Zurück zur Startseite

Datenschutzerklärung — Legal Monitor

Version 1.0.2 — Stand 31.05.2026

Verantwortlich: Thorsten Ahrens, Serahr — serahr.de

1. Verantwortlicher

Thorsten Ahrens, Serahr
Zillestr. 75, 51067 Köln, Deutschland
E-Mail: contact@serahr.de
Vollständige Anbieterangaben: Impressum

Diese Datenschutzerklärung gilt für die Nutzung des Dienstes **Serahr Legal Monitor** (Domain legalmonitor.serahr.de und zugehörige API/Webhook-Endpunkte). Soweit Daten **im Auftrag des Kunden**verarbeitet werden, regelt die zusätzlich abgeschlossene Auftragsverarbeitungsvereinbarung die Pflichten gemäß Art. 28 DSGVO.

1a. Datenschutzbeauftragter

Wir haben keinen Datenschutzbeauftragten bestellt. Eine Pflicht zur Bestellung nach Art. 37 DSGVO besteht für uns nicht, da wir weder Verarbeitungen besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO) in großem Umfang noch eine systematische Überwachung Betroffener durchführen und weniger als 20 Personen

ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind. Anfragen zum Datenschutz richten Sie bitte direkt an contact@serahr.de.

2. Allgemeines

Wir verarbeiten personenbezogene Daten nur, soweit dies zur Erbringung des Dienstes erforderlich ist oder eine andere Rechtsgrundlage greift. Maßgebliche Rechtsgrundlagen sind insbesondere:

- Art. 6 Abs. 1 lit. b DSGVO — Vertragserfüllung (Account, Domain-Monitoring, Abrechnung).
- Art. 6 Abs. 1 lit. c DSGVO — gesetzliche Pflicht (Aufbewahrung von Rechnungen).
- Art. 6 Abs. 1 lit. f DSGVO — berechtigtes Interesse (Logging zur Sicherheit, Audit-Trail, Missbrauchsabwehr).
- Art. 6 Abs. 1 lit. a DSGVO — Einwilligung, soweit zusätzlich eingeholt (z.B. Marketing-Newsletter).

3. Verarbeitete Datenarten

3.1 Account-Stammdaten

- E-Mail-Adresse, Firma, Land, Branche, Mitarbeiterzahl, Umsatzklasse (selbstangegeben).
- Stripe-Customer-ID und zugehörige Subscription-Daten (kein Speichern von Kartendaten — diese verbleiben bei Stripe).
- Account-Typ (solo / agency), Plan, Abrechnungsintervall, Periodengrenzen.
- Speicherdauer: bis 30 Tage nach Account-Löschungswunsch (siehe Abschnitt 7), danach Hard-Delete inkl. Cascade.

3.2 Authentifizierungsdaten

Auth-User in Supabase: E-Mail + Passwort-Hash (gehasht, nie im Klartext gespeichert).

- Session-Token (HttpOnly-Cookie); automatischer Logout nach 15 Minuten Inaktivität.
- Speicherdauer: bis Account-Löschung; Sessions verfallen nach Inaktivität.

3.3 Domain- und Verifikationsdaten

- Hostname der überwachten Domain(s).
- Verifikationsmethode (email_match, impressum_mail, meta_tag, dns_txt) und Zeitpunkt der Verifikation.
- Verifikations-Audit-Trail (Tabelle `lm_verification_attempts`): erfolgreiche und fehlgeschlagene Versuche, Methode, anonymisierte Fehlerursache (kein PII). Zweck: Missbrauchserkennung, Support.
- Soft-Delete-Status (`deletion_requested_at`, `deletion_reason`) und Reminder-Tracking.
- Speicherdauer: bis 30 Tage nach Domain-Soft-Delete, danach Hard-Delete.

3.4 Scan-Daten

- Scan-Ergebnisse (Befunde zu Cookies, Tracking, Impressum, Datenschutzerklärung, AGB) verknüpft mit der Domain.
- Aufgerufene URLs während des Scans, HTTP-Header, eingebundene Skripte, Cookie-Werte (technische Daten der öffentlich zugänglichen Site).
- Speicherdauer: für die Dauer des Vertrags. Beim Domain-Hard-Delete oder Account-Hard-Delete werden die Scan-Daten via Cascade gelöscht.

3.5 Audit-Log

- Tabelle `lm_domain_audit`: protokolliert sicherheitsrelevante Lifecycle-Events (Soft-Delete, Restore, Hard-Delete, Domain-Wechsel, Add-On-Aktionen, Stripe-Quantity-Änderungen).

Akteur-Klassifizierung (User-ID, Cron-Name oder Webhook-Quelle), Zeitstempel, optionale Metadaten.

- Rechtsgrundlage: Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse: Nachvollziehbarkeit, Forensik).
- Speicherdauer: bis Account-Hard-Delete; einzelne Einträge können auf Antrag früher gelöscht werden, soweit keine Sicherheitsinteressen entgegenstehen.

