITIONLED Oy processes personal data on behalf of customers of the Clafk service. It forms part of the agreement between the Customer and Clafk for the provision of the Service (the “Service Terms”).

Clafk provides email organisation, classification, and reply drafting. The Service connects to a customer mailbox through the Google Gmail API or the Microsoft Graph API, and uses Large Language Model (LLM) technology to classify messages and prepare draft replies.

1.2 Our commitments

Customer Data is processed only to provide the Clafk service.

Customer Data is not sold, and is not shared for advertising purposes.

Customer Data is not used to train the models of LLM providers.

Complete inbound email bodies are not permanently stored and are not transmitted to LLM providers. Limited excerpts of message content may be temporarily processed by Clafk’s systems when required to provide classification and draft generation functionality.

Email attachments are not retrieved, processed, or stored.

Normal operation of the Service does not involve human access to mailbox content. Processing is automated and performed by secure server-side systems.

1.3 Definitions

Term	Meaning
Clafk, we, us	FITIONLED Oy, a company registered in Finland under Business ID 3462861-3, which operates the Clafk service.
Customer, you	The business that has agreed to the Service Terms and whose mailboxes are connected to the Service.
Customer Data	Data made available to Clafk through use of the Service, including mailbox data accessed under the Customer’s authorisation.
Personal Data	Personal data within Customer Data that Clafk processes on the Customer’s behalf.
LLM provider	A Large Language Model provider engaged as a subprocessor for classification, draft generation, and related language processing.
Subprocessor	A third party engaged by Clafk to process Personal Data in connection with the Service.

2. Roles and scope

The Customer is the controller of Personal Data processed through the Service, and Clafk is the processor. Where applicable law uses the terms business and service provider, the Customer is the business and Clafk is the service provider.

Clafk processes Personal Data on the Customer’s documented instructions, which are given through this DPA, the Service Terms, and the settings the Customer chooses in the Service. Clafk also processes Personal Data where required by law, and will inform the Customer before doing so unless the law prevents it.

Clafk uses specialised technology providers to operate the Service, covering hosting, database services, authentication, transactional email, monitoring, payment processing, and LLM processing. Each subprocessor is engaged only for the purposes necessary to provide the Service. Clafk’s production database infrastructure is hosted through Supabase’s European Union (Ireland) region configuration.

3. What Clafk processes

3.1 People whose data is processed

Authorised users of the Customer whose mailboxes are connected to the Service, and the senders and recipients of messages in those mailboxes. The categories of people and of personal data depend on the content of the Customer’s mailboxes and remain within the Customer’s control.

3.2 Categories of personal data

Category	What it covers
Account information	Name, email address, and account identifiers of authorised users, together with Service settings.
Email metadata	Sender name and address, subject line, timestamps, and message and conversation identifiers.
Email excerpts	A short preview provided by the mail provider and a limited excerpt of message text.
Generated drafts	Draft replies prepared by the Service for the Customer to review.
Writing style information	Where the feature is enabled, representative phrases and stylistic attributes derived from the user’s sent messages.
Knowledge base content	Material the Customer chooses to upload to support draft generation.
Mailbox integration authorisation data	The authorisation issued by Google or Microsoft that allows Clafk to maintain the connected mailbox integration.
Usage information	Records of Service activity, such as processing counts and model usage, used for operating the Service and for billing.

Clafk does not request special categories of personal data. Customers remain responsible for ensuring that their use of the Service complies with applicable data protection requirements.

4. How email is processed

4.1 Mailbox access and email processing

Clafk accesses a mailbox only after an authorised user has granted access through Google or Microsoft. Access can be withdrawn by the user at any time, either in the Service or in the mail provider’s own account settings.

When a message arrives, the Service retrieves it so that it can be classified and, where the Customer has enabled drafting, so that a reply draft can be prepared. Message content is processed in Clafk’s secure server-side infrastructure for the time needed to perform these functions.

