Data Processing Agreement (DPA / AVV)

Last updated: 13 July 2026

This Data Processing Agreement (the "DPA" or "Auftragsverarbeitungsvertrag / AVV") is concluded pursuant to Art. 28 GDPR between you, the customer using the FAIND services (the "Customer"), and leif ventures UG (haftungsbeschränkt) ("FAIND", "we", "us"). It forms part of, and is governed by, our Terms of Service and supplements our Privacy Policy. It sets out the terms on which we process personal data on the Customer's behalf when providing the Agentic Web CDN / Knowledge Graph and the associated site snippet for the Customer's publicly accessible pages. For a plain-language description of exactly what the snippet does and does not read, write and transmit, see Snippet Data Statement.

1) Parties and roles

The Customer is the controller (Art. 4(7) GDPR) with respect to the personal data processed through the FAIND services in connection with the Customer's own website and Knowledge Graph pages. FAIND is the processor (Art. 4(8) GDPR) acting on the Customer's behalf.

- Processor: leif ventures UG (haftungsbeschränkt), Karl-Marx-Str. 250, 12057 Berlin, Germany. Commercial Register HRB 170145 B, Amtsgericht Charlottenburg. Represented by Leif Pritzel. Email privacy@getfaind.com. VAT ID DE344532119.
- Processor's privacy contact: Leif Pritzel (no Data Protection Officer is appointed, as one is not legally required).
- Controller: the Customer, as identified in the applicable order or account registration.

Where the Customer is itself a processor acting for its own client, references to "controller" apply to that arrangement mutatis mutandis, and the Customer warrants it is authorized to instruct FAIND accordingly.

2) Subject-matter, duration, nature and purpose of processing

- Subject-matter: processing of personal data that occurs when FAIND operates the Agentic Web CDN / Knowledge Graph (an AI-optimized static mirror of the Customer's publicly accessible pages) and the one-line site snippet embedded on the Customer's website.
- Nature of processing: receiving, transmitting, analyzing, structuring, storing, hosting via CDN, aggregating and deleting the data described in Section 3, by automated means.
- Purpose: generating and maintaining the Customer's Knowledge Graph; detecting when the Customer's public pages change so the Knowledge Graph stays current; measuring AI-driven visits and bot-vs-human traffic to those pages in aggregate; and delivering the contracted AI-visibility services. FAIND does not build visitor profiles and does not use the data for its own purposes.
- Duration: for the term of the main agreement (the Customer's subscription), plus the deletion or return period set out in Section 11.

3) Categories of data subjects and categories of personal data

Categories of data subjects:

- Visitors to the Customer's website on which the snippet is embedded, and visitors to the Customer's Knowledge Graph / CDN pages.

Categories of personal data. The snippet stores nothing on and reads nothing from the visitor's device (no cookies, no localStorage, no sessionStorage, no IndexedDB, no device or browser fingerprinting). It reads the Customer's own page content, not visitor-entered data or form inputs. The only elements that could relate to a person are transient technical request metadata:

- IP address: inherent to any HTTP request (as with any embedded resource); used transiently to serve the request and to classify bot-vs-human traffic. It is not stored as an identifier and the raw IP is not stored in the analytics.
- User-agent string: inherent to any HTTP request; used only to classify bot-vs-human. The raw user-agent is not stored — only the derived category is retained.

- Page URL / path of the Customer's own pages: arbitrary or personal-data query parameters are stripped in the browser before transmission; only a small set of functional parameters (e.g. page/sort/filter/q/category) is kept.
- Technical content signals derived from the Customer's own public page content, used only to detect when that content changes. These are not visitor data.

Not processed under this DPA: no stored visitor identifier, no cross-site tracking identifier, no cookies, no form inputs or input values, and no special-category data (Art. 9) or data relating to criminal convictions (Art. 10). The Customer must not instruct FAIND to process such categories through the services.

The server-side records derived from the above are aggregated and page-level: they contain no per-visitor rows, no raw IP and no raw user-agent. Further plain-language detail is set out in the Snippet Data Statement and summarized in Annex A.

4) Processing on documented instructions

FAIND processes personal data only on the Customer's documented instructions, including with regard to international transfers, unless required to do so by Union or Member-State law to which FAIND is subject; in that case FAIND informs the Customer of that legal requirement before processing, unless the law prohibits such information on important grounds of public interest.

- Documented instructions: this DPA, the Terms of Service, the Customer's configuration of the services (e.g. connecting a domain, embedding the snippet), and any further written instructions the Customer gives.
- If FAIND believes an instruction infringes the GDPR or other applicable data-protection law, it will inform the Customer without undue delay (Art. 28(3), second sentence).

5) Confidentiality

FAIND ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and that access is limited to personnel who need it to provide the services.

6) Security of processing (Art. 32)

FAIND implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing. The measures in force are described in Annex C and are reviewed and updated as appropriate. FAIND may update specific measures over time provided the overall level of protection is not reduced.

7) Sub-processors

The Customer grants FAIND general written authorization to engage sub-processors for the provision of the services. The current sub-processors are listed in Annex B.

