Data Processing Agreement — FRITS AI ApS

Version 2026-10-30 — last updated October 30, 2026

100% European — and how you can check it

- **A European company.** GDPRchat is made by FRITS AI ApS, a Danish company (CVR 45733785), and runs under EU law.
- **Every company that handles your data for us is European.** Scaleway (France) runs the AI and sends our emails, Hetzner (Germany) stores everything, IONOS (Germany) generates images and Mollie (Netherlands) handles payments. All of them are bound by EU law.
- **Your chats never leave the EU.** Your chats and the files you share are processed by Scaleway in Paris, France — pictures you ask for by IONOS in Germany — and stored by Hetzner in Germany, in those companies' own data centres. No American or Chinese company receives them — not even the companies that built the AI models, because Scaleway runs the models on its own machines and their makers receive nothing. That matters for the US CLOUD Act, which lets US authorities order US companies to hand over data they hold anywhere in the world: no US company holds your chats, and Scaleway states that its AI services are not subject to the CLOUD Act.
- **Nothing else leaves the EU unless you choose it.** Only these companies outside the EU receive anything, and only when you use the feature that needs them: Apple Inc. (signing in with Apple, or buying inside the iOS app), Google LLC (signing in with Google), Microsoft Corporation (signing in with Microsoft) and OpenStreetMap Foundation (viewing a map, or turning on precise location). None of them receives your chats. When the assistant searches the web, it sends a search it wrote itself to Linkup, a company established in France, with nothing attached that identifies you — so no personal data travels with it. Asked for the words of a song, the assistant looks up only the song's title and artist on lyrics sites: songtexte.com (Molindo GmbH, Austria) first, and only when the song is not there, LRCLIB (an open lyrics database) and Genius (Genius Media Group, United States). Nothing that identifies you is sent with that either.
- **One level further down, stated too.** Scaleway rents building and rack space in Italy, the Netherlands and Poland from Equinix, Iron Mountain and Digital Realty, which are incorporated in the United States. None of them is listed against Scaleway's AI services, and the AI does not run in those buildings. Mollie handles payments as a regulated payment institution, and its own privacy statement says third parties outside the European Economic Area may process payment data in some cases, under Standard Contractual Clauses. That concerns payment details only — never your chats. Sources: scaleway.com/en/subprocessorlist and Scaleway's Generative APIs privacy documentation (read 14 September 2026), and mollie.com/privacy (read 17 September 2026).
- **What changed on 18 September 2026.** Until then most chat answers came from Mistral AI, a French company whose own published list of suppliers names US-owned companies, among them Microsoft, Google, CoreWeave and Cloudflare. That was the one exception to "100% European", so we stopped using it: Mistral AI has received nothing since, and our code can no longer reach it.

Checked 17 September 2026 against each supplier's published list · next check by 17 March 2027.

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 Processor’s AI model sub-processors (Scaleway (France), as listed in Section 7) for generating responses
- Transcribing voice input to text via the Processor’s voice model run by our AI sub-processor in 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 and editing images via IONOS Cloud GmbH (Berlin, Germany)
- Performing web searches via Linkup (France) when requested by the user
- Sending transactional emails (account-related) via Scaleway (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, or is in the process of concluding, a data processing agreement with each sub-processor, in each case imposing equivalent data protection obligations. The current status for each sub-processor is published at gdprchat.eu/transparency.

Sub-processor	Location	Purpose
Scaleway	Paris, France	AI language model processing, text embeddings, voice transcription, and reading answers aloud
Hetzner Online GmbH	Germany	Infrastructure hosting (servers, database, file storage)
IONOS Cloud GmbH	Berlin, Germany (EU/EEA under the AVV)	AI image generation and image editing
Mollie B.V.	Amsterdam, Netherlands (EEA)	Payment processing
Scaleway (Transactional Email)	Paris, France	Transactional email delivery

Sub-processors' own suppliers. Each sub-processor above engages infrastructure suppliers of its own in order to deliver its service, and under Article 28(4) GDPR is bound to impose equivalent data protection obligations on them. Some of those suppliers are companies incorporated outside the EU that operate equipment situated within the EU/EEA. Scaleway, which performs all AI processing under this Agreement, publishes its list at scaleway.com/en/subprocessorlist; it names data-centre suppliers, of which Equinix, Iron Mountain and Digital Realty are US-incorporated and provide building and rack space in Italy, the Netherlands and Poland. Scaleway lists no sub-processor against its AI services, which it operates on its own infrastructure, so no company in the chain that processes the content of the Service is established outside the EU. The Processor discloses this level too, so that the Controller can verify for itself what "100% European" covers. Because the data continues to be processed within the EU/EEA, this is not a transfer to a third country under Chapter V GDPR. Each sub-processor maintains its own current list. Last reviewed by the Processor on 17 September 2026.

The following services receive limited, non-account data and are not engaged as sub-processors: Linkup (a French company) receives the web-search query text only — a query the AI assistant composes itself and the Processor's servers send. No account, no user identifier, no IP address and no conversation content travels with it, and nothing in the request links it to a person, so no Personal Data is transmitted (Section 8). Linkup processes queries on its own infrastructure in the EU, the United States, Canada and Asia-Pacific and does not guarantee local processing, so an individual query may be handled outside the EU/EEA. Open-Meteo, OpenStreetMap Nominatim, Wikipedia, and Frankfurter.dev receive only non-personal query parameters. openrouteservice (HeiGIT gGmbH, Germany) receives route coordinates from the Processor's server; these include an end user's own position only when that user taps "Route here" on a map, and never an account, identifier or IP address. 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:** Scaleway (France)
- **Database and hosting:** Hetzner, Germany
- **Image generation:** IONOS Cloud GmbH, Berlin, Germany
- **Email:** Scaleway, France

Payment processing on the web is carried out by Mollie B.V., which is established in Amsterdam, the Netherlands. Mollie’s own privacy statement says that third parties outside the EEA may process payment data in some cases, under Standard Contractual Clauses; this concerns payment data only, and no content of the Service reaches Mollie.