Email processing is automated. Normal operation of the Service does not involve human access to mailbox content. Clafk’s internal operational tooling reports processing metadata, such as timing, model routing, and volumes, rather than message content. Administrative access to production systems is limited to authorised personnel and is used only where operationally necessary, for example to investigate an issue a customer has reported.

Complete inbound email bodies are not permanently stored. What Clafk retains for each processed message is the sender name and address, the subject line, the short preview provided by the mail provider, a limited excerpt of message text, the message timestamps, and the classification and routing information the Service generates.

Email attachments are not retrieved, processed, transmitted, or stored.

4.2 Large Language Model processing

Clafk engages LLM providers as subprocessors to classify messages and prepare draft replies. Only the information needed for the requested operation is sent, consisting of sender information, the subject line, and limited excerpts of message text.

- **Complete inbound email bodies are not sent to LLM providers.**
- **Customer Data is not used to train the models of LLM providers.**
- Requests to LLM providers are made by Clafk's server-side systems. Customer Data is not sent to LLM providers from the user's browser.
- Connections to LLM providers are protected using TLS encryption.

LLM providers act only as technical subprocessors for the purpose of providing Clafk functionality. They do not determine the purposes or means of the processing, and their involvement does not create an independent purpose for processing Customer Data. The LLM providers Clafk engages are listed in Section 6.

4.3 Generated drafts

Generated drafts are saved to the connected mailbox as ordinary drafts and remain under the Customer's control. **Clafk does not send a reply without an action by an authorised user.** Drafts are prepared using LLM technology and should be reviewed before sending.

4.4 Writing style profiles

If the Customer enables this feature, Clafk builds a short writing style profile from a limited sample of the user's sent messages, so that drafts match the user's usual tone. The profile holds representative phrases, greetings, closings, and stylistic attributes. Complete sent messages are not kept as part of the profile.

4.5 Knowledge base

If the Customer uses the knowledge base, uploaded content is stored in segments together with the representations used to retrieve relevant passages during drafting. The Customer decides what is uploaded.

4.6 Service emails

Clafk sends service-related email, such as account and lifecycle notifications, through a transactional email provider. This covers the recipient address, the content required to deliver the message, and delivery status information. **This provider is not used to process mailbox content retrieved through the Gmail API or the Microsoft Graph API.**

5. Security

Clafk maintains technical and organisational measures to protect Personal Data against unauthorised access and against accidental loss or damage, taking into account the nature and purposes of the processing.

5.1 Encryption

Customer Data is protected using encryption controls provided by Clafk and its infrastructure providers. Data transmitted between Clafk services, customers, and integrated third-party services is protected using TLS encryption. Encryption implementation, key management, and rotation are managed by the applicable infrastructure providers.

5.2 Technical and organisational measures

Measure	Description
Encrypted connections	Connections to and from the Service, including mail provider, LLM provider, and infrastructure interfaces, are protected using TLS.
Mailbox integration authorisation data	Mailbox connection authorisation data is handled only by server-side systems, is not exposed to end users or to code running in the browser, and is used solely to access the mailbox the user has authorised. It is removed when a mailbox is disconnected.
Server-side key handling	Service keys and provider API keys are held only in server-side environments and are not included in code delivered to the browser.
Customer separation	Customer Data is separated by account. Access is limited to records belonging to the signed-in user.
Database access controls	PostgreSQL Row Level Security is enabled on application data tables, with access rules applied by the database itself rather than by application code alone.
Least privilege	Service components run with the minimum database permissions they need, and privileged operations are scoped to the signed-in user's own records.
Webhook authentication	Incoming notifications from mail and payment providers are authenticated before any processing takes place. Requests that fail authentication are rejected.
Logging	Diagnostic logging is designed to exclude email content. Log records hold identifiers, outcomes, timing, and counts.
Error monitoring	Clafk monitors application errors in production. Sensitive data is reduced automatically before information is sent to the monitoring provider.
Administrative access	Access to production systems is limited to authorised personnel and granted on the basis of operational need.

Clafk periodically reviews and improves its technical and organisational security measures.

