Achtung.app

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

Art. 28 DSGVO

Version: 1.14
Stand: 18.08.2026

Vertragsparteien

Auftraggeber (Verantwortlicher oder seinerseits Auftragsverarbeiter, siehe § 1 Ziffer 3)

Firma: .....
Anschrift: .....
Vertreten durch: .....
Ansprechpartner Datenschutz: .....

Auftragsverarbeiter (nachfolgend "Auftragnehmer")

Martin Kulawik, Marketing & Digitalisierung
Chodowieckistr. 40, 10405 Berlin
USt-IdNr. DE293087048
Kontakt in Datenschutzangelegenheiten: daten@martinkulawik.de

---

Präambel

Der Auftragnehmer betreibt unter achtung.app einen Dienst zur Messung der Sichtbarkeit von Marken in KI-Assistenten und Suchsystemen. Der Auftraggeber nutzt diesen Dienst auf Grundlage der Nutzungsbedingungen unter achtung.app/agb (nachfolgend "Hauptvertrag").

Bei der Erbringung dieser Leistung verarbeitet der Auftragnehmer personenbezogene Daten, für die der Auftraggeber datenschutzrechtlich einsteht, sei es als Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO oder als Auftragsverarbeiter eines Dritten (§ 1 Ziffer 3). Dieser Vertrag konkretisiert die Pflichten der Parteien nach Art. 28 DSGVO. Er gilt für alle Tätigkeiten, die mit dem Hauptvertrag zusammenhängen und bei denen Beschäftigte des Auftragnehmers oder von ihm beauftragte Dritte personenbezogene Daten des Auftraggebers verarbeiten.

Dieser Vertrag ist Bestandteil des Hauptvertrages. Er kommt in seiner jeweils unter achtung.app/avv veröffentlichten Fassung mit dem Abschluss des Hauptvertrages zustande, ohne dass es einer gesonderten Unterzeichnung bedarf (Art. 28 Abs. 9 DSGVO, elektronische Form). Die Verarbeitung beginnt damit nicht vor dem Vertragsschluss. Der Auftraggeber kann jederzeit eine vom Auftragnehmer unterzeichnete Ausfertigung anfordern; die nachfolgenden Unterschriftsfelder dienen allein diesem Zweck und sind für die Wirksamkeit nicht erforderlich.

---

§ 1 Gegenstand, Dauer und Beendigung

1. Gegenstand des Auftrags ist die Verarbeitung derjenigen personenbezogenen Daten, die der Auftraggeber im Rahmen der Nutzung des Dienstes in die Anwendung einbringt oder die dort für ihn erhoben werden (nachfolgend "Kundendaten"), zur Erbringung der im Hauptvertrag vereinbarten Leistungen. Art, Umfang und Zweck der Verarbeitung, die Art der Daten sowie der Kreis der betroffenen Personen ergeben sich abschließend aus Anlage 1.

2. Nicht Gegenstand dieses Vertrages sind Verarbeitungen, die der Auftragnehmer zu eigenen Zwecken und in eigener Verantwortlichkeit vornimmt. Das sind:

   a) Abrechnung, Buchführung und die Erfüllung steuerlicher Pflichten,
   b) die Abwehr von Missbrauch und Angriffen sowie die dafür geführten eigenen Sicherheits- und Serverprotokolle,
   c) die Geltendmachung und Verteidigung von Rechtsansprüchen,
   d) die Erstellung aggregierter und anonymisierter Branchen-Auswertungen nach Maßgabe des Hauptvertrages.

   Für diese Verarbeitungen ist der Auftragnehmer selbst Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO. Sie richten sich nicht nach den Weisungen des Auftraggebers, sondern nach der Datenschutzerklärung unter achtung.app/datenschutz.

3. Auftraggeber im Sinne dieses Vertrages ist der Vertragspartner des Hauptvertrages, unabhängig davon, ob er die Kundendaten als Verantwortlicher oder seinerseits als Auftragsverarbeiter für einen Dritten verarbeitet. Verarbeitet der Auftraggeber die Kundendaten als Auftragsverarbeiter, etwa eine Agentur für ihren Kunden, so sichert er zu, dass er zur Beauftragung des Auftragnehmers als weiterem

Auftragsverarbeiter berechtigt ist und die erforderlichen Weisungen des Verantwortlichen einholt. Der Auftragnehmer nimmt Weisungen in diesem Fall ausschließlich vom Auftraggeber entgegen.