- Change notice: FAIND informs the Customer of any intended addition or replacement of a sub-processor at least 30 days in advance, by email, during which the Customer may object on reasonable data-protection grounds.
- Objection: if the Customer reasonably objects and the parties cannot agree on a resolution, the Customer may terminate the affected part of the services.
- Flow-down: FAIND imposes on each sub-processor, by contract, data-protection obligations that are essentially equivalent to those in this DPA (Art. 28(4)), and remains fully liable to the Customer for the sub-processor's performance of those obligations.

8) Assistance with data-subject requests

Taking into account the nature of the processing, FAIND assists the Customer by appropriate technical and organizational measures, insofar as this is possible, in fulfilling the Customer's obligation to respond to requests for exercising the data subject's rights under Chapter III GDPR (Arts. 12–22). Because the services store no persistent visitor identifier, FAIND is generally unable to attribute the transient technical metadata to an identified

individual; FAIND will nonetheless provide reasonable cooperation. If a data subject contacts FAIND directly regarding the Customer's processing, FAIND forwards the request to the Customer without undue delay.

9) Assistance with Arts. 32–36

FAIND assists the Customer, taking into account the nature of processing and the information available to FAIND, in ensuring compliance with the obligations under Art. 32 (security), Arts. 33–34 (breach notification), Art. 35 (data protection impact assessment) and Art. 36 (prior consultation).

10) Personal data breaches

FAIND notifies the Customer without undue delay and in any event within 48 hours after becoming aware of a personal data breach affecting personal data processed on the Customer's behalf, and provides the information reasonably available to it to enable the Customer to meet its obligations under Arts. 33–34.

11) Deletion or return on termination

At the Customer's choice, FAIND deletes or returns all personal data processed on the Customer's behalf after the end of the provision of the services, and deletes existing copies, unless Union or Member-State law requires storage.

- Deletion / return period: product artifacts processed on the Customer's behalf — the Knowledge Graph pages and the content-based change-detection signals (all derived from the Customer's own public pages; they carry no visitor identifier, no raw IP and no raw user-agent) — are deleted or returned, at the Customer's choice, and existing copies removed, within 30 days of termination, unless Union or Member-State law requires storage.
- Aggregated statistics: traffic data held only in aggregated, page-level form that does not identify a data subject (no visitor identifier, no raw IP, no raw user-agent) may be retained as a long-term statistical record, including in anonymized/aggregated form, because it no longer constitutes personal data.
- Retention scope under this DPA: the artifacts and content signals above carry no visitor identifier, so they are not personal visitor data; they are retained for the duration of the subscription and deleted or anonymized within 30 days of termination. This is FAIND's retention policy, not a contractual guarantee — a time-based purge job is being implemented to enforce these limits. Server logs (which may include IP and user-agent) are retained for 90 days, longer only to investigate a specific security incident. Account and contract/billing records are kept for the statutory periods (up to 10 years, § 147 AO / § 257 HGB). FAIND-website lead and visitor-journey data fall outside this Customer DPA — see the Privacy Policy.

12) Audits and information

FAIND makes available to the Customer all information necessary to demonstrate compliance with the obligations laid down in Art. 28 and allows for and contributes to audits, including inspections, conducted by the Customer or an auditor mandated by the Customer.

- Practical arrangements: audits take place during regular business hours, once per calendar year on 30 days' written notice (and additionally where required by law or following a personal-data breach), subject to confidentiality, and in a manner that does not disrupt FAIND's operations.
- FAIND may satisfy audit requests by providing existing certifications, reports or self-assessments where these reasonably address the Customer's queries.

13) International transfers

Personal data is hosted in the EU (DigitalOcean, region FRA1 / Germany). Where a sub-processor (see Annex B) processes personal data outside the EEA — in particular in the USA — such transfers are made only on the basis of an appropriate transfer mechanism under Chapter V GDPR, namely an adequacy decision where available, or the EU Standard Contractual Clauses (SCCs) together with any necessary supplementary measures. Copies of the relevant transfer mechanisms are available on request. FAIND does not transfer personal data to a third country except as necessary to provide the services through the sub-processors listed in Annex B, or on the Customer's documented instructions.

14) Liability, order of precedence, governing law

- Order of precedence: in the event of a conflict regarding the processing of personal data, this DPA prevails over the Terms of Service and other agreements between the parties; the SCCs (where incorporated) prevail over this DPA to the extent of any conflict.
- Liability: the liability provisions of the main agreement / Terms of Service apply to this DPA, without prejudice to the rights of data subjects and the allocation of liability under Art. 82 GDPR.
- Governing law and jurisdiction: German law applies, excluding its conflict-of-laws rules; exclusive place of jurisdiction is Berlin, Germany, unless mandatory law provides otherwise.

15) Effect

This DPA forms part of and is incorporated into the agreement between the parties and takes effect when the Customer accepts the Terms of Service or otherwise orders the services. Where a separately signed copy is required, one is available on request.

