Data Processing Agreement — FRITS AI ApS

Last updated: June 12, 2026

This Data Processing Agreement ("DPA") forms part of the Terms of Service between FRITS AI ApS and the entity or person subscribing to GDPRchat ("Controller"). This DPA is entered into pursuant to Article 28 of Regulation (EU) 2016/679 (the "GDPR") and governs the processing of personal data by FRITS AI ApS on behalf of the Controller.

This DPA applies where the subscriber uses the Service in the course of business or otherwise processes other people's personal data through the Service. Where an individual uses GDPRchat purely for personal purposes, FRITS AI ApS is the data controller for that use as described in the Privacy Policy, and the controller–processor roles defined in this DPA do not apply to that use.

1. Definitions

- **"Processor"** means FRITS AI ApS, CVR: 45733785, Nyhavn 38, 1051 København K, Denmark.
- **"Controller"** means the subscriber who has accepted the GDPRchat Terms of Service and on whose behalf the Processor processes personal data.
- **"Personal Data"** means any information relating to an identified or identifiable natural person, as defined in Article 4(1) GDPR.
- **"Sub-processor"** means any third party engaged by the Processor to process Personal Data on behalf of the Controller.
- **"Data Subjects"** means the individuals whose Personal Data is processed under this DPA.
- **"Service"** means the GDPRchat AI chatbot platform accessible at gdprchat.eu.

2. Subject Matter and Duration

The Processor shall process Personal Data on behalf of the Controller for the purpose of providing the Service. This DPA shall remain in effect for the duration of the Controller's subscription to the Service and shall automatically terminate upon the deletion of all Personal Data following termination of the subscription, in accordance with Section 12 below.

3. Nature and Purpose of Processing

The Processor provides an AI-powered chatbot service. Processing activities include:

- Receiving, storing, and displaying chat messages submitted by the Controller's users
- Transmitting chat messages to the AI model provider (Mistral AI, France) for generating responses
- Transcribing voice input to text via Mistral's Voxtral model (France) when a user actively uses the microphone button
- Storing conversation history in a database hosted within the EU (Hetzner, Germany)
- Processing uploaded documents for in-chat analysis
- Generating images based on text prompts via Black Forest Labs (Germany)
- Performing web searches via Brave Search when requested by the user
- Sending transactional emails (account-related) via Brevo (France)
- Processing payments via Mollie B.V. (Amsterdam, Netherlands — intra-EEA; web) or Apple's App Store (iOS in-app purchases, billed by Apple as an independent controller)

4. Types of Personal Data Processed

The following categories of Personal Data may be processed:

- **Account data:** name, email address, cryptographic password hash, profile image
- **Chat content:** messages, prompts, and AI-generated responses that may contain Personal Data entered by users

- **Uploaded documents:** files shared in conversations that may contain Personal Data
- **Usage metadata:** timestamps, token counts, feature usage statistics
- **Payment data:** email address and subscription metadata (card details are processed exclusively by Mollie and never touch the Processor's servers)
- **Technical data:** IP addresses (rate-limiting in server memory only; web-server logs; and a security audit log of account events that retains the IP for 24 months — see the Privacy Policy, sections 3.3 and 7)

5. Categories of Data Subjects

Data Subjects include:

- The Controller's employees and team members who use the Service
- Any individuals whose Personal Data is included in chat messages or uploaded documents by the Controller's users

6. Obligations of the Processor

In accordance with Article 28(3) GDPR, the Processor shall:

6.1 Documented Instructions

Process Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data to a third country, unless required to do so by EU or Member State law to which the Processor is subject. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless the law prohibits such notification on important grounds of public interest.

6.2 Confidentiality

Ensure that persons authorised to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Access to Personal Data is limited to personnel who require it for the operation and maintenance of the Service.

6.3 Security (Article 32 GDPR)

Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as described in Section 9 (Technical and Organisational Measures) of this DPA.

6.4 Sub-processors

Not engage another processor without prior general written authorisation of the Controller. The Controller hereby grants general authorisation for the sub-processors listed in Section 7. The Processor shall inform the Controller of any intended changes concerning the addition or replacement of sub-processors, giving the Controller the opportunity to object to such changes. Objections must be raised within 30 days of notification.

6.5 Data Subject Rights

Assist the Controller, taking into account the nature of the processing, by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights laid down in Chapter III GDPR (Articles 15–22), as further described in Section 11.

6.6 Assistance with Compliance

Assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36

GDPR, taking into account the nature of processing and the information available to the Processor, including obligations relating to security of processing, data breach notification, data protection impact assessments, and prior consultation with supervisory authorities.

6.7 Deletion or Return

At the choice of the Controller, delete or return all Personal Data to the Controller after the end of the provision of the Service, and delete existing copies unless EU or Member State law requires storage of the Personal Data. See Section 12 for details.

6.8 Audits

Make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller. See Section 13 for details.

7. Authorised Sub-processors

The Controller hereby authorises the use of the following sub-processors. The Processor has entered into data processing agreements with each sub-processor that impose equivalent data protection obligations.