4. Die Laufzeit dieses Vertrages entspricht der Laufzeit des Hauptvertrages. Er endet automatisch mit dessen Beendigung, ohne dass es einer gesonderten Kündigung bedarf.
5. Der Auftraggeber kann diesen Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen datenschutzrechtliche Vorschriften oder gegen die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

---

§ 2 Weisungsrecht des Auftraggebers

1. Der Auftragnehmer verarbeitet die Kundendaten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierten Weisungen des Auftraggebers, es sei denn, er ist nach dem Recht der Union oder der Mitgliedstaaten zu einer anderen Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
2. Die Weisungen werden anfänglich durch diesen Vertrag und die Konfiguration des Dienstes durch den Auftraggeber festgelegt. Der Auftraggeber erteilt einzelne Weisungen insbesondere durch seine Eingaben in der Anwendung, etwa durch das Anlegen und Löschen von Marken, Keywords und Nutzerkonten.
3. Einzelweisungen, die über die vertraglich vereinbarte Leistung hinausgehen, erteilt der Auftraggeber in Textform an daten@martinkulawik.de. Der Auftragnehmer bestätigt den Eingang. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform nach.
4. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung auszusetzen, bis der Auftraggeber sie bestätigt oder ändert.

---

§ 3 Pflichten des Auftragnehmers

1. **Zweckbindung.** Der Auftragnehmer verarbeitet die Kundendaten ausschließlich zu den in Anlage 1 genannten Zwecken. Kopien oder Duplikate werden ohne Kenntnis des Auftraggebers nicht erstellt; ausgenommen sind Sicherungskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
2. **Vertraulichkeit.** Der Auftragnehmer stellt sicher, dass sich alle Personen, die zur Verarbeitung der Daten befugt sind, zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Die Verpflichtung gilt auch nach Beendigung der Tätigkeit fort.
3. **Technische und organisatorische Maßnahmen.** Der Auftragnehmer trifft die Maßnahmen nach Art. 32 DSGVO. Der Stand der Maßnahmen zum Zeitpunkt des Vertragsschlusses ist in Anlage 2 beschrieben. Der Auftragnehmer darf die Maßnahmen weiterentwickeln, solange das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen dokumentiert er und teilt sie dem Auftraggeber auf Anfrage mit.
4. **Unterstützung des Auftraggebers.** Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Betroffenenrechte nach Art. 12 bis 23 DSGVO, bei der Datenschutz-Folgenabschätzung nach Art. 35 DSGVO, bei einer vorherigen Konsultation nach Art. 36 DSGVO sowie bei der Meldung von Verletzungen des Schutzes personenbezogener Daten nach Art. 33 und 34 DSGVO.
5. **Berichtigung, Löschung und Sperrung.** Der Auftragnehmer berichtigt, löscht oder schränkt die Verarbeitung der Daten nur nach Weisung des Auftraggebers ein. Von der Anwendung selbst ausgelöste Löschungen nach den in Anlage 1 genannten Fristen gelten als vom Auftraggeber angewiesen.
6. **Betroffenenanfragen.** Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, um Rechte nach Art. 15 bis 22 DSGVO hinsichtlich der Kundendaten geltend zu machen, beantwortet der Auftragnehmer die Anfrage nicht selbst. Er leitet sie unverzüglich an den Auftraggeber weiter und teilt der betroffenen Person mit, dass die Anfrage weitergeleitet wurde.
7. **Keine besonderen Datenkategorien.** Die Eingabe personenbezogener Daten besonderer Kategorien nach Art. 9 DSGVO sowie von Daten über strafrechtliche Verurteilungen nach Art. 10 DSGVO in die Anwendung ist dem Auftraggeber untersagt. Der Auftragnehmer trifft für solche Daten keine besonderen Schutzmaßnahmen und prüft Freitexteingaben nicht vorab.
8. **Kontaktstelle.** Der Auftragnehmer benennt daten@martinkulawik.de als Kontaktstelle für alle Anfragen des Auftraggebers zu diesem Vertrag.
9. **Mitteilungspflichten.** Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen einer Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen, sowie über Ermittlungen von Strafverfolgungsbehörden, die die Verarbeitung im Auftrag betreffen.

