Back to homepage

Privacy Policy — SerahrChat

Note: This English version is provided for informational purposes only. The German text constitutes the sole legal basis.

Version 1.2 — effective from May 19, 2026 (legal change: data protection officer status, Art. 22 clarification)

Table of Contents

1. Data Controller

Thorsten Ahrens
Serahr — serahr.de
Email: contact@serahr.de

This policy covers the product page at serahr.de/chat and the SerahrChat software product.

1a. Data Protection Officer

We have not appointed a data protection officer. Under Art. 37 GDPR no appointment is required because we neither carry out large-scale processing of special categories of personal data (Art. 9 GDPR) nor systematic monitoring of data subjects, and we employ fewer than 20 persons routinely processing personal data. Please send data protection enquiries directly to contact@serahr.de.

2. Overview: Where Is Data Stored?

SerahrChat is self-hosted. Most data remains on the customer's server.

DATA	STORAGE LOCATION	PURPOSE
Uploaded documents	Customer server	Knowledge base for the chatbot
Vector index (embeddings)	Customer server (LanceDB)	Semantic search
Chat histories	Customer server (SQLite)	Analytics, auto-deleted after 90 days
Aggregated analytics	Customer server	Usage statistics, 90-day rotation

TA	STORAGE LOCATION	PURPOSE
Audit logs	Customer server	Security log, IP-anonymized, 90-day rotation
Admin credentials	Customer server	Authentication (Argon2-hashed)
Chat queries (for answering)	Customer-chosen LLM provider (e.g. OpenRouter, OpenAI, Mistral, or local)	AI response generation — forwarded, not permanently stored
Document embeddings (on creation)	Customer-chosen embedding provider (e.g. OpenAI, OpenRouter, or local)	Document vectorization for semantic search — result stored locally on customer server
License key + Instance ID	License server (licence.serahr.de)	License validation
Payment data	Stripe	Payment processing (PCI-compliant)
Email address	License server + Resend	License communication, password reset, trial onboarding
Consent records (accepted AGB version, DSE version, timestamp)	License server (licence.serahr.de)	Proof of consent to legal documents (Art. 7(1) GDPR)
Double-opt-in evidence (email-confirmation IP + timestamp)	License server (licence.serahr.de)	Proof of consent to email communication (§ 7(2)(2) UWG)

- **Art. 6(1)(a) GDPR** — Consent: double-opt-in on trial sign-up, optional marketing/product news.
- **Art. 6(1)(b) GDPR** — Contract performance and pre-contractual measures: license purchase, license validation, update/license server communication, Stripe billing, trial onboarding emails.
- **Art. 6(1)(c) GDPR** — Legal obligation: tax retention of invoice data (§ 147 AO, 10 years), disclosure to law enforcement under Regulation (EU) 2023/1543, proof of consent (Art. 7(1) GDPR + § 7(2)(2) UWG).
- **Art. 6(1)(f) GDPR** — Legitimate interest: server logs, abuse prevention (rate limiting), security audit log. Balancing: processing is limited to what is technically necessary, not used for profiling, and IP addresses in audit logs are anonymized (last octet = 0); legitimate interests therefore prevail.

3. Data Processing in Detail

3.1 Website Visits

Server automatically collects: IP addresses (in server logs, automatic rotation), browser type, operating system, referrer URL, date and time of access.

Legal basis: Art. 6(1)(f) GDPR (legitimate interest). No tracking cookies or third-party trackers used.

3.2 License Purchase and Payment

- **Email address:** For license delivery, invoices, and support communication. Stored on the license server (Supabase, EU region).
- **Payment data:** Processed exclusively through Stripe (PCI-DSS certified). We do not store credit card or bank account data.

Legal basis: Art. 6(1)(b) GDPR (contract performance).

3.3 License Validation (Phone-Home)

- **Transmitted data:** Instance ID, license key
- **Frequency:** Maximum once per 7 days (local cache)
- **If unreachable:** Grace period — the chatbot continues to function

No usage data, document content, or chat histories are transmitted. Legal basis: Art. 6(1)(b) GDPR.

