



[← Back to homepage](#)

# Privacy Policy — Legal Monitor

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

Version 1.2 — effective from 15.04.2026 (legal: Anthropic as sub-processor, AI Art. 50, TDDDG, scanner logs, webhook)

## Table of Contents

1. [Data Controller](#)
2. [Overview: What Data Is Processed?](#)
3. [Legal Basis](#)
4. [AI Processing](#)
5. [Website Scan](#)
6. [Disclosure to Law Enforcement](#)
7. [Processors](#)
8. [Retention](#)
9. [Your Rights and Deletion](#)
10. [Right to Complain](#)
11. [AI Transparency \(Art. 50 AI Act\)](#)
12. [Necessity of Data Provision](#)
13. [Cookies and Tracking](#)
14. [Webhook Notifications](#)

 Chat

## 1. Data Controller

Thorsten Ahrens, Serahr

Email: [contact@serahr.de](mailto:contact@serahr.de)

Website: [serahr.de](https://serahr.de)

## 2. Overview: What Data Is Processed?

Account (email, hashed password, email confirmation timestamp + IP), consent records (accepted AGB/DSE version and timestamp), company profile, data processing details, keywords, website scan data (URL, cookies, third-party services, legal-page extracts, scan authorization confirmation), contract data (subscription status, Stripe IDs, scan tokens), signup source (UTM + referrer, one-time), API key (hashed), webhook URL, payment data (via Stripe), server logs (Vercel IP + request path, 30 days), scanner logs (Hetzner, 14 days).

## 3. Legal Basis

- **Art. 6(1)(b) GDPR** — Contract performance: account, monitoring, scan, webhook calls to customer-configured URLs, Stripe email sync.
- **Art. 6(1)(f) GDPR** — Legitimate interest: server logs, scanner logs, abuse prevention (rate limiting), pseudonymous marketing-channel analysis (UTM/referrer). Balancing results in favor of the processor, because processing is limited to what is technically necessary and does not profile individuals.
- **Art. 6(1)(a) GDPR** — Consent: scan authorization (active confirmation that the customer is authorized to scan the given website).
- **Art. 6(1)(c) GDPR** — Legal obligation: tax retention (§ 147 AO, 10 years for invoices), disclosure to law enforcement under Regulation (EU) 2023/1543.

Legal source analysis uses an AI language model. **Model provider: Anthropic PBC (USA)**. Access is via OpenRouter Inc. (USA) as intermediary. Both are listed as processors in § 7.

**What is transmitted:** public legal texts; anonymized company profile (industry, size — no name, email, or other identifying attributes); aggregated keywords of all active subscribers in **pseudonymized** form (without subscriber attribution). This multi-subscriber aggregation enables cross-topic relevance checks. Therefore do **not** enter confidential or personally identifying terms as keywords.

**What is NOT transmitted:** name, email, company name, payment data, webhook URL, API key, scan URL, raw customer scan results (other than the aggregated pseudonymized inputs above).

**Scanner AI:** During a website scan, scan results (cookies, third-party services, legal-page extracts max. 1500 characters) are sent to the AI model to obtain a structured legal assessment. These data refer exclusively to the website the customer has **authorized to scan** (Terms § 3).

## 5. Website Scan

The scanner uses Playwright/Chromium to visit the customer-provided URL, captures only what a visitor would see, identifies itself as `SerahrLegalMonitor/1.0 (+https://serahr.de/legal-monitor/bot)`, respects `robots.txt`, stores only the first 1500 characters of linked legal pages, blocks internal / cloud metadata endpoints, runs on a Hetzner server in Germany. Scan requires active scan-authorization confirmation (Terms § 3), logged with a timestamp.

## 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 Preservation Order pursuant to



## 7. Processors

Supabase Inc. (database, EU Ireland), Vercel Inc. (hosting + cron, EU Edge), Hetzner Online GmbH (scanner server, Germany), Resend Inc. (email, USA/DPF), Stripe Inc. (payments, USA/DPF), OpenRouter Inc. (AI access intermediary, USA/DPF), **Anthropic PBC (AI language model Claude Sonnet 4, USA/DPF)**. DPAs under Art. 28 GDPR exist with all. SCCs under Art. 46(2)(c) GDPR additionally in place with US processors independent of DPF status.

## 8. Retention

Account data: until deletion + 30-day grace. Company profile: until deletion. Consent records (AGB/DSE version + timestamp, Art. 7(1) GDPR): until deletion + 30 days. Double-opt-in evidence (email-confirmation IP + timestamp, § 7(2)(2) UWG): until deletion + 30 days. Scan results (incl. DSE extract): max 12 months. Monitoring results: max 12 months. Vercel server logs: 30 days. Hetzner scanner logs: 14 days (docker log rotation 3 × 10 MB). Resend delivery logs: up to 180 days per Resend's policy. Stripe transactions: 10 years per § 147 AO (customer removed on deletion; invoices retained for tax). Two automated jobs enforce retention: daily hard-delete for requests > 30 days, monthly purge for expired scan/monitoring data.

## 9. Your Rights and Deletion

Under GDPR: Access (Art. 15), Rectification (Art. 16), Erasure (Art. 17), Restriction (Art. 18), Portability (Art. 20), Objection (Art. 21). **Deletion flow:** via Dashboard → Settings → Delete Account (or email contact@serahr.de); sets `deletion_requested_at` + cancels Stripe subscription immediately; after 30-day grace (export available), account incl. Stripe customer is permanently deleted by the hard-delete cron.



You have the right to lodge a complaint with a data protection supervisory authority.

## 11. AI Transparency (Art. 50 AI Act)

Pursuant to Art. 50(2) AI Act (EU 2024/1689, transparency duties effective 02.08.2026): **All topic summaries, relevance/recommendation outputs and scan assessments generated by the service are AI-generated** (model: Claude Sonnet 4, Anthropic PBC, via OpenRouter). The AI outputs are machine-readable labelled (attribute `data-ai-generated="true"` in emails, "AI" badge in the UI) and post-processed against hard scan facts to reduce obvious hallucinations. No automated decision-making under Art. 22 GDPR. Independent professional review remains necessary.

## 12. Necessity of Data Provision

Email and company profile are required for contract performance (Art. 6(1)(b) GDPR). Keywords, webhook URL, and data-processing details are voluntary.

## 13. Cookies and Tracking

No tracking cookies, no third-party trackers. Auth uses Supabase Auth with secure HTTP cookies (httpOnly, SameSite=Lax). Legal basis for technically necessary cookies: **§ 25 para 2 no 2 TDDDG** (Telecommunications and Digital Services Data Protection Act, replaced TTDSG on 14.05.2024).

## 14. Webhook Notifications

If you configure a webhook URL, we send HTTP POST on new findings: timestamp, your company name, finding status, structured topics. Legal basis: Art. 6(1)(b) GDPR (contract performance). The transfer goes directly from our server to your U



accepted.

## 15. Changes

We reserve the right to update this Policy. Changes will be published on this page.  
Material changes are announced to subscribers by email.

Current version: Version 1.2, effective from 04/15/2026.

### Serahr

Prototyping for software solutions.

#### PRODUCTS

[SerahrRemind](#)

[SerahrChat](#)

[SerahrLegalMonitor](#)

#### LEGAL

[Imprint](#)

[Privacy Policy](#)

[Contact](#)

Our products are intended exclusively for businesses, freelancers, and commercial users (B2B).

© 2026 Thorsten Ahrens. All rights reserved.

 Chat