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 1.0.3 — as of 10.07.2026

Controller: Thorsten Ahrens, Serahr — serahr.de

1. Controller

Thorsten Ahrens, Serahr
Zillestr. 75, 51067 Köln, Germany
E-mail: contact@serahr.de
Full provider details: Imprint

This Privacy Policy applies to the use of the **Serahr Legal Monitor** service. Where data is processed **on behalf of the customer**, the separate Data Processing Agreement governs Art. 28 GDPR obligations.

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. General

We process personal data only as needed to provide the service or under another lawful basis:

- Art. 6(1)(b) GDPR — contract performance.
- Art. 6(1)(c) GDPR — legal obligation (invoice retention).
- Art. 6(1)(f) GDPR — legitimate interest (security logging, audit trail, abuse defense).
- Art. 6(1)(a) GDPR — consent where additionally obtained (e.g. marketing newsletter).

3. Data Categories Processed

3.1 Account master data

- Email, company, country, industry, employee count, revenue range (self-declared).
- Stripe customer ID and subscription data (no card data stored — kept by Stripe).
- Account type, plan, billing interval, period boundaries.
- Retention: until 30 days after account deletion request (see section 7), then cascade hard-delete.

3.2 Authentication data

- Supabase auth user: email + hashed password (never plaintext).
- Session token (HttpOnly cookie); automatic logout after 15 minutes of inactivity.

3.3 Domain and verification data

- Hostname of monitored domain(s).

Verification method (email_match / impressum_mail / meta_tag / dns_txt) and timestamp.

- Verification audit trail (table `lm_verification_attempts`): success/failure, method, anonymized error cause (no PII). Purpose: abuse detection, support.
- Soft-delete state and reminder tracking.
- Retention: until 30 days after domain soft-delete, then hard-delete.

3.4 Scan data

- Scan results linked to the domain.
- URLs visited during scan, HTTP headers, embedded scripts, cookie values (technical data of publicly accessible site).
- Retention: for contract duration. Cascade-deleted on domain or account hard-delete.

3.5 Audit log

- Table `lm_domain_audit`: logs security-relevant lifecycle events.
- Actor (user ID / cron name / webhook source), timestamp, optional metadata.
- Lawful basis: Art. 6(1)(f) GDPR (legitimate interest).
- Retention: until account hard-delete.

3.6 API and webhook configuration

- API keys (account master key on `lm_accounts` and per-domain keys on `lm_domains`) stored in plaintext, RLS-protected (only accessible via service role) and at-rest-encrypted by Supabase. Webhook URL plus webhook secret per domain (HMAC-SHA256 signatures, also plaintext storage).
- Account master key usage timestamp (`api_key_last_used_at`): updated best-effort at most every 60 seconds on each API call. Purpose: forensics on key leak + inactivity indicator in dashboard. No request payload or IP, only the timestamp. Lawful basis Art. 6 (1) f GDPR. Deleted on key rotation or account deletion.
- Rate-limit counters (in-memory, short-lived).

3.7 Email lifecycle

- Transactional emails sent via Resend.
- Soft-delete confirmation includes a JSON attachment with domain configuration (no secrets).

3.8 Server logs

- Standard HTTP access logs by hosting provider (Vercel): time, IP, user-agent, URL.
- Lawful basis: Art. 6(1)(f) GDPR.
- Retention: no longer than 30 days; not systematically linked to account data.

4. Recipients / Sub-Processors

Full list with purpose, location and third-country basis: see DPA section 4. Currently: Vercel (USA), Hetzner (Germany), Supabase (USA / EU data residency), Resend (USA), OpenRouter (USA), Stripe (Ireland).

5. Third-Country Transfers

Where data is transferred to third countries (notably USA), this is based on EU Standard Contractual Clauses and, where applicable, the EU-US Data Privacy Framework.

6. Cookies

Only strictly necessary cookies (session, CSRF) are used — no consent required (§ 25(2)(2) TDDDG). No tracking, analytics or marketing cookies.

7. Retention and Deletion

- **Domain soft-delete:** 30-day grace, then cascade hard-delete.

- **Account soft-delete:** 30-day grace, then hard-delete incl. cascade plus Stripe customer + auth user delete.
- **Verification audit trail:** until account hard-delete.
- **Audit log:** until account hard-delete.
- **Invoices / Stripe data:** 10 years per German tax/commercial law (§§ 147 AO, 257 HGB).

