Zurück zur Startseite

AV-Vertrag — Legal Monitor

Version 1.0.0 — Stand 01.05.2026

Anbieter: Thorsten Ahrens, Serahr — serahr.de

1. Gegenstand und Geltung

Diese Vereinbarung über die Auftragsverarbeitung (im Folgenden „AVV") konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien gemäß Art. 28 DSGVO im Rahmen der Nutzung des Dienstes Legal Monitor (im Folgenden „Dienst") durch den Kunden. Sie gilt automatisch mit Abschluss des Hauptvertrags (AGB Legal Monitor) als Bestandteil dieses Vertrags ohne separate Unterschrift.

Verantwortlicher im Sinne der DSGVO ist der Kunde. Auftragsverarbeiter ist der Anbieter (Serahr / Thorsten Ahrens).

2. Gegenstand der Verarbeitung

- **Zweck:** Automatisiertes Monitoring der vom Kunden registrierten Domains auf datenschutz- und rechtsrelevante technische Auffälligkeiten (Cookies, Tracking-Skripte, Impressum, Datenschutzerklärung, AGB); regelmäßige Berichte; Webhook-/API-Auslieferung der Befunde.
- **Art der Daten:** Domain-Hostname, technische Konfiguration der Site (HTTP-Header, eingebundene Skripte, Cookie-Werte), Account-Stammdaten des Kunden (Firma, Email, Rechnungsdaten), Login-Daten der Nutzer des Dienstes, Scan-Ergebnisse (Befunde, KI-generierte Hinweise).

- **Betroffene Personen:** Mitarbeiter und Geschäftsführer des Kunden, gegebenenfalls Endnutzer der gescannten Site (technische Daten, soweit sie beim Scan eines öffentlich zugänglichen Bereichs der Site anfallen).
- **Dauer:** für die Dauer des Vertragsverhältnisses, anschließend Löschung nach Maßgabe der gesetzlichen Aufbewahrungsfristen (siehe Datenschutzerklärung).

3. Pflichten des Anbieters

- Verarbeitung ausschließlich auf Weisung des Kunden, im durch diese AVV und die AGB definierten Rahmen.
- Vertraulichkeitsverpflichtung aller mit der Verarbeitung betrauten Personen.
- Technisch-organisatorische Maßnahmen gemäß Anhang am Ende dieser AVV.
- Unterstützung des Kunden bei Anfragen Betroffener: für die Datenportabilität (Art. 20 DSGVO) steht ein JSON-Export der Domain-Konfiguration unmittelbar im Dashboard zur Verfügung. Compliance-Reports sind als HTML/PDF herunterladbar.
- Lifecycle-Events (Soft-Delete, Restore, Hard-Delete, Domain-Wechsel, Add-On-Aktionen, Stripe-Quantity-Änderungen) werden in der Tabelle `lm_domain_audit` protokolliert, um Nachvollziehbarkeit für Audits durch den Kunden sicherzustellen. Verifikations-Versuche werden in `lm_verification_attempts` ohne PII geloggt (Methode, anonymisierte Fehlerursache).
- Unverzügliche Meldung von Datenschutzverletzungen, spätestens innerhalb von 72 Stunden nach Kenntniserlangung.
- Löschung oder Rückgabe sämtlicher Daten nach Vertragsende: für Domains gilt eine 30-tägige Soft-Delete-Frist (in der Reports/JSON-Export weiterhin abrufbar sind), danach Cascade-Hard-Delete. Für Accounts greift dieselbe 30-tägige Frist; nach Ablauf werden Account-Daten, Stripe-Customer und Auth-User unwiderruflich gelöscht, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

4. Sub-Auftragsverarbeiter

Der Kunde stimmt der Hinzuziehung der nachfolgend aufgeführten Sub-Auftragsverarbeiter zu. Bei Wechsel oder Hinzuziehung weiterer Sub-Auftragsverarbeiter wird der Kunde mit angemessener Frist (mindestens 14 Tage) per E-Mail informiert; ein Widerspruchsr
wichtigem Grund bleibt vorbehalten.

