Back to homepage

DPA — Legal Monitor

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

Version 1.0.1 — as of 31.05.2026

Provider: Thorsten Ahrens, Serahr — serahr.de

1. Subject and Scope

This Data Processing Agreement ("DPA") governs the parties' data protection obligations under Art. 28 GDPR in the context of using the Legal Monitor service. It becomes part of the main contract (Legal Monitor Terms) upon acceptance of those Terms — no separate signature required.

Controller within the meaning of GDPR is the customer. Processor is the provider (Serahr / Thorsten Ahrens).

2. Subject of Processing

- **Purpose:** automated monitoring of customer-registered domains for privacy and legal-relevant findings (cookies, tracking scripts, imprint, privacy policy, terms); regular reports; webhook/API delivery of findings.

- **Type of data:** domain hostname, technical configuration of the site, customer account master data, login data of service users, scan results.
- **Affected persons:** employees and managing directors of the customer; possibly end-users of the scanned site (technical data only, from publicly accessible site sections).
- **Duration:** for the duration of the contract; subsequent deletion subject to statutory retention obligations.

3. Provider's Obligations

- Processing only on customer instructions, within the framework defined by this DPA and the Terms.
- Confidentiality obligation of all persons involved in processing.
- Technical-organizational measures per the appendix.
- Support for customer with data subject requests: portability (Art. 20 GDPR) is supported via in-dashboard JSON export of domain configuration; compliance reports available as HTML/PDF download.
- Lifecycle events (soft-delete, restore, hard-delete, domain change, add-on actions, Stripe quantity changes) are logged in `lm_domain_audit` for customer audit traceability. Verification attempts are logged without PII in `lm_verification_attempts` (method, anonymized error cause).
- Immediate notification of personal data breaches, at the latest within 72 hours of awareness.
- Deletion or return of all data after end of contract: domains follow a 30-day soft-delete grace (reports + JSON export remain available), then cascade hard-delete. Accounts follow the same 30-day grace; thereafter account data, Stripe customer and auth user are permanently deleted, subject to statutory retention.

4. Sub-Processors

Customer consents to engagement of the sub-processors listed below. Customer will be informed by email with adequate notice (at least 14 days) of changes; right to object on important grounds is reserved.

SUB-PROCESSOR	PURPOSE	LOCATION	LEGAL BASIS
Vercel Inc.	Hosting (web + API)	USA (HQ); processing also via EU edge (Frankfurt)	DPA with EU SCCs
Hetzner Online GmbH	Scanner container hosting	Germany	DPA (Art. 28 GDPR)
Supabase Inc.	Database, authentication	EU (Ireland, eu-west-1)	DPA with EU SCCs
Resend, Inc.	Email delivery	US	DPA with EU SCCs
OpenRouter Inc.	AI scan analysis	US	DPA with EU SCCs, ZDR (data_collection: deny)
Stripe Payments Europe Ltd.	Payment processing	Ireland	DPA with EU SCCs

In case of doubt the German version of this DPA is the legally binding text; the English version is provided for convenience.

5. Customer's Obligations

- Customer is responsible owner of registered domain; confirms via domain verification.
- Customer ensures lawful processing of data provided to or collected by the service.
- Multi-domain usage (agency tier): customer ensures contractual basis with their clients (separate DPA between customer and client; this DPA forms the underlying tier).

- Request information about processing of customer-related data.
- Request confirmation of compliance (audit right; provider may refer to existing certifications or audit reports).
- Right to terminate this contract for material breach; written form (email sufficient).

7. Liability

The liability provisions of the Legal Monitor Terms apply. In particular, the provider is not liable for consequences arising from customer's implementation or non-implementation of findings delivered by the service — the service is an information provider, not a legal service within the meaning of the German Legal Services Act (RDG).

8. Final Provisions

German law applies. Place of jurisdiction is Köln where legally permissible. Severability clause applies.

Appendix: Technical-Organizational Measures (Art. 32 GDPR)

- **Confidentiality:** access control (MFA), authorization control (role-based access, service-role separation), tenant isolation (account-scoping in database).
- **Integrity:** input control (audit log for security-relevant actions including account-master-key lifecycle), transmission control (TLS for all data transfers), HMAC-SHA256 for webhook signatures. API keys are stored in plaintext but RLS-protected (service-role-only access) and at-rest-encrypted by Supabase.
- **Availability:** daily automated backups via sub-processor (Supabase), availability monitoring, geo-redundant hosting infrastructure.

Resilience: zone-redundant database (Supabase), DDoS protection at application layer (Vercel), rate-limiting on API endpoints.

- **Recovery:** Point-in-time recovery of database (7 days), restore processes documented.
- **Regular review procedures:** logging of security-relevant events, periodic audit-log review, annual sub-processor review.

Current version: Version 1.0.1, effective from 05/31/2026.

Previous Versions

Version 1.0.0	Valid: 05/01/2026 to 05/31/2026	DE (PDF)	EN (PDF)