CiteTop

Auftragsverarbeitungsvertrag (AVV)

nach Art. 28 Datenschutz-Grundverordnung (DSGVO) für die Nutzung von CiteTop

Version 1.0 · Stand: 26. Oktober 2026

Vertragsparteien

VERANTWORTLICHER (AUFTRAGGEBER)

Das Unternehmen, das ein Konto bei CiteTop (citetop.ai) führt, mit den bei der Registrierung bzw. in den Rechnungsangaben hinterlegten Daten – nachfolgend „Kunde“.

AUFTRAGSVERARBEITER (AUFTRAGNEHMER)

Antom Media UG (haftungsbeschränkt)
Am BioPark 13
93053 Regensburg, Deutschland
Amtsgericht Regensburg, HRB 19907 · Geschäftsführer: Andreas Ehret
nachfolgend „Anbieter“, „wir“

1. Gegenstand, Geltung und Dauer

(1) Dieser AVV regelt die Verarbeitung personenbezogener Daten, die der Anbieter im Auftrag des Kunden bei der Bereitstellung von CiteTop verarbeitet („Auftragsdaten“). Gegenstand, Art und Zweck der Verarbeitung, die Datenarten und die betroffenen Personen beschreibt Anlage 1.

(2) Der AVV ist Bestandteil der Allgemeinen Geschäftsbedingungen (AGB) von CiteTop und wird mit deren Annahme bei der Registrierung bzw. Buchung geschlossen. Er liegt in elektronischem Format vor (Art. 28 Abs. 9 DSGVO); einer Unterschrift bedarf es nicht.

(3) Der AVV gilt für die Laufzeit des Nutzungsvertrags und darüber hinaus, solange der Anbieter Auftragsdaten verarbeitet.

(4) Nicht unter diesen AVV fallen Daten, für die der Anbieter selbst Verantwortlicher ist, insbesondere die Konto-, Vertrags- und Abrechnungsdaten des Kunden. Hierfür gilt die Datenschutzerklärung unter citetop.ai/datenschutz.

(5) Bei Widersprüchen geht dieser AVV den AGB vor, soweit es um den Schutz personenbezogener Daten geht.

2. Weisungen

(1) Der Anbieter verarbeitet Auftragsdaten nur auf dokumentierte Weisung des Kunden, es sei denn, er ist nach dem Recht der EU oder eines Mitgliedstaats zu einer Verarbeitung verpflichtet; in diesem Fall teilt er dem Kunden diese Pflicht vorab mit, sofern das Recht dies nicht verbietet.

(2) Die Weisungen ergeben sich abschließend aus den AGB, diesem AVV sowie aus den Einstellungen und Aktionen, die der Kunde in der App vornimmt (z. B. Anlegen von Prompts, Starten von Analysen, Verbinden einer Website). Weitere Weisungen erteilt der Kunde in Textform.

(3) Ist der Anbieter der Ansicht, dass eine Weisung gegen Datenschutzrecht verstößt, informiert er den Kunden unverzüglich und darf die Ausführung bis zur Klärung aussetzen.

3. Pflichten des Kunden

(1) Der Kunde ist für die Rechtmäßigkeit der Verarbeitung und für die Wahrung der Rechte der betroffenen Personen verantwortlich. Er stellt sicher, dass er die Daten, die er in CiteTop eingibt oder über verbundene Dienste (z. B. Google Search Console, WordPress) übermittelt, verarbeiten darf.

(2) CiteTop ist nicht für besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) oder Daten über strafrechtliche Verurteilungen (Art. 10 DSGVO) bestimmt. Der Kunde gibt solche Daten nicht ein.

4. Vertraulichkeit

Der Anbieter gewährt Zugriff auf Auftragsdaten nur Personen, die diesen für die Leistungserbringung benötigen und die zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung besteht auch nach Ende ihrer Tätigkeit fort.

5. Technische und organisatorische Maßnahmen

(1) Der Anbieter trifft die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO und hält sie während der Vertragslaufzeit ein.

(2) Die Maßnahmen unterliegen dem technischen Fortschritt. Der Anbieter darf sie durch gleichwertige oder bessere Maßnahmen ersetzen; das Schutzniveau darf dabei nicht sinken.

