

Data Processing Agreement (DPA)

pursuant to Art. 28 of the General Data Protection Regulation (GDPR) for the use of CiteBoost

Version 1.0 · As of 26 October 2026

Parties

CONTROLLER

The company that holds an account with CiteBoost (citeboost.ai), with the details provided at registration or in the billing information – hereinafter “Customer”.

PROCESSOR

Antom Media UG (haftungsbeschränkt)
Am BioPark 13
93053 Regensburg, Germany
Local Court (Amtsgericht) Regensburg, HRB
19907 · Managing Director: Andreas Ehret
hereinafter “Provider”, “we”

1. Subject Matter, Scope and Term

- (1) This DPA governs the processing of personal data that the Provider processes on behalf of the Customer when providing CiteBoost (“Customer Data”). The subject matter, nature and purpose of the processing, the types of data and the data subjects are described in Annex 1.
- (2) This DPA forms part of the CiteBoost Terms of Service and is concluded upon their acceptance at registration or purchase. It is provided in electronic form (Art. 28(9) GDPR); no signature is required.
- (3) This DPA applies for the term of the service agreement and beyond for as long as the Provider processes Customer Data.
- (4) This DPA does not cover data for which the Provider is itself the controller, in particular the Customer's account, contract and billing data. These are governed by the Privacy Policy at citeboost.ai/privacy.
- (5) In the event of conflict, this DPA prevails over the Terms of Service with regard to the protection of personal data.

2. Instructions

- (1) The Provider processes Customer Data only on documented instructions from the Customer, unless required to do so by EU or Member State law; in that case the Provider informs the Customer of that requirement in advance unless the law prohibits this.
- (2) The instructions are set out in the Terms of Service, this DPA and the settings and actions the Customer makes in the app (e.g. creating prompts, starting analyses, connecting a website). Further instructions are given by the Customer in text form.
- (3) If the Provider considers that an instruction infringes data protection law, it informs the Customer without undue delay and may suspend its execution until clarified.

3. Customer Obligations

- (1) The Customer is responsible for the lawfulness of the processing and for safeguarding the rights of data subjects. The Customer ensures that it is entitled to process the data it enters into CiteBoost or transmits

via connected services (e.g. Google Search Console, WordPress).

(2) CiteBoost is not intended for special categories of personal data (Art. 9 GDPR) or data relating to criminal convictions (Art. 10 GDPR). The Customer does not enter such data.

4. Confidentiality

The Provider grants access to Customer Data only to persons who need it to provide the service and who have committed themselves to confidentiality or are under a statutory obligation of confidentiality. This obligation continues after their engagement ends.

5. Technical and Organisational Measures

(1) The Provider implements the technical and organisational measures described in Annex 2 pursuant to Art. 32 GDPR and maintains them for the term of the agreement.

(2) The measures are subject to technical progress. The Provider may replace them with equivalent or better measures; the level of protection must not be reduced.

6. Assistance to the Customer

(1) The Provider assists the Customer with appropriate measures in responding to data subject requests (Art. 12–22 GDPR). If a data subject contacts the Provider directly, the Provider forwards the request to the Customer without undue delay.

(2) The Provider assists the Customer to a reasonable extent in complying with the obligations under Art. 32–36 GDPR (security, breach notification, data protection impact assessment, prior consultation).

7. Sub-processors

(1) The Customer grants general authorisation for the engagement of sub-processors. The sub-processors engaged at the time of conclusion are listed in Annex 3 and are deemed approved.

(2) The Provider concludes an agreement with each sub-processor imposing essentially the same data protection obligations as this DPA.

(3) The Provider informs the Customer of any intended addition or replacement of a sub-processor at least 14 days in advance by email to the account address. The Customer may object in text form within this period on reasonable data protection grounds. If the parties cannot find a solution, the Customer may terminate the agreement with effect from the date of the change; fees already paid for the period thereafter are refunded pro rata.

(4) If a sub-processor must be replaced at short notice to ensure operations or security, the Provider informs the Customer without undue delay; paragraph 3 applies accordingly.

8. Transfers to Third Countries

Processing outside the EU/EEA only takes place if the requirements of Art. 44 et seq. GDPR are met, in particular on the basis of an adequacy decision (e.g. the EU-US Data Privacy Framework) or the EU Standard Contractual Clauses. The respective basis is stated in Annex 3.

9. Personal Data Breaches

The Provider notifies the Customer of a breach affecting Customer Data without undue delay, where possible within 48 hours of becoming aware of it, by email to the account address. The notification

contains, as far as known, the information required by Art. 33(3) GDPR. The Provider takes immediate measures to contain the breach and mitigate its consequences.

10. Deletion and Return

- (1) During the term, the Customer can download its data using the export functions of the app; on request, the Provider provides it in a common format.
- (2) After the end of the agreement or deletion of the account, the Provider deletes the Customer Data from its live systems. Backups are overwritten in the regular backup cycle, at the latest after 35 days.
- (3) Statutory retention obligations remain unaffected; affected data is restricted until the retention period expires.

11. Information and Audits

- (1) On request, the Provider makes available to the Customer the information necessary to demonstrate compliance with this DPA, in particular a current description of the measures in Annex 2.
- (2) If this information demonstrably proves insufficient, the Customer may carry out an on-site audit itself or have it carried out by an auditor bound to confidentiality who is not a competitor of the Provider. Audits must be announced at least 30 days in advance, take place during normal business hours, no more than once a year (except after a breach under Section 9), and must not affect operations or the data of other customers. The Customer bears the costs of the audit.