3.6 API- und Webhook-Konfiguration

- API-Keys (Account-Master-Key auf `lm_accounts` sowie pro-Domain-Keys auf `lm_domains`) im Klartext gespeichert, RLS-geschützt (nur über Service-Role-Client zugreifbar) und at-rest-verschlüsselt durch Supabase. Webhook-URL plus Webhook-Secret pro Domain (für HMAC-SHA256-Signaturen, ebenfalls Klartext-Speicherung).
- Nutzungs-Zeitstempel des Account-Master-Keys (`api_key_last_used_at`): wird bei jedem API-Aufruf maximal alle 60 Sekunden best-effort aktualisiert. Zweck: Forensik bei Schlüsselleak + Inaktivitäts-Anzeige im Dashboard. Keine Anfrageinhalte oder IP-Adressen, nur Zeitstempel. Rechtsgrundlage Art. 6 Abs. 1 lit. f DSGVO. Wird bei Schlüsselrotation oder Account-Löschung mit gelöscht.
- Rate-Limit-Counter (im Speicher, kurzlebig).
- Speicherdauer: bis Domain-Löschung oder explizite Rotation durch den Kunden.

3.7 E-Mail-Lifecycle

- Transaktionsmails (Account-Bestätigung, Domain-Verifikation, Soft-Delete-Bestätigung + 7d/1d Reminder, Verify-Timeout, Welcome) werden über Resend versendet.
- Empfängerin: jeweilige Account-E-Mail bzw. die für die Verifikation hinterlegte Adresse.
- Inhalt enthält bei Soft-Delete einen JSON-Anhang mit der Domain-Konfiguration (ohne API-Key, ohne Webhook-Secret).

3.8 Server-Logs

Beim Aufruf der Web-Anwendung speichert unser Hosting-Anbieter (Vercel) standardmäßig HTTP-Zugriffsdaten (Zeitpunkt, IP-Adresse, User-Agent, aufgerufene URL).

- Rechtsgrundlage: Art. 6 Abs. 1 lit. f DSGVO (Sicherheit, Stabilität, Missbrauchsabwehr).
- Speicherdauer gemäß Vercel-Default; eine Verknüpfung mit Account-Daten erfolgt nicht systematisch.

4. Empfänger / Sub-Auftragsverarbeiter

Wir setzen sorgfältig ausgewählte Sub-Auftragsverarbeiter ein. Die vollständige Liste mit Zweck, Sitz und Rechtsgrundlage für Drittlandübermittlungen findet sich in der Auftragsverarbeitungsvereinbarung, Abschnitt 4. Aktuell:

- **Vercel Inc.** (USA) — Hosting der Web-Anwendung. SCC + EU-US Data Privacy Framework.
- **Hetzner Online GmbH** (Deutschland) — Scanner-Infrastruktur. Innerhalb EU.
- **Supabase Inc.** (USA, Datenhaltung in EU-Region Irland, eu-west-1) — Datenbank, Auth, Storage. SCC.
- **Resend** (USA) — E-Mail-Versand. SCC + EU-US Data Privacy Framework.
- **OpenRouter** (USA) — KI-Routing für Befund-Analyse. SCC, Zero-Data-Retention konfiguriert (X-OR-Provider-Setting `data_collection: deny`; eingesehene Vereinbarung über contact@serahr.de auf Anfrage).
- **Stripe Payments Europe Ltd.** (Irland) — Zahlungsabwicklung. Innerhalb EU.

5. Drittlandübermittlung

Soweit personenbezogene Daten in Drittländer (insbesondere USA) übermittelt werden, erfolgt dies auf Basis der EU-Standardvertragsklauseln und — wo anwendbar — des EU-US Data Privacy Frameworks. Eine Übersicht der Maßnahmen findet sich in der AVV.

6. Cookies und vergleichbare Technologien

Wir setzen ausschließlich technisch notwendige Cookies (Session-Cookies, CSRF-Schutz). Diese sind ohne Einwilligung zulässig (§ 25 Abs. 2 Nr. 2 TDDDG). Tracking-, Analyse- oder Marketing-Cookies werden nicht eingesetzt.

7. Speicherdauer und Löschung

- **Domain-Soft-Delete:** 30-Tage-Frist, danach Cascade-Hard-Delete der Domain inkl. zugehöriger Scan-Daten.
- **Account-Soft-Delete:** 30-Tage-Frist, danach Hard-Delete inkl. lm_users, lm_domains, lm_scans, lm_account_resolved (Cascade) sowie Stripe-Customer-Delete und Auth-User-Delete.
- **Verifikations-Audit-Trail:** bis Account-Hard-Delete (Cascade über account_id-FK).
- **Audit-Log:** bis Account-Hard-Delete; einzelne Einträge auf Antrag löschbar, soweit keine Sicherheitsinteressen entgegenstehen.
- **Rechnungen / Stripe-Daten:** 10 Jahre gemäß §§ 147 AO, 257 HGB (gesetzliche Aufbewahrungspflicht — überdauert die Account-Löschung).