6. Unterstützung des Kunden

(1) Der Anbieter unterstützt den Kunden mit geeigneten Maßnahmen bei der Beantwortung von Anträgen betroffener Personen (Art. 12–22 DSGVO). Wendet sich eine betroffene Person direkt an den Anbieter, leitet er die Anfrage unverzüglich an den Kunden weiter.

(2) Der Anbieter unterstützt den Kunden im angemessenen Umfang bei der Einhaltung der Pflichten aus Art. 32–36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation).

7. Unterauftragnehmer

(1) Der Kunde erteilt die allgemeine Genehmigung zum Einsatz von Unterauftragnehmern. Die bei Vertragsschluss eingesetzten Unterauftragnehmer sind in Anlage 3 aufgeführt und gelten als genehmigt.

(2) Der Anbieter schließt mit jedem Unterauftragnehmer einen Vertrag, der ihm im Wesentlichen dieselben Datenschutzpflichten auferlegt wie dieser AVV.

(3) Über die geplante Hinzunahme oder den Austausch eines Unterauftragnehmers informiert der Anbieter den Kunden mindestens 14 Tage vorher per E-Mail an die Kontoadresse. Der Kunde kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Finden die Parteien keine Lösung, kann der Kunde den Vertrag zum Zeitpunkt des Wechsels außerordentlich kündigen; bereits gezahlte Entgelte für die Zeit danach werden anteilig erstattet.

(4) Muss ein Unterauftragnehmer kurzfristig ersetzt werden, um den Betrieb oder die Sicherheit zu gewährleisten, informiert der Anbieter den Kunden unverzüglich; Absatz 3 gilt entsprechend.

8. Übermittlung in Drittländer

Eine Verarbeitung außerhalb der EU bzw. des EWR erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere auf Grundlage eines Angemessenheitsbeschlusses (z. B. EU-US Data

Privacy Framework) oder der EU-Standardvertragsklauseln. Die jeweilige Grundlage ist in Anlage 3 angegeben.

9. Verletzungen des Schutzes personenbezogener Daten

Der Anbieter meldet dem Kunden eine Verletzung des Schutzes von Auftragsdaten unverzüglich, möglichst innerhalb von 48 Stunden nach Kenntnis, per E-Mail an die Kontoadresse. Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO. Der Anbieter ergreift unverzüglich Maßnahmen, um die Verletzung einzudämmen und ihre Folgen zu mindern.

10. Löschung und Rückgabe

(1) Der Kunde kann seine Daten während der Laufzeit über die Exportfunktionen der App herunterladen; auf Anfrage stellt der Anbieter sie in einem gängigen Format bereit.

(2) Nach Vertragsende bzw. Löschung des Kontos löscht der Anbieter die Auftragsdaten in den laufenden Systemen. Sicherungskopien werden im regulären Sicherungszyklus überschrieben, spätestens nach 35 Tagen.

(3) Gesetzliche Aufbewahrungspflichten bleiben unberührt; betroffene Daten werden bis zum Ablauf der Frist gesperrt.

11. Nachweise und Kontrollen

(1) Der Anbieter stellt dem Kunden auf Anfrage die Informationen bereit, die zum Nachweis der Einhaltung dieses AVV erforderlich sind, insbesondere eine aktuelle Beschreibung der Maßnahmen nach Anlage 2.

(2) Reichen diese Informationen nachweislich nicht aus, kann der Kunde eine Prüfung vor Ort durchführen oder durch einen zur Verschwiegenheit verpflichteten Prüfer durchführen lassen, der kein Wettbewerber des Anbieters ist. Prüfungen sind mit mindestens 30 Tagen Vorlauf anzumelden, finden zu den üblichen Geschäftszeiten statt, höchstens einmal im Jahr (außer nach einer Verletzung nach Abschnitt 9) und dürfen den Betrieb sowie die Daten anderer Kunden nicht beeinträchtigen. Die Kosten der Prüfung trägt der Kunde.

12. Haftung und Schlussbestimmungen

(1) Für die Haftung gilt Art. 82 DSGVO; im Übrigen gelten die Haftungsregeln der AGB.