5.3 Security incidents

Clafk will notify the Customer without undue delay after becoming aware of a personal data breach affecting Personal Data, and will provide the information reasonably available to help the Customer meet its own obligations. Security matters can be raised at any time at security@clafk.com.

6. Subprocessors

The Customer authorises Clafk to engage the subprocessors listed below. Clafk requires subprocessors to provide appropriate data protection obligations consistent with the services they provide and applicable data protection requirements. Clafk remains responsible for its obligations under this DPA. Clafk will give reasonable notice before adding or replacing a subprocessor, and the Customer may raise an objection on reasonable data protection grounds.

Subprocessor	Purpose
Supabase	Database, authentication, and backend infrastructure
Vercel	Application hosting and deployment infrastructure
Resend	Transactional email delivery
Anthropic	Large Language Model processing
OpenAI	Large Language Model processing
Google	Gmail API integration
Microsoft	Microsoft Graph and Outlook API integration
Sentry	Error monitoring and diagnostics
Stripe	Payment processing

The processing locations and data protection terms of each subprocessor are those published by that subprocessor.

7. International transfers

Clafk is established in Finland and its production database infrastructure is hosted through Supabase's European Union (Ireland) region configuration. Some subprocessors listed in Section 6 process data outside the European Economic Area. Where that is the case, transfers are made on the basis of a transfer mechanism recognised under applicable data protection law, such as Standard Contractual Clauses or an adequacy decision. Customers can request current details of the mechanism relied on for a given subprocessor at security@clafk.com.

8. Data retention and deletion

Clafk retains Personal Data for as long as it is needed to provide the Service. When a customer deletes their account, the associated records are deleted through Clafk's account deletion process and the deletion mechanisms of its infrastructure providers. When a mailbox is disconnected, the integration authorisation data for that mailbox is removed.

Data held in backups by infrastructure providers is subject to those providers' backup retention arrangements.

9. Confidentiality

Clafk treats Personal Data as confidential. Personnel and authorised persons with access to Personal Data are subject to confidentiality obligations, and access is limited to what is necessary to perform Clafk's obligations.

10. Responsibilities

10.1 The Customer

- Decides the purposes for which the Service is used and ensures there is a lawful basis for it;
- Provides any notices and obtains any consents required in respect of the people whose data is processed, including senders and recipients outside the Customer's organisation;
- Manages who has access to the Service and removes access when it is no longer needed; and

- Reviews draft replies before sending them.

10.2 Clafk

- Processes Personal Data only on the Customer's instructions;
- Maintains the measures described in Section 5;
- Engages subprocessors only as described in Section 6;
- Assists the Customer, so far as reasonable and taking into account the information available to Clafk, in responding to requests from individuals exercising their data protection rights, and with data protection impact assessments;
- Notifies the Customer of personal data breaches as described in Section 5.3; and
- Deletes Personal Data as described in Section 8.

11. Information and audit

Clafk will make available the information reasonably needed to demonstrate compliance with this DPA, which may take the form of written answers to security questions, a description of the measures in Section 5, and the published security documentation of its subprocessors. Where applicable data protection law requires an audit and that information is not sufficient, the parties will agree its scope and timing in advance, and it will be carried out during normal business hours and subject to confidentiality. Clafk's infrastructure is operated by the subprocessors listed in Section 6, and Clafk cannot grant access to their premises.

12. Contact

Questions about privacy, security, or data protection, requests relating to this DPA, and notifications under Section 5.3 can be sent to the Clafk Security Team.

Provided by	FITIONLED Oy, Business ID 3462861-3, Finland
Service	Clafk
Contact	Clafk Security Team, security@clafk.com

13. Acknowledgement

This Data Processing Agreement describes the data processing terms applicable to the Clafk Service provided by FITIONLED Oy. It is made available to customers on request.

By using the Clafk Service, customers acknowledge that Personal Data may be processed as described in this Data Processing Agreement and the applicable Service Terms. Clafk can provide a counter-signed copy on request.