8. Rechte der betroffenen Person

Sie haben jederzeit folgende Rechte:

- **Auskunft** über die zu Ihrer Person gespeicherten Daten (Art. 15 DSGVO).
- **Berichtigung** unrichtiger Daten (Art. 16 DSGVO).
- **Löschung** Ihrer Daten (Art. 17 DSGVO), soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.
- **Einschränkung** der Verarbeitung (Art. 18 DSGVO).
- **Datenübertragbarkeit** (Art. 20 DSGVO) — ein JSON-Export der Domain-Konfiguration ist im Dashboard direkt verfügbar.

- **Widerspruch** gegen Verarbeitung auf Basis berechtigten Interesses (Art. 21 DSGVO).
- **Widerruf** erteilter Einwilligungen mit Wirkung für die Zukunft (Art. 7 Abs. 3 DSGVO).
- **Beschwerde** bei einer Aufsichtsbehörde (Art. 77 DSGVO) — für unseren Sitz in Köln zuständig: Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen.

9. Demo-Report

Auf der öffentlichen Landing-Page bieten wir unter `/api/legal-monitor/demo-report` einen Beispiel-Compliance-Report an. Dieser enthält ausschließlich **fiktive Daten**(„Muster GmbH“) und wird ohne Authentifizierung ausgeliefert. Beim Aufruf erhebt unser Hosting-Anbieter standardmäßige Zugriffsdaten (siehe 3.8); eine Verknüpfung mit Account-Daten findet nicht statt.

10. Anonyme statistische Auswertung

Wir werten Ergebnisse durchgeführter Scans in **anonymisierter, nicht reidentifizierbarer Form** aus, um Branchen- und Länder-Statistiken zur DSGVO-Compliance zu erstellen, das Produkt zu verbessern und aggregierte Branchenberichte für Marketing- und PR-Zwecke zu veröffentlichen.

Was aggregiert wird (Tabelle `lm_study_aggregates`): Branche, Land, Monat des Scans, Boolean-Flags (Impressum/DSE/Cookie-Banner gefunden ja/nein), numerische Counts (Anzahl Cookies, Drittanbieter-Requests, Impressum-/DSE-Befunde) und der numerische AI-Compliance-Score. **KEIN** Hostname, **KEIN** Account- oder Domain-ID, **KEIN** Bezug zu Ihrem Account.

Anonymität-Schwelle: Veröffentlichungen aus dieser Aggregation erfolgen ausschließlich für Bucket-Kombinationen mit mindestens zehn Datenpunkten (k≥10-Anonymität nach Art. 29-Datenschutzgruppe Opinion 05/2014). Kleinere Buckets werden zur nächsten gröberen Kategorie zusammengefasst oder nicht veröffentlicht.

Rechtsgrundlage: Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse — Produktverbesserung, öffentliche Branchen-Statistik). Da die aggregierten Werte keinen Personenbezug mehr aufweisen, fällt die weitere Verarbeitung gemäß Art. 4 Nr. 1 DSGVO und Erwägungsgrund 26 nicht mehr in den Anwendungsbereich der DSGVO.

Speicherdauer: Aggregate werden zeitlich unbegrenzt gespeichert, da sie nach Anonymisierung keine personenbezogenen Daten mehr darstellen.

Widerspruch (Opt-Out): Sie können der Auswertung jederzeit widersprechen unter *Account → Einstellungen → Statistische Auswertung*. Ab Aktivierung des Widerspruchs erfolgt kein weiterer Aggregat-Eintrag aus Ihren Scans. Bereits zuvor erstellte, anonymisierte Aggregate bleiben unberührt (kein Personenbezug → keine Löschpflicht nach Art. 17 DSGVO).

11. Sicherheit

Wir treffen technisch-organisatorische Maßnahmen gemäß Art. 32 DSGVO. Eine ausführliche Beschreibung findet sich im AVV-Anhang. Wesentliche Maßnahmen: TLS für alle Datenübertragungen, gehasht gespeicherte Passwörter (Supabase-Auth, bcrypt) und Klartext-API-Keys mit RLS- und Service-Role-Beschränkung, HMAC-SHA256-signierte Webhooks, Account-Scoping in der Datenbank (Row-Level-Security), Audit-Log sicherheitsrelevanter Aktionen, Rate-Limiting auf API-Endpunkten, automatischer Logout nach 15 Minuten Inaktivität.

12. Änderungen dieser Datenschutzerklärung

Wir können diese Datenschutzerklärung bei wesentlichen Änderungen der Verarbeitung anpassen. Maßgeblich ist jeweils die zum Zeitpunkt der Datenerhebung gültige Fassung. Wesentliche Änderungen kommunizieren wir mit mindestens sechs Wochen Vorlauf per E-Mail an Bestandskunden. Frühere Versionen sind im Versions-archiv am Ende dieser Seite abrufbar.

Bei Fragen zur Verarbeitung Ihrer Daten oder zur Ausübung Ihrer Rechte:
contact@serahr.de

Aktuelle Fassung: Version 1.0.2, gültig ab 31.05.2026.

Frühere Fassungen

Version 1.0.0 Gültig: 01.05.2026 bis 19.05.2026 DE (PDF) EN (PDF)

Version 1.0.1 Gültig: 19.05.2026 bis 31.05.2026 DE (PDF) EN (PDF)