(2) Änderungen dieses AVV teilt der Anbieter dem Kunden in Textform mit. Es gilt deutsches Recht; Gerichtsstand ist, soweit zulässig, Regensburg.

(3) Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Fragen zu diesem AVV: info [at] antom.media (Betreff „Datenschutz“) oder über citetop.ai/support

Anlage 1 – Beschreibung der Verarbeitung

Gegenstand	Bereitstellung der Plattform CiteTop für Sichtbarkeit in KI-Antworten (GEO/AEO) und Suchmaschinen (SEO) nach den AGB.
Art der Verarbeitung	Speichern, Analysieren, Auswerten, Übermitteln an KI-Modelle und Suchdatendienste, Erzeugen von Inhalten und Berichten, Löschen.
Zweck	Messung, wie KI-Systeme und Suchmaschinen den Kunden, seine Marke und seine Wettbewerber darstellen; Analyse von Websites und Suchdaten; Erstellung und Veröffentlichung von Inhalten; Auswertung von KI-Crawler-Besuchen; Support.
Arten von Daten	• Eingaben des Kunden: Prompts, Marken-, Produkt- und Wettbewerbernamen, Domains, Suchbegriffe, Markenfakten, Wissensdatenbank, Briefings und Artikel • Ergebnisse: Antworten von KI-Modellen und Suchoberflächen, die Namen von Personen enthalten können, sowie daraus abgeleitete Kennzahlen • Inhalte verbundener Websites und WordPress-Installationen (z. B. Seiteninhalte, Autorennamen) • Daten aus der Google Search Console, sofern der Kunde sie verbindet (Suchanfragen, Seiten, Klicks, Impressionen) • KI-Crawler-Besuche verbundener Websites: Bot-Name, aufgerufener Pfad, Statuscode, Zeitpunkt. Die IP-Adresse des Bots wird nur kurz zur Echtheitsprüfung verwendet und nicht gespeichert; Besuche von Menschen werden nicht erfasst • Nutzungs- und Protokolldaten der App, API und MCP-Schnittstelle des Kunden; Inhalte von Support-Anfragen
Betroffene Personen	Beschäftigte und Beauftragte des Kunden, die CiteTop nutzen; Personen, die in Eingaben, Website-Inhalten oder Ergebnissen genannt werden (z. B. Ansprechpartner, Autoren, Mitarbeiter von Wettbewerbern); Personen, deren Suchanfragen in Search-Console-Daten enthalten sind.
Ort der Verarbeitung	Rechenzentren in Deutschland; KI-Modelle und Dienste gemäß Anlage 3.
Dauer	Laufzeit des Nutzungsvertrags zuzüglich der Löschfristen nach Abschnitt 10.

Anlage 2 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Vertraulichkeit

- **Zutrittskontrolle:** Betrieb ausschließlich in Rechenzentren der Unterauftragnehmer in Deutschland mit deren Zutrittsschutz (u. a. personalisierte Zutrittssysteme, Videoüberwachung, Alarmanlage, protokollierte Besuche).
- **Zugangskontrolle:** Kundenkonten mit Passwörtern, die nur als bcrypt-Hash gespeichert werden, E-Mail-Bestätigung bei der Registrierung und optionaler Zwei-Faktor-Anmeldung; Begrenzung von Anmeldeversuchen; Administrationsbereich nur mit Anmeldung plus Authenticator-Code; Serverzugang nur verschlüsselt (SSH) und nur für die Geschäftsführung.
- **Zugriffskontrolle:** Jede Anfrage wird serverseitig dem angemeldeten Konto zugeordnet; Kunden sehen nur eigene Daten; interne Dateien und Protokolle sind vom Webserver gesperrt; Zugangsschlüssel liegen in nur für den Systembenutzer lesbaren Konfigurationsdateien bzw. verschlüsselt in der Datenbank.
- **Trennung:** Logische Trennung der Kundendaten über Kontokennungen; getrennte Test- und Live-Umgebung für Zahlungen.
- **Pseudonymisierung und Datensparsamkeit:** E-Mail-Adressen werden in Server-Protokollen gekürzt; an KI-Modelle und Suchdatendienste gehen nur die für die jeweilige Analyse nötigen Inhalte, keine Kontodaten; Ortssuche und Adressvorschläge laufen über unseren Server ohne Weitergabe der IP-Adresse.