12. Liability and Final Provisions

- (1) Liability is governed by Art. 82 GDPR; otherwise the liability provisions of the Terms of Service apply.
- (2) The Provider notifies the Customer of changes to this DPA in text form. German law applies; to the extent permitted, the place of jurisdiction is Regensburg, Germany.
- (3) Should any provision be invalid, the validity of the remaining provisions is not affected.
- (4) This English version is a translation for convenience; in case of doubt, the German version prevails.

Questions about this DPA: info [at] antom.media (subject "Data protection") or via citeboost.ai/support

Annex 1 – Description of the Processing

Subject matter	Provision of the CiteBoost platform for visibility in AI answers (GEO/AEO) and search engines (SEO) in accordance with the Terms of Service.
Nature of processing	Storage, analysis, evaluation, transmission to AI models and search data services, generation of content and reports, deletion.
Purpose	Measuring how AI systems and search engines present the Customer, its brand and its competitors; analysis of websites and search data; creation and publication of content; analysis of AI crawler visits; support.
Types of data	• Customer input: prompts, brand, product and competitor names, domains, keywords, brand facts, knowledge base, briefs and articles • Results: answers from AI models and search surfaces, which may contain names of individuals, and metrics derived from them • Content of connected websites and WordPress installations (e.g. page content, author names) • Google Search Console data, if connected by the Customer (search queries, pages, clicks, impressions) • AI crawler visits to connected websites: bot name, requested path, status code, time. The bot's IP address is used only briefly to verify authenticity and is not stored; visits by humans are not recorded • Usage and log data of the Customer's app, API and MCP interface usage; content of support requests
Data subjects	Employees and agents of the Customer who use CiteBoost; individuals named in input, website content or results (e.g. contact persons, authors, employees of competitors); individuals whose search queries are contained in Search Console data.
Location	Data centres in Germany; AI models and services as listed in Annex 3.
Duration	Term of the service agreement plus the deletion periods under Section 10.

Annex 2 – Technical and Organisational Measures (Art. 32 GDPR)

Confidentiality

- **Physical access control:** Operation exclusively in data centres of the sub-processors in Germany with their access protection (including personalised access systems, video surveillance, alarm systems, logged visits).
- **System access control:** Customer accounts with passwords stored only as bcrypt hashes, email verification at registration and optional two-factor sign-in; limits on sign-in attempts; administration area only with sign-in plus authenticator code; server access only encrypted (SSH) and only for management.
- **Data access control:** Every request is assigned to the signed-in account on the server; customers only see their own data; internal files and logs are blocked by the web server; access keys are stored in configuration files readable only by the system user or encrypted in the database.
- **Separation:** Logical separation of customer data by account identifiers; separate test and live environments for payments.
- **Pseudonymisation and data minimisation:** Email addresses are truncated in server logs; AI models and search data services only receive the content needed for the respective analysis, no account data; location search and address suggestions run via our server without passing on the IP address.

Integrity

- **Transfer control:** All connections to the app and to sub-processors are TLS (HTTPS) encrypted; off-site backups are encrypted before upload.
- **Input control:** Server logs (rotated daily, kept for 14 days) and a log of actions in the administration area.
- **Abuse protection:** Length and volume limits for input, per-account throttling, signature verification of webhooks and plugin requests.

Availability and Resilience

- Daily database backups with integrity check (14 days on the server) and daily encrypted backups at a second location (7 daily and 4 weekly versions).
- Automatic service restarts, graceful shutdown during updates, monitoring of service availability and balances every 10 minutes with alerting.
- Restoration from backups following a documented procedure.

Procedures for Regular Review

- Regular security reviews of the code and server configuration; timely installation of security updates.
- Selection of sub-processors based on their data protection and security measures, each with an agreement under Art. 28 GDPR.
- Defined procedure for data protection incidents (contain, assess, notify under Section 9).

Annex 3 – Sub-processors

Company	Purpose	Location	Transfer basis
1blu GmbH Riedemannweg 60, 13627 Berlin	Hosting of the platform: application server, database, billing system, email server and on-server backups	Germany	EU/EEA
Hetzner Online GmbH Industriestr. 25, 91710 Gunzenhausen	Rendering service for bot rendering: creates fully rendered versions of the public pages of connected websites for AI crawlers (only if this feature is used)	Germany	EU/EEA
Dataforseo OÜ Vesivärava tn 50-201, 10152 Tallinn	Real search data (search volume, rankings, backlinks) and answers from AI search surfaces (e.g. Google AI Overviews, AI Mode); keywords, prompts and domains are transmitted	Estonia	EU/EEA
OpenRouter, Inc. 169 Madison Ave #2404, New York, NY 10016	Routing of prompts and analysis requests to the AI models selected by the customer (e.g. from OpenAI, Anthropic, Google, Perplexity, xAI, Mistral). The respective model providers process the request as further sub-processors of OpenRouter; the location depends on the selected model	USA	EU Standard Contractual Clauses
Google Cloud EMEA Limited 70 Sir John Rogerson's Quay, Dublin 2	Gemini models for AI analyses, text generation, image generation and the AI assistant; storage for end-to-end encrypted backups (the key is held only by us)	Ireland / USA	EU-US Data Privacy Framework, supplemented by EU Standard Contractual Clauses

We operate the database, billing system, web analytics and email server ourselves on the servers of 1blu GmbH. Not listed are service providers that only process data for which we are the controller ourselves (e.g. payment processing by Stripe) – see the Privacy Policy.