LEGAL

Data processing agreement

Anyone using ChatFlamingo processes personal data of their visitors. Art. 28 GDPR requires a contract for that. Version of 26 September 2026.

English translation. This is a convenience translation. The legally binding version is the German original.

Parties

The **controller** is the customer who uses ChatFlamingo on their website.

The **processor** is CertoClav Sterilizer GmbH, Peintner Straße 10, 4060 Leonding, Austria, FN 122912d, Landesgericht Linz.

This agreement forms part of the terms and conditions and is deemed concluded when an account is created.

When creating the account, the controller expressly confirms this agreement by ticking a separate box. We record when and in which version this happened and provide the controller with the record on request. This satisfies the written form of Art. 28(9) GDPR in electronic form.

1. Subject matter and duration

The subject matter is the processing of personal data arising from the operation of the chat widget on the controller's website. The processing lasts as long as the underlying contract.

2. Nature and purpose of the processing

Provision of a chat widget with live chat, storage of the conversation histories, display of visitors in the dashboard, sending of email tickets and — where activated by the controller — automatic answering of questions by a language model.

3. Categories of data subjects

- visitors to the controller's website
- employees of the controller who use the dashboard

4. Types of personal data

- content of the chat messages and conversation histories
- contact details, in so far as provided by visitors or recognised in the conversation text (name, email address, phone number)
- usage data: pages visited, page history, time on site, browser and operating system
- IP address and the approximate location derived from it, unless location lookup is switched off
- files and images uploaded by visitors
- access and profile data of dashboard users

Special categories under Art. 9 GDPR are not the subject of this agreement. The controller ensures that such data is not collected through the chat as a matter of course.

5. Instructions

We process the data exclusively on documented instructions from the controller. The settings the controller makes in the dashboard also count as instructions. If we consider an instruction unlawful, we say so.

6. Confidentiality

All persons with access to the data are bound to confidentiality.

7. Technical and organisational measures

The measures under Art. 32 GDPR are described in appendix 1. The built-in measures include in particular:

- a separate database per customer instead of a shared data set
- binding of the widget to the domains approved by the controller
- retention periods for attachments and whole conversations that the controller can set
- location lookup from the IP address that can be switched off
- roles in the dashboard (owner, administrator, read only)
- limits on requests per visitor and a blocking function

The full description is in appendix 1 at the end of this agreement.

8. Sub-processors

The controller consents to the use of the sub-processors named in appendix 2. We give four weeks' notice in text form of a change or an addition. Within that period the controller may object for an important data protection reason. If they object, we may terminate the contract in respect of the affected service as of the date of the change; there is no entitlement to continue with the previous sub-processor.

The full list is in appendix 2 at the end of this agreement.

9. Transfers to third countries

The sub-processors named in appendix 2 also process data in the United States. The basis for the transfer is the European Commission's standard contractual clauses under Art. 46(2)(c) GDPR, which we have concluded with each of these recipients. In so far as a recipient is certified under the EU-US Data Privacy Framework, the transfer is additionally based on the Commission's adequacy decision of 10 July 2023 under Art. 45 GDPR.

In addition, the following apply: encryption in transit and at rest, limiting the transmitted data to what is necessary for the particular processing, no use for training purposes, and an obligation on the recipient to inform us about official requests for information, in so far as that is legally permitted. We inform the controller without delay when we learn of such a request.

10. Support for the controller

We support the controller as far as possible in answering requests from data subjects and with data protection impact assessments and notification duties under Art. 32 to 36 GDPR.

11. Notification of breaches

We notify the controller of personal data breaches without delay after becoming aware of them.

The notification is made at the latest 24 hours after the breach came to our attention, in text form, to the address stored in the dashboard. It contains, where available, the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences and the measures taken. If not all details are available, we first report what is known and provide the rest without delay.