8. Data Subject Rights

You may at any time exercise the following rights:

- **Access** (Art. 15 GDPR).
- **Rectification** (Art. 16 GDPR).
- **Erasure** (Art. 17 GDPR), subject to statutory retention.
- **Restriction** (Art. 18 GDPR).
- **Data portability** (Art. 20 GDPR) — a JSON export of domain configuration is available directly in the dashboard.
- **Object** to processing based on legitimate interest (Art. 21 GDPR).
- **Withdraw consent** with future effect (Art. 7(3) GDPR).
- **Complaint** to a supervisory authority (Art. 77 GDPR) — competent for our seat in Köln: Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen.

9. Demo Report

On the public landing page we offer a sample compliance report at `/api/legal-monitor/demo-report` containing **fictional data only**("Muster GmbH"), delivered without authentication.

10. Anonymous Statistical Analysis

We analyze scan results in **anonymized, non-reidentifiable form** to produce industry-country-level statistics on GDPR compliance, improve the product, and publish aggregated industry reports for marketing and PR purposes.

What is aggregated (table `lm_study_aggregates`): industry, country, scan month, boolean flags (imprint/privacy/cookie banner present yes/no), numeric counts (cookies, third-party requests, imprint and privacy issues) and the numeric AI compliance score. **NO** hostname, **NO** account or domain ID, **NO** link back to your account.

Anonymity threshold: Publications from this aggregation occur only for bucket combinations with at least ten data points (k≥10 anonymity per Article 29 Working Party Opinion 05/2014). Smaller buckets are merged into the next coarser category or not published.

Legal basis: Art. 6(1)(f) GDPR (legitimate interest — product improvement, public industry statistics). Since the aggregated values no longer constitute personal data, further processing falls outside the scope of the GDPR per Art. 4(1) and Recital 26.

Retention: Aggregates are retained indefinitely as they no longer constitute personal data after anonymization.

Opt-out: You may opt out at any time under *Account → Settings → Statistical Analysis*. After activation no further aggregate entries from your scans are written. Aggregates already produced remain unaffected (no personal data → no deletion obligation under Art. 17 GDPR).

10a. Use of AI and automated decisions

We use AI models to prepare and prioritize scan findings and legal topics (accessed via the sub-processor OpenRouter, see section 4). AI-assisted evaluations (e.g. finding summaries, AI compliance score) are informational only.

There is **no automated decision in an individual case** within the meaning of Art. 22(1) GDPR: the evaluations produce neither legal effects nor a similarly significant impact; they make no decisions about rights or obligations. Reviewing and acting on findings remains the customer's responsibility.

Technical-organizational measures per Art. 32 GDPR; details in the DPA appendix. Key measures: TLS for all transfers, hashed passwords (Supabase Auth, bcrypt) and plaintext API keys with RLS/service-role restriction, HMAC-SHA256-signed webhooks, account-scoping (row-level security), audit log, API rate-limiting, automatic logout after 15 minutes of inactivity.

12. Changes to this Privacy Policy

We may amend this Privacy Policy in case of material changes to processing. Material changes are notified by email to existing customers at least six weeks in advance. Earlier versions remain in the archive at the bottom of this page.

13. Contact

For questions or to exercise your rights: contact@serahr.de

Current version: Version 1.0.3, effective from 07/10/2026.

Previous Versions

Version 1.0.0 Valid: 05/01/2026 to 05/19/2026 DE (PDF) EN (PDF)

Version 1.0.1 Valid: 05/19/2026 to 05/31/2026 DE (PDF) EN (PDF)

Version 1.0.2 Valid: 05/31/2026 to 07/10/2026 DE (PDF) EN (PDF)

Version 1.0.3 Valid: 07/10/2026 to today DE (PDF) EN (PDF)

Serahr

Prototyping for software solutions.

Current study: GDPR status check 2026 →

PRODUCTS

SerahrRemind Privacy Policy

SerahrChat
Terms | Privacy Policy

SerahrLegalMonitor
Terms | Privacy Policy | DPA

SerahrUHU
Terms | Privacy Policy

LEGAL

Imprint

Privacy Policy

Contact

SISTER SITES

kineangst.de — AI risk assessment by profession

kineahnung.de — AI tools by profession

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