Annex A — Details of processing

- Nature and purpose: operating the Agentic Web CDN / Knowledge Graph and the site snippet; detecting when the Customer's public pages change; aggregated AI-driven and bot-vs-human traffic measurement for the Customer's public pages. See Section 2.
- Categories of data subjects: visitors to the Customer's website and Knowledge Graph / CDN pages. See Section 3.
- Categories of personal data: transient technical request metadata only — IP address (not stored in analytics), user-agent (only the derived bot-vs-human category is stored), and the Customer's own page URL/path (query parameters stripped in the browser). Content-based change-detection signals derived from the Customer's own public pages are also processed, but are not visitor data. No stored visitor identifier, no cookies, no device storage. See Section 3.
- Server-side storage (page-level, not visitor profiles): the Customer's own public page content and the content-based change-detection signals derived from it, plus aggregated traffic counters keyed by day/host/path/source. These records contain no per-visitor rows, no raw IP and no raw user-agent.
- Frequency: continuous / on visitor page-loads and on the Customer's content changes, for the duration of the subscription.
- Retention: Knowledge Graph artifacts and content-based change-detection signals are retained for the duration of the subscription and deleted or returned within 30 days of termination; aggregated page-level statistics, which carry no visitor identifier, may be retained as long-term statistical records in anonymized/aggregated form. See Section 11.

Annex B — Sub-processors

General authorization is granted for the following sub-processors. This Annex lists only those that process personal data of the Customer's data subjects under this DPA — i.e. that host or deliver the Knowledge Graph and content signals, process the Customer's public page content, or receive the Customer's public URLs. The current, itemized sub-processor list is provided to the Customer on request and before any intended change, so that the Customer may object.

- Hosting: DigitalOcean, LLC (United States; EU hosting region Frankfurt, Germany) — purpose: hosting the Knowledge Graph and the page-level content signals / aggregated statistics. Entity + jurisdiction as stated; further particulars on request.
- CDN / security: Cloudflare, Inc. (United States) — purpose: content delivery and security for the Knowledge Graph / snippet traffic. Entity + jurisdiction as stated; further particulars on request.
- AI/LLM analysis of the Customer's publicly available page content: Providers for AI/LLM analysis of the Customer's publicly available page content — purpose: technical analysis / restructuring of the Customer's publicly accessible page content. Entity details provided to the Customer on request.

- Search-indexing recipients: Search-indexing recipients receiving the Customer's public URLs — purpose: submitting indexing signals (the Customer's public URLs) for the Customer's pages. Entity details provided to the Customer on request.

The current, itemized sub-processor list is provided to the Customer on request and before any intended change, so that the Customer may object.

Outside this DPA (FAIND own-site processing). Payment, email, analytics and lead-enrichment providers process personal data only in connection with FAIND's own website and business operations (billing, FAIND's transactional/marketing email, FAIND's 1:1 correspondence, and FAIND's own lead-generation and analytics on getfaind.com), not the Customer's data subjects. They are therefore not sub-processors under this Customer DPA; they are described in the Privacy Policy.

Annex C — Technical and organizational measures (Art. 32)

The following measures are in place, subject to ongoing review.

- Encryption in transit: all snippet and CDN traffic uses TLS 1.2+ / HTTPS; the snippet is served with Cache-Control: no-store and can be read in the open.
- Data minimization / pseudonymization: no visitor identifier is created; IP and raw user-agent are not stored; page paths are stripped of arbitrary/personal query parameters in the browser; analytics are held only in aggregated, page-level (pseudonymized/aggregated) form. Change detection uses technical content signals derived from the Customer's own pages, not visitor data.
- Data location: data hosted in the EU (Frankfurt, Germany; DigitalOcean, FRA1).
- Access control: access on a least-privilege, need-to-know basis with individual named accounts and multi-factor authentication for administrative access; separation of production and non-production environments.
- Confidentiality: staff bound by confidentiality (Section 5).
- Availability and resilience: regular encrypted backups and CDN-based delivery.
- Logging / monitoring: server, application and access logging for security and operations.
- Fail-safe design: the snippet is async and non-blocking and fails closed under a strict CSP without affecting the Customer's page.
- Sub-processor controls: data-protection terms flowed down to sub-processors (Section 7).
- Onboarding / offboarding: documented staff onboarding and offboarding procedures.
- Deletion: deletion / return procedures per Section 11 — Knowledge Graph artifacts and content signals deleted or returned within 30 days of termination; aggregated statistics retained only in non-identifying form.

Questions about this DPA: leif ventures UG (haftungsbeschränkt), Karl-Marx-Str. 250, 12057 Berlin, Germany · Email privacy@getfaind.com. See also our Privacy Policy and the snippet privacy note.

Signatures

Processor — pre-signed

For the Processor: **leif ventures UG (haftungsbeschränkt)**, Karl-Marx-Str. 250, 12057 Berlin, HRB 170145 B (Amtsgericht Charlottenburg), represented by its managing director Leif Pritzel. The Processor accepts this DPA in advance; it is concluded upon countersignature by the Controller.

Place / Date: Berlin, 13 July 2026

Leif Pritzel, Managing Director (pre-signed)

Controller — please complete and sign

Legal entity / company

Address

Represented by (name, role)

Place

Date

Signature / stamp