---

§ 4 Verletzungen des Schutzes personenbezogener Daten

1. Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten, die die Verarbeitung im Auftrag betrifft, unverzüglich nach Bekanntwerden, in der Regel innerhalb von 24 Stunden. Die Meldung erfolgt in Textform an die vom Auftraggeber benannte Kontaktadresse.
2. Die Meldung enthält, soweit dem Auftragnehmer bekannt, eine Beschreibung der Art der Verletzung, die Kategorien und die ungefähre Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen sowie die ergriffenen oder vorgeschlagenen Gegenmaßnahmen. Stehen nicht alle Angaben sofort zur Verfügung, meldet der Auftragnehmer zunächst den bekannten Sachverhalt und reicht die weiteren Angaben unverzüglich nach.
3. Der Auftragnehmer dokumentiert jede Verletzung einschließlich der ergriffenen Abhilfemaßnahmen nach Art. 33 Abs. 5 DSGVO und stellt die Dokumentation dem Auftraggeber auf Anfrage zur Verfügung.
4. Die Meldung an die Aufsichtsbehörde und an die betroffenen Personen obliegt dem Auftraggeber. Der Auftragnehmer nimmt eine solche Meldung nicht eigenständig für den Auftraggeber vor.

---

§ 5 Unterauftragsverhältnisse

1. Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter hinzuzuziehen (Art. 28 Abs. 2 Satz 2 DSGVO). Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in Anlage 3 aufgeführt und werden hiermit genehmigt.
2. Der Auftragnehmer informiert den Auftraggeber mindestens 30 Tage vor der Hinzuziehung eines weiteren oder dem Austausch eines bestehenden Unterauftragsverarbeiters in Textform. Der Auftraggeber kann der Änderung innerhalb von 14 Tagen nach Zugang der Information aus einem wichtigen datenschutzrechtlichen Grund widersprechen.
3. Widerspricht der Auftraggeber und lässt sich die beabsichtigte Leistung ohne den betreffenden Unterauftragsverarbeiter nicht mit zumutbarem Aufwand erbringen, steht beiden Parteien ein Sonderkündigungsrecht für den Hauptvertrag zum Wirksamwerden der Änderung zu.
4. Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter vertraglich auf dieselben Datenschutzpflichten, die in diesem Vertrag festgelegt sind, insbesondere auf hinreichende Garantien für geeignete technische und organisatorische Maßnahmen (Art. 28 Abs. 4 DSGVO). Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Auftragnehmer gegenüber dem Auftraggeber für dessen Einhaltung.
5. Nicht als Unterauftragsverhältnis im Sinne dieser Regelung gelten Nebenleistungen, die der Auftragnehmer bei Dritten in Anspruch nimmt und die die Verarbeitung der Daten des Auftraggebers nicht zum Gegenstand haben, etwa Telekommunikationsleistungen, Post- und Transportdienstleistungen oder Wartungsleistungen an Endgeräten.

---

§ 6 Übermittlung in Drittländer

1. Eine Verarbeitung der Daten außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums findet ausschließlich bei den in Anlage 3 als solche gekennzeichneten Unterauftragsverarbeitern und ausschließlich im dort beschriebenen Umfang statt.
2. Die Übermittlung ist abgesichert über das EU-US Data Privacy Framework, soweit der Empfänger zertifiziert ist, und in allen übrigen Fällen über EU-Standardvertragsklauseln nach Art. 46 Abs. 2 lit. c DSGVO. Der Auftragnehmer stellt dem Auftraggeber auf Anfrage eine Kopie der jeweils anwendbaren Garantien zur Verfügung.
3. Der Auftragnehmer übermittelt an die in Anlage 3 genannten KI-Anbieter ausschließlich die für die Messung erforderlichen Angaben. Das sind der Markenname, die Domain, die vom Auftraggeber angelegten Keywords und Wettbewerbernamen sowie weitere Freitextangaben, die der Auftraggeber zur Steuerung der Messung hinterlegt, etwa Beschreibungen einer Nische. Keywords und Beschreibungsfelder sind Freitextfelder; ihr Inhalt wird vom Auftraggeber bestimmt. Kontaktdaten der Nutzenden des Auftraggebers, Zugangsdaten, IP-Adressen und Zahlungsdaten werden nicht an diese Empfänger übermittelt.
4. Der Auftragnehmer prüft den Inhalt der Freitextfelder nicht vorab. Der Auftraggeber trägt dafür Sorge, dass er dort keine personenbezogenen Daten einträgt, deren Übermittlung in ein Drittland er nicht wünscht.
5. Die Keywords des Auftraggebers werden zusätzlich an den in Anlage 3 genannten Suchanbieter übermittelt. Übermittelt wird ausschließlich die Suchanfrage selbst.

   Gegenstand des Dienstes ist die Messung der Sichtbarkeit von Marken. Dass dabei Markennamen und Suchbegriffe an Suchmaschinen und KI-Anbieter gerichtet werden, ist der Zweck der Leistung und die Weisung des Auftraggebers. Das gilt auch für Marken, die den Namen einer natürlichen Person tragen: Ein solcher Name ist zwar ein personenbezogenes Datum, seine Verwendung als Suchanfrage entspricht aber genau der Nutzung, für die der Markeninhaber ihn veröffentlicht hat.