3.4 Update Checks

The installation automatically checks for new versions via update.serahr.de. Only the current version number is compared. No personal data is transmitted.

3.5 Chat Queries, Embedding, and LLM Providers

This is the most important point for data protection assessment:

a) Document Embedding (on upload):

When the customer uploads documents, they are converted into vectors (embedding) to enable semantic search. The embedding provider is chosen by the customer:

- **External provider (e.g. OpenAI, OpenRouter):** Document content is transmitted to the chosen provider to generate embedding vectors. The resulting vectors are stored locally on the customer's server (LanceDB).
- **Local models:** No external data transfers — fully local on the customer's server.

b) Chat queries (during use):

1. The question is processed on the customer's server
2. Relevant text passages from uploaded documents are identified via semantic search (local, LanceDB)
3. Question + relevant text passages are sent to the configured LLM provider to generate an answer
4. The answer is returned to the visitor

Both the LLM provider and the embedding provider are chosen and configured by the customer (own API key). Possible providers: OpenRouter (USA), OpenAI (USA), Mistral (France/EU), or local models (Ollama, LMStudio) with no external data transfers.

Note on GDPR compliance: Stored data (documents, chat histories, analytics, embedding vectors) remains entirely on the customer's server. When using external LLM or embedding providers, data is transmitted to third parties. For full GDPR compliance, we recommend local models or EU-based providers. The choice and responsibility lies with the customer.

3.6 Email Communication

Emails are sent exclusively for: license delivery, password reset codes, email verification codes, and onboarding emails during the free trial.

Sent via Resend. Onboarding emails are sent only during the 7-day trial. Legal basis: Art. 6(1)(b) GDPR.

4. Data Storage on Customer Server

- **Documents:** Encrypted storage (Fernet/AES)
- **Vector database:** Document embedding vectors (LanceDB)
- **Chat histories:** Anonymized, automatic deletion after 90 days
- **Analytics:** Aggregated daily statistics, 90-day rotation
- **Audit log:** Security events, IP-anonymized, 90-day rotation
- **Admin database:** Configuration, password hash (Argon2), recovery codes (HMAC-SHA256)

5. Retention Periods

DATA	PERIOD
Chat histories	90 days (automatic deletion)
Analytics	90 days (automatic rotation)
Audit logs	90 days (automatic rotation)
Documents	Until manual deletion by customer
Email + name (license server)	Until license deletion; on erasure request (Art. 17 GDPR) immediately
License-validation logs (IP, instance ID)	90 days automatic rotation; on erasure request immediately
Error reports (IP, stack traces)	90 days automatic rotation; on erasure request immediately
Trial onboarding data	Until purchase or 30 days after trial ends; on erasure request immediately
Consent records (AGB/DSE version + timestamp)	Until license deletion + 30 days (Art. 7(1) GDPR proof obligation)
Double-opt-in evidence (confirmation IP + timestamp)	Until license deletion + 30 days (§ 7(2)(2) UWG)
Plan-change confirmations (anonymized)	Permanent retention as proof of purchase (§ 305 BGB), without IP/instance ID after erasure
Stripe customer data (email, name, address)	Until license deletion; afterwards anonymized in Stripe (Stripe retains invoice data for 10 years per § 147 AO)
Payment metadata in our DB (amount, date)	10 years (§ 147 AO accounting obligation), without PII
Admin access after contract end	30 days after expiry, then revoked

Anonymization note: When you exercise your right to erasure (Art. 17 GDPR), personal data is deleted immediately. Where statutory retention obligations apply (in particular § 147 AO for tax records), only the legally required metadata (amount, date) is retained — all direct identifiers are anonymized. You will receive a confirmation email of the deletion as required by Art. 12(3) GDPR.

6. Disclosure to Law Enforcement

We may be legally required to disclose stored data to law enforcement authorities on the basis of a European Production Order or European Preservation Order pursuant to Regulation (EU) 2023/1543. Such disclosure is made exclusively on the basis of a lawful order and to the extent required by law. Legal basis: Art. 6(1)(c) GDPR (legal obligation).