Integrität

- **Weitergabekontrolle:** Alle Verbindungen zur App und zu Unterauftragnehmern sind per TLS (HTTPS) verschlüsselt; Sicherungskopien außerhalb des Rechenzentrums werden vor dem Hochladen verschlüsselt.
- **Eingabekontrolle:** Server-Protokolle (täglich rotiert, 14 Tage aufbewahrt) und ein Protokoll der Aktionen im Administrationsbereich.
- **Schutz vor Missbrauch:** Längen- und Mengenbegrenzungen für Eingaben, Drosselung je Konto, Prüfung von Webhooks und Plugin-Anfragen per Signatur.

Verfügbarkeit und Belastbarkeit

- Tägliche Sicherung der Datenbanken mit Integritätsprüfung (14 Tage auf dem Server) sowie tägliche, verschlüsselte Sicherung an einem zweiten Ort (7 Tages- und 4 Wochenstände).
- Automatischer Neustart von Diensten, geordnetes Herunterfahren bei Updates, Überwachung von Erreichbarkeit und Guthaben der Dienste alle 10 Minuten mit Alarmierung.
- Wiederherstellung aus den Sicherungen nach dokumentiertem Verfahren.

Verfahren zur Überprüfung

- Regelmäßige Sicherheitsprüfungen des Codes und der Serverkonfiguration; zeitnahes Einspielen von Sicherheitsupdates.
- Auswahl von Unterauftragnehmern nach ihren Datenschutz- und Sicherheitsmaßnahmen, jeweils mit Vertrag nach Art. 28 DSGVO.
- Festgelegter Ablauf für Datenschutzvorfälle (Eindämmen, Bewerten, Melden nach Abschnitt 9).

Anlage 3 – Unterauftragnehmer

Unternehmen	Zweck	Standort	Grundlage
1blu GmbH Riedemannweg 60, 13627 Berlin	Hosting der Plattform: Anwendungsserver, Datenbank, Abrechnungssystem, E-Mail-Server und Sicherungen auf dem Server	Deutschland	EU/EWR
Hetzner Online GmbH Industriestr. 25, 91710 Gunzenhausen	Render-Dienst für das Bot-Rendering: erzeugt fertig gerenderte Fassungen der öffentlichen Seiten verbundener Websites für KI-Crawler (nur bei Nutzung dieser Funktion)	Deutschland	EU/EWR
Dataforseo OÜ Vesivärava tn 50-201, 10152 Tallinn	Echte Suchdaten (Suchvolumen, Rankings, Backlinks) und Antworten aus KI-Suchoberflächen (z. B. Google AI Overviews, AI Mode); übermittelt werden Suchbegriffe, Prompts und Domains	Estland	EU/EWR
OpenRouter, Inc. 169 Madison Ave #2404, New York, NY 10016	Weiterleitung von Prompts und Analyseaufträgen an die vom Kunden gewählten KI-Modelle (z. B. von OpenAI, Anthropic, Google, Perplexity, xAI, Mistral). Die jeweiligen Modellanbieter verarbeiten die Anfrage als weitere Unterauftragnehmer von OpenRouter; der Standort hängt vom gewählten Modell ab	USA	EU-Standardvertragsklauseln
Google Cloud EMEA Limited 70 Sir John Rogerson's Quay, Dublin 2	Gemini-Modelle für KI-Analysen, Texterstellung, Bildgenerierung und die KI-Hilfe; Speicher für Ende-zu-Ende-verschlüsselte Sicherungskopien (der Schlüssel liegt nur bei uns)	Irland / USA	EU-US Data Privacy Framework, ergänzend EU-Standardvertragsklauseln

Datenbank, Abrechnungssystem, Reichweitenmessung und E-Mail-Server betreiben wir selbst auf den Servern der 1blu GmbH. Nicht aufgeführt sind Dienstleister, die ausschließlich Daten verarbeiten, für die wir selbst verantwortlich sind (z. B. die Zahlungsabwicklung durch Stripe) – siehe Datenschutzerklärung.