   Untersagt sind dagegen Eingaben, die über diesen Zweck hinausgehen: Angaben zu Privatpersonen ohne Bezug zur getrackten Marke, Kontaktdaten, Anschriften, Kennnummern sowie Daten nach Art. 9 und Art. 10 DSGVO. Ein entsprechender Hinweis ist an den Eingabefeldern der Anwendung angebracht.

§ 7 Kontrollrechte des Auftraggebers

1. Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen einschließlich Inspektionen (Art. 28 Abs. 3 lit. h DSGVO).
2. Der Nachweis erfolgt vorrangig durch Auskunft in Textform, durch Vorlage der Beschreibung der technischen und organisatorischen Maßnahmen nach Anlage 2 oder durch Vorlage eines aktuellen Testats, Berichts oder Berichtsauszugs einer unabhängigen Stelle, soweit ein solcher vorliegt.
3. Reichen diese Nachweise im Einzelfall nicht aus, kann der Auftraggeber nach angemessener Vorankündigung von mindestens 30 Tagen zu den üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs eine Überprüfung vor Ort durchführen oder durch einen zur Verschwiegenheit verpflichteten Prüfer durchführen lassen, der kein Wettbewerber des Auftragnehmers sein darf. Ohne besonderen Anlass ist eine solche Überprüfung einmal je Kalenderjahr vorzunehmen.

   Die Ankündigungsfrist und die Beschränkung auf eine Prüfung je Kalenderjahr gelten nicht, wenn eine Verletzung des Schutzes personenbezogener Daten eingetreten ist, wenn ein begründeter Verdacht auf einen erheblichen Verstoß gegen diesen Vertrag besteht oder wenn eine Aufsichtsbehörde die Prüfung verlangt. In diesen Fällen ist die Prüfung mit angemessener, den Umständen entsprechender Vorankündigung zulässig.
4. Für den Aufwand einer Überprüfung, die über den Umfang nach Absatz 3 hinausgeht und die nicht durch einen Verdacht auf einen Verstoß des Auftragnehmers veranlasst ist, kann der Auftragnehmer eine angemessene Vergütung verlangen.

§ 8 Löschung und Rückgabe nach Beendigung

1. Nach Beendigung des Hauptvertrages löscht der Auftragnehmer die im Auftrag verarbeiteten personenbezogenen Daten oder gibt sie nach Wahl des Auftraggebers zurück, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten eine Verpflichtung zur Speicherung besteht (Art. 28 Abs. 3 lit. g DSGVO).
2. Der Auftraggeber kann bis zum Ablauf von 30 Tagen nach Beendigung des Hauptvertrages die Herausgabe der Daten in einem gängigen maschinenlesbaren Format verlangen. Danach erfolgt die Löschung nach den in Anlage 1 genannten Fristen.
3. Von der Löschung nicht erfasst sind die Daten, die der Auftragnehmer nach § 1 Ziffer 2 in eigener Verantwortlichkeit verarbeitet, insbesondere die Abrechnungsdaten und die dafür geltenden gesetzlichen Aufbewahrungspflichten, sowie Daten in aggregierter und anonymisierter Form, die keinen Personenbezug mehr aufweisen und deren Verwendung im Hauptvertrag geregelt ist.
4. Die Löschung aus Datensicherungen erfolgt nicht sofort, sondern mit dem regulären Ablauf des jeweiligen Sicherungszyklus, spätestens jedoch zwei Monate nach der Löschung im Produktivsystem. Bis dahin sind die Daten gesperrt und werden ausschließlich zur Wiederherstellung im Störungsfall verarbeitet.
5. Der Auftragnehmer weist die Löschung auf Anfrage in Textform nach.

§ 9 Haftung und Schlussbestimmungen

1. Für die Haftung der Parteien gilt Art. 82 DSGVO. Im Übrigen gelten die Haftungsregelungen des Hauptvertrages.
2. Änderungen und Ergänzungen dieses Vertrages sowie seiner Anlagen bedürfen der Textform. Das gilt auch für die Aufhebung dieses Formerfordernisses.
3. Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen die Regelungen dieses Vertrages vor, soweit sie die Verarbeitung personenbezogener Daten betreffen.
4. Sollte eine Bestimmung dieses Vertrages unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien ersetzen die unwirksame Bestimmung durch eine wirksame Regelung, die dem wirtschaftlichen Zweck am nächsten kommt.
5. Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist, soweit zulässig vereinbar, Berlin.