7. Your Rights

Under GDPR: Access (Art. 15), Rectification (Art. 16), Erasure (Art. 17), Restriction (Art. 18), Data portability (Art. 20), Objection (Art. 21).

Direct requests to contact@serahr.de. For data on your own server, you can export or delete data anytime via the admin panel.

8. Right to Complain

You have the right to lodge a complaint with a data protection supervisory authority. The competent authority for Serahr is the **North Rhine-Westphalia Commissioner for Data Protection and Freedom of Information (Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, LDI NRW), Kavalleriestr. 2-4, 40213 Düsseldorf, Germany**.

9. Cookies and Tracking

This website uses no tracking cookies, no third-party trackers, and no analytics tools.

SerahrChat widget: No cookies. Session management uses a JWT token in localStorage. No consent required (§ 25(2)(2) TDDDG — TDDDG replaced the TTDSG on 14.05.2024).

10. Processors and Sub-Processors

SERVICE PROVIDER	PURPOSE	LOCATION
Stripe, Inc.	Payment processing	USA (DPF + SCCs)
Supabase, Inc.	License server backend	USA / EU region (Frankfurt) (DPF + SCCs)
Resend, Inc.	Transactional email	USA (DPF + SCCs)
Vercel, Inc.	License server hosting	USA (DPF + SCCs)
GitHub, Inc.	Update manifest hosting	USA (DPF + SCCs)
netcup GmbH	Web hosting	Germany
Hetzner Online GmbH	Server hosting for the demo chat widget on serahr.de	Germany
OpenRouter Inc.	AI access intermediary for the demo chat widget on serahr.de/chat	USA (DPF + SCCs)
Anthropic PBC	AI language model (Claude) for the demo chat widget on serahr.de/chat	USA (DPF + SCCs)

DPF = EU-U.S. Data Privacy Framework (European Commission adequacy decision of 10 July 2023). For US processors, Standard Contractual Clauses (SCCs) under Art. 46(2)(c) GDPR are additionally in place to ensure protection independent of DPF status.

Note on LLM and embedding providers (customer installations): In a customer-operated installation, LLM and embedding providers (OpenRouter, OpenAI, Mistral, Anthropic, etc.) are not commissioned by us but chosen and configured by the customer (own API key). In this respect the customer acts as controller under the GDPR and is responsible for the data protection assessment of their chosen providers.

Demo chat widget on serahr.de/chat: For the demo widget hosted on the Serahr website, **Anthropic PBC (USA/DPF) via OpenRouter Inc. (USA/DPF)** are active as sub-processors. This applies exclusively to our own demo instance; in customer instances the customer remains responsible for the choice of provider.

Data Processing Agreements (DPAs): Data processing agreements pursuant to Art. 28 GDPR are in place with all processors listed above. These agreements bind the providers to process personal data only on our documented instructions and to implement appropriate technical and organisational measures.

10a. AI Transparency (Art. 50 AI Act)

Pursuant to Art. 50(2) AI Act (Regulation (EU) 2024/1689, transparency duties effective 02.08.2026): **Chatbot answers are AI-generated content**. The demo widget on serahr.de/chat uses a model by Anthropic PBC (Claude, via OpenRouter). In customer installations, the customer chooses the model.

AI outputs are machine-readable labelled (attribute `data-ai-generated="true"` on widget answers) and permanently displayed as AI-generated via a visible badge in the chat widget. The customer may neither remove nor disable this labelling (see Terms § 2).

There is **no automated decision in an individual case** within the meaning of Art. 22(1) GDPR. The AI generates text answers, but these produce neither legal effects nor a similarly significant impact on the end user; they are orientation-only and make no decisions about a user's rights or obligations. The customer or end user reviews the answers on their own responsibility.

This privacy policy may be updated as needed. The current version is always available on this page.

Current version: Version 1.2, effective from 05/19/2026.

Previous Versions

Version 1.1 Valid: 04/16/2026 to 05/19/2026 DE (PDF) EN (PDF)

Version 1.2 Valid: 05/19/2026 to today DE (PDF) EN (PDF)