B-FTRAGSVERARBEITER	ZWECK	SITZ	RECHTSGRUNDLAGE DRITTLAND
Vercel Inc.	Hosting der Web-Anwendung (App-Server, statische Assets)	USA (Sitz); Verarbeitung auch über EU-Edge (Frankfurt)	EU-Standardvertragsklauseln + EU-US Data Privacy Framework
Hetzner Online GmbH	Scanner-Infrastruktur (Cloud-Server für Domain-Scans)	Deutschland	Innerhalb EU — keine Drittlandübermittlung
Supabase Inc.	Datenbank, Authentifizierung, Storage	USA (Datenhaltung in EU-Region: Irland/Frankfurt)	EU-Standardvertragsklauseln, Datenhaltung ausschließlich EU
Resend	Transaktionale E-Mail-Auslieferung (Bestätigungs-, System-Mails)	USA	EU-Standardvertragsklauseln + EU-US Data Privacy Framework
OpenRouter	KI-gestützte Analyse von Scan-Befunden (Routing zu LLM-Anbietern wie Anthropic, OpenAI)	USA (Routing-Anbieter)	EU-Standardvertragsklauseln, kein Modell-Training auf Kundendaten (Zero Data Retention vereinbart)
Stripe Payments Europe Ltd.	Zahlungsabwicklung, Rechnungsverwaltung	Irland (EU)	Innerhalb EU — keine Drittlandübermittlung

5. Pflichten des Kunden

- Der Kunde ist verantwortlicher Eigentümer der von ihm registrierten Domain. Er bestätigt durch Domain-Verifikation, dass er berechtigt ist, die Domain überwachen zu lassen.
- Der Kunde stellt sicher, dass die Verarbeitung der von ihm bereitgestellten oder über den Dienst erhobenen Daten rechtmäßig erfolgt (Rechtsgrundlage, Information seiner Betroffenen, ggf. Einwilligung).
- Bei Multi-Domain-Nutzung (Agentur-Tarif) gewährleistet der Kunde, dass die nötigen vertraglichen Grundlagen mit seinen Mandanten bestehen (eigene AVV zwischen Kunde und Mandant; diese AVV bildet die unterlagerte Stufe).

- Anforderung von Auskünften über die Verarbeitung der ihn betreffenden Daten.
- Anforderung einer Bestätigung über die Einhaltung dieser Vereinbarung (Audit-Recht; Anbieter kann auf bestehende Zertifizierungen oder Auditberichte verweisen).
- Recht zur Kündigung dieses Vertrags bei wesentlicher Verletzung; Kündigung erfolgt schriftlich (E-Mail genügt).

7. Haftung

Es gilt die Haftungsregelung der AGB Legal Monitor. Insbesondere haftet der Anbieter nicht für Folgen, die sich aus der Umsetzung oder Nicht-Umsetzung der vom Dienst gelieferten Befunde durch den Kunden ergeben — der Dienst ist Informationsdienstleister, keine Rechtsdienstleistung im Sinne des RDG.

8. Schlussbestimmungen

Es gilt deutsches Recht. Gerichtsstand ist Köln, soweit gesetzlich zulässig. Sollte eine Bestimmung dieser AVV unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Anhang: Technisch-organisatorische Maßnahmen (Art. 32 DSGVO)

- **Vertraulichkeit:** Zugangskontrolle (Multi-Factor-Authentifizierung), Zugriffskontrolle (Role-Based Access, Service-Role-Trennung), Trennungskontrolle (Mandantenfähigkeit über Account-Scoping in Datenbank).
- **Integrität:** Eingabekontrolle (Audit-Log für sicherheitsrelevante Aktionen), Weitergabekontrolle (TLS für alle Datenübertragungen), Hash-basierte Token (HMAC-SHA256 für Webhook-Signaturen).
- **Verfügbarkeit:** Tägliche automatische Backups durch Sub-Auftragsverarbeiter (Supabase), Verfügbarkeits-Monitoring, georedundante Hosting-Infrastruktur.

- **Belastbarkeit:** Zonenredundante Datenbank (Supabase), DDoS-Schutz auf Anwendungsschicht (Vercel), Rate-Limiting auf API-Endpunkten.
- **Wiederherstellung:** Point-in-Time-Recovery der Datenbank (7 Tage), Restore-Prozesse dokumentiert.
- **Verfahren zur regelmäßigen Überprüfung:** Logging sicherheitsrelevanter Ereignisse, periodische Audit-Log-Auswertung, jährliche Sub-Auftragsverarbeiter-Prüfung.

Aktuelle Fassung: Version 1.0.0, gültig ab 01.05.2026.

Frühere Fassungen

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