Sub-processor	Location	Purpose
Mistral AI	Paris, France	AI language model processing, text embeddings, and voice transcription
Hetzner Online GmbH	Germany	Infrastructure hosting (servers, database, file storage)
Black Forest Labs	Germany	AI image generation
Mollie B.V.	Netherlands (EEA — no third-country transfer)	Payment processing
Brevo (Sendinblue)	France	Transactional email delivery

The following services receive limited, non-account data and are not engaged as sub-processors: Brave Search (US) receives the web-search query text only — composed by the AI assistant and sent from the Processor’s servers with no user identifier or IP address attached, so queries cannot be linked to any person. Query text can, depending on what a user typed, itself contain personal data; see the Privacy Policy, sections 5 and 6, for how this is handled. Open-Meteo, OpenStreetMap Nominatim, Wikipedia, and Frankfurter.dev receive only non-personal query parameters. The European Commission’s VIES service (ec.europa.eu) receives a business customer’s VAT number — only when they voluntarily enter one to claim a reverse-charge VAT exemption — solely to confirm its validity; VIES is operated by the European Commission, not by the Processor.

Google, Microsoft and Apple are available as optional sign-in identity providers, and Apple additionally processes iOS App Store purchases. In those roles they act as independent data controllers, not as sub-processors of FRITS AI ApS.

8. International Data Transfers

The core processing infrastructure is located entirely within the European Union:

- **AI processing:** Mistral AI, Paris, France
- **Database and hosting:** Hetzner, Germany
- **Image generation:** Black Forest Labs, Germany
- **Email:** Brevo, France

Payment processing on the web is also entirely intra-EEA: Mollie B.V. is based in Amsterdam, the Netherlands, so no third-country transfer takes place for the payment-processing sub-processor.

Transfers of Personal Data outside the EU/EEA are limited to the following. iOS App Store purchases and Sign in with Apple involve Apple Inc. (United States) — protected by the European Commission's adequacy decision for the EU-US Data Privacy Framework (Article 45 GDPR), under which Apple is certified. Web-search query text is sent to Brave Search, Inc. (United States) with no user identifiers or IP address attached (see Section 7). Map tiles and reverse geocoding involve the OpenStreetMap Foundation (United Kingdom), covered by the European Commission's UK adequacy decision.

No Personal Data is transferred to any country outside the EU/EEA that lacks an adequacy decision or appropriate safeguards under Article 46 GDPR.

9. Technical and Organisational Measures

The Processor implements the following measures pursuant to Article 32 GDPR to ensure the security of Personal Data. GDPRchat employs a layered data protection architecture:

Layer 1: EU Infrastructure

All core services — AI model processing (Mistral AI, France), server infrastructure and database (Hetzner, Germany), and image generation (Black Forest Labs, Germany) — are hosted within the European Union. This means your data is processed exclusively by EU-based companies under EU jurisdiction. There is no data mining, no profiling, and no sharing of data with US or Chinese technology companies for their own purposes.

Layer 2: PII Filter (Client-Side)

GDPRchat includes a built-in Personal Identifiable Information (PII) scanner with 124+ detection patterns covering all 27 EU member states. This scanner runs entirely in the user's web browser — on the user's own device. Detected PII (emails, phone numbers, IBANs, national ID numbers, credit card numbers, passport numbers, VAT numbers, and more) is highlighted and blocked before the message ever leaves the device. No data flagged by this filter is transmitted to any server.

Additional Security Measures

- **Encryption in transit:** All data is transmitted over TLS 1.2 or higher.
- **Encryption at rest:** The extracted text of every user-uploaded document is encrypted at the application layer with AES-256-GCM, under a key held only in the runtime environment — never written to the database or to backups, so the document text cannot be read from a copied database snapshot or backup without that key. Key rotation is supported without service interruption.
- **Infrastructure & physical security:** All servers are hosted in Hetzner's ISO 27001-certified data centres in Germany, with the physical access controls, monitoring, and environmental safeguards that certification requires.
- **Password security:** User passwords are stored as bcrypt hashes; plaintext passwords are never retained.
- **Access control:** Role-based access control with JWT-based session authentication. Administrative access is restricted and separately authenticated.
- **No tracking or analytics:** GDPRchat does not use Google Analytics, tracking pixels, fingerprinting, or any third-party analytics. No profiling of user behaviour is performed.
- **Data minimisation:** Unstarred conversations are automatically deleted after a configurable retention period (default: 8 days of inactivity).
- **Cookie minimisation:** Only strictly necessary cookies (authentication, security) and preference cookies tied to features the user has actively chosen are used — no tracking, analytics, or advertising cookies. See the Privacy Policy's cookie section for the complete list and the ePrivacy Article 5(3) exemption analysis.

10. Data Breach Notification

The Processor shall notify the Controller without undue delay, and in any event within 48 hours, after becoming aware of a personal data breach

affecting the Controller's data. This is stricter than the 72-hour window specified in Article 33 GDPR for the Controller's notification to the supervisory authority.