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. Where a user chooses Google or Microsoft as a sign-in identity provider, the name and email address held by that account are received from Google LLC or Microsoft Corporation (United States), both certified under the same Framework. 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: the Apple, Google and Microsoft transfers rest on the EU-US Data Privacy Framework and the OpenStreetMap transfer on the United Kingdom adequacy decision, both under Article 45 GDPR.

Web search is not among those transfers. When the assistant searches the web it sends a query it composed itself. No account, no user identifier, no IP address and no conversation content travel with it. Nothing links it to a person. It is our system's own outbound request — the same as a browser fetching

a page — not the user's data. No personal data leaves the EU when a search runs. Chapter V GDPR does not engage for it. Set out in full, the request carries the search query, composed by the assistant, a depth setting (how thoroughly to search), an output type (a result list, or a sourced answer), how many results to return and sometimes a domain filter, an image flag, or an earliest date for news — and nothing else. This is verified against src/lib/services/linkup-search.ts (callLinkup), the single outbound gateway, rather than asserted; a field added there would falsify this paragraph.

Where the query is handled is disclosed all the same. Linkup is a French company, it operates its own search infrastructure in the EU, the United States, Canada and Asia-Pacific, it allocates queries across those regions by load, and it does not guarantee that an individual search is handled locally; its API carries no region parameter, so the Processor cannot pin one search to Europe and does not claim to. Linkup is the sole recipient — if a search fails it fails, and the query is not sent onward to any other provider. Chat content, uploaded documents and all data stored at rest are never sent on that path and remain within the EU/EEA. Asked for the words of a song, the assistant looks up only the song's title and artist on lyrics sites: songtexte.com (Molindo GmbH, Austria) first, and only when the song is not there, LRCLIB (an open lyrics database) and Genius (Genius Media Group, United States). Nothing that identifies you is sent with it.

Change of 3 September 2026 — how this Section characterises web search. Until that date this Section characterised web search as a transfer of Personal Data outside the EU/EEA for which the Processor identified no Chapter V footing, and described a second such flow: a failed Linkup call was automatically retried on Brave Search, Inc. (United States). Two things changed. Brave was removed as a provider, so no United States company receives a web search — which is a narrower statement than the paragraph above, and deliberately so: Linkup’s own routing across regions is a separate matter and is unchanged. And the Processor determined, on the verified contents of the request, that a query the assistant composes and sends with no account, no identifier, no IP address and no conversation content is not Personal Data, so no Chapter V transfer arises on the search path. The earlier characterisation is superseded. A Controller holding a copy of this Agreement dated before 3 September 2026 will find that wording in it: what is sent and where it goes have not changed, and no disclosure has been withdrawn — the conclusion drawn from the same facts has, in the Controller’s favour.

The complete current list of recipients outside the EU/EEA is published at gdprchat.eu/security — each with what is sent, when it happens, and the legal basis relied on — and is generated from the same record as this Section. For the Service itself those recipients are

Apple Inc., Google LLC, Microsoft Corporation and OpenStreetMap Foundation. Where the assistant's search queries go is set out on the same page, kept separate from that list and labelled as the different thing it is.

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 (Scaleway (France)), server infrastructure and database (Hetzner, Germany), and image generation (IONOS, 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 83 detection patterns covering all 27 EU member states and the United Kingdom, plus an optional Extended mode that adds 57 further patterns (140 in total). Both run 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 the message is held back before it ever leaves the device. No data flagged by this filter is transmitted to any server. Detection is pattern-based: it recognises data written in known formats, and cannot recognise personal data that has no fixed format — a person's name in ordinary prose, for example. This filter is a technical safeguard, not a guarantee.

Additional Security Measures

- **Encryption in transit:** All data is transmitted over TLS 1.2 or higher.
- **Encryption at rest:** The extracted text of documents uploaded **in chat** 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 that text cannot be read from a copied database snapshot or backup without that key. Key rotation is supported without service interruption. Content uploaded to Ask PDFs, or to a service bot, is **not** covered by this application-layer encryption, because it has to remain searchable: full-text and semantic search run over the stored text. That content is protected by the

access controls below, by EU-hosted infrastructure, and by AES-256-encrypted off-site backup archives.

- **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:** Conversations that are not starred and not in a folder are automatically deleted after a configurable retention period (default: 12 months of inactivity), and only after the user has been emailed a warning.
- **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

Execution

This Agreement is published by the Processor in executed form. No further signature from FRITS AI ApS is required, and the Controller does not need to request one. It takes effect for the Controller on the earlier of the Controller's acceptance of the Terms of Service and the Controller's first use of the service, and applies for as long as the Processor processes personal data on the Controller's behalf.

Signed for and on behalf of the Processor

FRITS AI ApS, CVR 45733785 Nyhavn 38, 1051 København K, Denmark Frits Lyneborg, Founder
Executed electronically on publication. Version 2026-10-30 (last updated October 30, 2026).

A countersignature is not required for this Agreement to bind either party. Where the Controller's own procurement process needs one for its records, the block below may be completed and retained by the Controller; it does not need to be returned to the Processor.

For the Controller (optional, for the Controller's records)

Organisation: _____ Name: _____ Title: _____ Date: _____ Signature: _____