12. Deletion and return

After the contract ends we delete the data or return it, at the controller's choice, unless a statutory retention obligation prevents this. Independently of that, the retention periods set by the controller apply during the term of the contract.

The controller tells us their choice within 30 days of the end of the contract. Within that period we make a machine-readable copy of the data available for download. After that we delete the data including the backups within a further 30 days at the latest and confirm the deletion in text form on request. This period matches point 8.4 of the terms and conditions.

13. Evidence and audits

We make available to the controller the information necessary to demonstrate compliance and allow for audits.

The controller announces audits at least two weeks in advance in text form. They take place during our business hours, must not unreasonably disrupt operations and take

place at most once per calendar year — unless there is a specific reason, such as a reported breach or an order from the supervisory authority.

We may replace an on-site audit with meaningful evidence, in particular current reports by independent auditors or certificates. If these do not satisfy the controller, their right to an on-site audit remains.

Each party bears its own costs. For the effort of an on-site audit without specific cause we may charge a reasonable fee.

14. Liability

Point 12 of the terms and conditions applies accordingly to liability under this agreement.

Liability towards data subjects under Art. 82 GDPR remains unaffected. Between the parties, each side bears the share corresponding to its contribution to the responsibility.

Appendix 1 — Technical and organisational measures

Measures under Art. 32 GDPR, as at 26 September 2026.

Confidentiality

- **A separate database per customer.** One customer's conversations are not in the same data set as another's. A mix-up across customer boundaries is therefore ruled out.
- **Domain binding.** The widget only runs on the domains the controller has approved in the dashboard. Requests from other origins are rejected.
- **Role-based access.** The dashboard has the roles owner, administrator and read only. Every sign-in is personal.
- **Access on our side only as needed.** Staff are given access to customer data only in so far as this is necessary for maintenance and fault resolution, and are bound to confidentiality.

Integrity

- **Encrypted transmission.** All connections run over TLS. Unencrypted requests are redirected to the encrypted address.

- **Encrypted storage.** Databases and backups are encrypted at rest.
- **Logging.** Administrative access to customer data is logged.
- **Abuse brake.** Limits on requests per visitor, a monthly budget per account, a blocking function for individual visitors.

Availability and resilience

- **Backups.** Daily backup of the databases; restoration is tested regularly.
- **Separation of environments.** Development and operations run separately. No real customer data is used in development.

Deletion

- **Periods set by the controller.** The controller sets the retention periods for attachments and whole conversations in the dashboard; they run automatically.
- **Location lookup can be switched off.** A switch in the dashboard stops the approximate location being looked up from the IP address.
- **After the contract ends.** Deletion under point 12 of this agreement, including the backups.

Review

- The measures are reviewed at least once a year and whenever there is cause, and adjusted where necessary. The status of this appendix is updated accordingly.

Appendix 2 — Sub-processors

As at 26 September 2026.

Cloudflare, Inc.	101 Townsend St, San Francisco, CA 94107, USA · delivery of the website and protection against attacks · processing worldwide, standard contractual clauses
Salesforce, Inc. (Heroku)	415 Mission Street, San Francisco, CA 94105, USA · operation of the application and the databases · data centre in the European Union,

	standard contractual clauses
Anthropic PBC	San Francisco, CA, USA · language model for the AI's answers · processing in the USA, standard contractual clauses, no use for training purposes
OpenAI Ireland Ltd.	1st Floor, The Liffey Trust Centre, 117–126 Sheriff Street Upper, Dublin 1, Ireland · language model for the AI's answers · processing also in the USA by OpenAI, L.L.C., standard contractual clauses, no use for training purposes

There is no sub-processor here for payment handling: payment runs through Stripe Payments Europe, Ltd. and — where the app is booked through the Shopify App Store — through Shopify International Limited. Both process the customer's own contract data, not the data of the customer's website visitors, which is what this agreement covers. External error monitoring is not currently in use. If a sub-processor is added, the procedure in point 8 applies.