AI Data Processing

linkeme.ai -- Easylab AI (TLI S.A.)

Document: AI Data Processing Documentation

Version: 1.0

Date: March 2026

Classification: Public

1. Purpose

This document describes what data is sent to third-party AI providers when using linkeme.ai, how it is processed, stored, and protected, and how this aligns with GDPR requirements.

2. AI Providers and Data Flows

2.1 Text Generation (Anthropic / OpenAI via OpenRouter)

Data Sent	Purpose	Retention by Provider
Brand description	Context for content generation	Not retained (zero-data-retention API)
Company name and industry	Content personalization	Not retained
Website content (extracted text)	Brand voice understanding	Not retained

Previous post samples	Style consistency	Not retained
User-provided guidelines	Content direction	Not retained
Target language	Multilingual generation	Not retained

> **OpenRouter API:** linkeme.ai accesses Claude and GPT-4o-mini through OpenRouter, which provides zero-data-retention guarantees. Prompts and responses are not stored or used for model training.

2.2 Image Generation (Stability AI / Nano Banana)

Data Sent	Purpose	Retention by Provider
Text prompt (post description)	Image generation	Transient (processing only)
Brand color codes	Visual consistency	Not retained

2.3 Video Generation (Google DeepMind / Veo 3.1 via FAL.ai)

Data Sent	Purpose	Retention by Provider
Video script/ description	Video generation	Transient (processing only)
Style parameters	Visual direction	Not retained

2.4 Research (Perplexity AI)

Data Sent	Purpose	Retention by Provider
Industry keywords	Trend research	Subject to Perplexity API terms
Topic queries	News discovery	Subject to Perplexity API terms

2.5 Content Extraction (Firecrawl / Jina AI)

Data Sent	Purpose	Retention by Provider
Website URL	Content extraction	Subject to provider terms

3. Data NOT Sent to AI Providers

The following data is **never** transmitted to any AI provider:

- **Social media access tokens** -- encrypted at rest with AES-256-GCM, used only for direct API calls to social platforms
- **User authentication credentials** -- managed by Firebase Auth, never exposed to AI APIs
- **Payment information** -- managed by Stripe, never exposed to AI APIs
- **Personal data of end users' customers or employees** -- not collected, not transmitted
- **Email addresses** -- used only for account management and notifications
- **Analytics data from social platforms** -- fetched directly from platform APIs, not sent to AI providers

4. Data Security Measures

Measure	Implementation
Encryption in transit	All API calls to AI providers use TLS 1.3
Encryption at rest	Sensitive data (tokens, credentials) encrypted with AES-256-GCM
API key management	AI provider API keys stored as environment variables, not in code
Access control	AI API calls made only from server-side functions (Netlify Functions), never from client-side code
Data minimization	Only necessary context data sent in each AI request
No data persistence	AI providers do not store our request/response data (zero-retention APIs where available)

5. Data Processing Agreements

We maintain Data Processing Agreements (DPAs) or equivalent contractual arrangements with our AI providers:

Provider	Agreement Type	Data Center Location
OpenRouter (Claude, GPT-4o-mini)	API Terms of Service + DPA	USA
FAL.ai (Veo 3.1)	API Terms of Service	USA/EU

Perplexity AI	API Terms of Service	USA
Firecrawl	API Terms of Service	USA
Jina AI	API Terms of Service	EU

6. GDPR Alignment

6.1 Legal Basis

Data processing for AI content generation is based on:

- **Contract performance (Art. 6(1)(b) GDPR):** Processing is necessary to provide the content generation service the user has subscribed to.
- **Legitimate interest (Art. 6(1)(f) GDPR):** Improving content quality through AI model interaction.

6.2 Data Subject Rights

Users can exercise their GDPR rights regarding AI-processed data:

- **Access:** View all data used for and generated by AI systems in their dashboard.
- **Rectification:** Update brand information and guidelines at any time.
- **Erasure:** Delete account and all associated data, including AI-generated content.
- **Portability:** Export all generated content and account data.
- **Objection:** Opt out of specific AI features or the service entirely.

6.3 International Transfers

Some AI providers process data in the United States. These transfers are protected by:

- EU-U.S. Data Privacy Framework (where applicable)
- Standard Contractual Clauses (SCCs) as a fallback mechanism
- Data minimization (limiting data sent to what is strictly necessary)

7. Data Retention

Data Type	Retention Period	Location
Generated content (posts)	Active account lifetime + 30 days after deletion	Google Firestore (EU)
Brand information	Active account lifetime	Google Firestore (EU)
Website extraction cache	Refreshed on re-analysis; deleted with account	Google Firestore (EU)
AI provider logs	Not retained by providers (zero-retention APIs)	N/A

8. Review and Updates

This document is reviewed quarterly and updated whenever data flows to AI providers change or new providers are added.