The notification shall include:

- A description of the nature of the personal data breach, including the categories and approximate number of Data Subjects and records concerned
- The name and contact details of the Processor's data protection contact point
- A description of the likely consequences of the breach
- A description of the measures taken or proposed to address the breach, including measures to mitigate its possible adverse effects

The Processor shall cooperate with the Controller and take reasonable steps to assist in the investigation, mitigation, and remediation of each personal data breach.

11. Assistance with Data Subject Rights

The Processor shall assist the Controller in fulfilling its obligations to respond to Data Subject requests under Chapter III GDPR, including:

- **Right of access (Article 15):** The Service provides a data export feature that allows users to download all their data in machine-readable JSON format.
- **Right to rectification (Article 16):** Users can update their account information directly through the Service.
- **Right to erasure (Article 17):** The Service provides account deletion functionality that performs a cascading deletion of all user data, including conversations, messages, documents, and associated records.
- **Right to data portability (Article 20):** The data export produces a structured, commonly used, machine-readable format (JSON).

For requests that cannot be fulfilled through the Service's self-service features, the Controller may contact the Processor at support@frits.ai.

12. Return and Deletion of Data

Upon termination of the Controller's subscription, the Controller may export all data using the Service's data export feature (Article 20 GDPR). The Processor shall:

- Make the data export available for a minimum of 30 days following termination
- Upon written request from the Controller, or automatically after the 30-day period, delete all Personal Data from its systems, including backups, within a further 30 days
- Provide written confirmation of deletion upon the Controller's request

The Processor may retain Personal Data to the extent required by EU or Danish law (e.g. bookkeeping obligations under the Danish Bookkeeping Act, bogføringsloven), in which case the Processor shall inform the Controller of the applicable legal basis and the retention period.

Operational backups. During normal operation, when a Data Subject or the Controller deletes individual data (a conversation, an uploaded file, an entire account) the data is removed from the live database immediately and any associated file is removed from disk in the same operation. The Processor maintains automated encrypted backups of the database and file storage for disaster-recovery purposes; these backups have a rolling retention window of up to 30 days, after which they are permanently destroyed. Deleted data is never accessed, restored or used during this window — backups are only read when recovering from infrastructure failure. To guarantee immediate and complete destruction across all backups (Article 17 GDPR), the Controller may request expedited backup purge by contacting support@frits.ai; this is fulfilled within the 30-day window required by Article 12(3) GDPR.

13. Audit Rights

The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR.

The Controller, or an independent third-party auditor appointed by the Controller, may conduct an audit of the Processor's processing activities, subject to the following conditions:

- The Controller shall provide at least 30 days' written notice before the audit
- Audits shall be conducted during normal business hours and shall not unreasonably disrupt the Processor's operations
- The auditor shall be bound by appropriate confidentiality obligations
- The Controller shall bear the costs of the audit, unless the audit reveals material non-compliance by the Processor
- The Processor may satisfy audit requests by

providing relevant third-party certifications, audit reports, or attestations, where available

14. Controller Responsibilities

The Controller is solely responsible for the Personal Data it processes through the Service and for the lawfulness of that processing. The Controller warrants that it has:

- a valid legal basis under Article 6 GDPR and, where it processes special categories of Personal Data (Article 9 GDPR) or personal data relating to criminal convictions and offences (Article 10 GDPR), a valid condition under those Articles and any applicable EU or Member State law;
- provided any information required under Articles 13 and 14 GDPR to, and where relevant obtained any consent required from, the Data Subjects;
- carried out any Data Protection Impact Assessment required under Article 35 GDPR and any prior consultation required under Article 36 GDPR; and
- the right to disclose the Personal Data to the Processor and to instruct the Processor to process it as set out in this DPA.

The Processor acts only on the Controller’s documented instructions, does not determine the purposes of the processing or the Controller’s legal basis, and is not responsible for the Controller’s compliance with the obligations above. The Controller shall not instruct the Processor to process Personal Data in a manner that infringes GDPR or other applicable data protection law. The Processor provides the tools and the technical and organisational safeguards described in this DPA and the Privacy Policy, but does not thereby assume the Controller’s own compliance responsibilities.

15. Liability

Each party’s liability under this DPA shall be subject to the limitations and exclusions of liability set out in the Terms of Service, except that neither party’s liability for breaches of its data protection obligations under GDPR shall be limited or excluded to the extent such limitation or exclusion is not permitted by applicable law.

In accordance with Article 82 GDPR, the Processor shall be liable for damage caused by processing only where it has not complied with obligations of the GDPR specifically directed to processors, or where it has acted outside or contrary to lawful instructions of the Controller.

16. Governing Law and Jurisdiction

This DPA shall be governed by and construed in accordance with the laws of Denmark, without regard to its conflict of law provisions. Any disputes arising out of or in connection with this DPA shall be subject to the exclusive jurisdiction of the courts of Copenhagen, Denmark.

Where there is any conflict between this DPA and the Terms of Service, the provisions of this DPA shall prevail with respect to data protection matters.

Contact

For questions about this Data Processing Agreement or our data protection practices, contact:

FRITS AI ApS CVR: 45733785 Nyhavn 38, 1051 København K Denmark Email: support@frits.ai

Supervisory authority: Datatilsynet (Danish Data Protection Agency), www.datatilsynet.dk