Unterschriften

Ort, Datum: ..... Ort, Datum: Berlin, ...

....

Auftraggeber Martin Kulawik (Auftragnehmer)

Anlage 1: Gegenstand der Verarbeitung

1. Zweck der Verarbeitung

Bereitstellung des Dienstes achtung.app: laufende Messung, Auswertung und Darstellung der Sichtbarkeit der vom Auftraggeber angelegten Marken in KI-Assistenten und Suchsystemen, einschließlich Benachrichtigungen, Berichten und Nutzerverwaltung.

2. Art der Verarbeitung

Erheben, Erfassen, Organisieren, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Übermitteln an die in Anlage 3 genannten Empfänger, Einschränken, Löschen und Vernichten.

3. Kategorien betroffener Personen

- Beschäftigte und Beauftragte des Auftraggebers, die ein Nutzerkonto besitzen
- natürliche Personen, die vom Auftraggeber in Freitextfeldern der Anwendung benannt werden, etwa in Keywords, Wettbewerbernamen oder Beschreibungsfeldern, im Rahmen der Einschränkung nach § 6 Ziffer 5
- Inhaber einer Personenmarke, sofern der Auftraggeber eine solche als Marke anlegt
- natürliche Personen, deren Daten in einem vom Auftraggeber verbundenen Analysekonto (Google Search Console, Google Analytics 4) enthalten sind, soweit der Auftraggeber eine solche Verbindung herstellt

4. Kategorien personenbezogener Daten

Kategorie	Beispiele
Bestandsdaten der Nutzenden	Name, E-Mail-Adresse, Rolle, Spracheinstellung, Zugehörigkeit zum Team
Zugangsdaten	Passwort-Hash, Sitzungskennung, Kennung der verbundenen SSO-Identität
Nutzungsdaten im Konto	Zeitstempel und Einträge des Audit-Logs, jeweils mit IP-Adresse und User-Agent der handelnden Person
Inhaltsdaten des Auftraggebers	Markenname, Domain, Keywords, Wettbewerber, Notizen, Beschreibungsfelder, erzeugte Berichte. Keywords, Notizen und Beschreibungsfelder sind Freitextfelder, deren Inhalt der Auftraggeber bestimmt
Daten verbundener Konten	OAuth-Token und abgerufene Kennzahlen aus Google Search Console und Google Analytics 4, sofern verbunden

Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO und Daten nach Art. 10 DSGVO sind nicht Gegenstand des Auftrags. Ihre Eingabe in die Anwendung ist dem Auftraggeber nach § 3 Ziffer 7 dieses Vertrages untersagt.

Nicht Gegenstand dieser Anlage und dieses Vertrages sind die Daten, die der Auftragnehmer nach § 1 Ziffer 2 in eigener Verantwortlichkeit verarbeitet. Das sind insbesondere die Abrechnungsdaten einschließlich der Stripe-Kundenkennung, die Server- und Sicherheitsprotokolle der Infrastruktur sowie die Support-Korrespondenz. Für sie gilt die Datenschutzerklärung, nicht dieser Vertrag.

5. Dauer der Verarbeitung und Löschfristen

Die Verarbeitung dauert für die Laufzeit des Hauptvertrages. Es gelten die folgenden Fristen, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen:

Datenkategorie	Frist
Kontodaten (Name, E-Mail, Einstellungen)	Dauer des Kontos plus 30 Tage nach Löschung
Audit-Log (Aktivitätsprotokoll des Teams)	Dauer des Kontos; wird mit dem Team gelöscht
Sichtbarkeitswerte, Quellen und Berichte	Dauer des Kontos plus 90 Tage

Die Löschung nicht verlängerter oder gekündigter Konten ist als täglich laufender automatischer Vorgang umgesetzt.

Für die Daten, die der Auftragnehmer nach § 1 Ziffer 2 in eigener Verantwortlichkeit verarbeitet, gelten eigene Fristen: Server-Logdateien 30 Tage, Support-Korrespondenz 3 Jahre nach dem letzten Kontakt, Abrechnungsdaten 8 Jahre für Buchungsbelege nach § 147 Abs. 3 AO. Diese Fristen sind in der Datenschutzerklärung geregelt und hier nur zur Einordnung genannt.

Anlage 2: Technische und organisatorische Maßnahmen

Art. 32 DSGVO

Stand: 18.08.2026

1. Vertraulichkeit

Zutrittskontrolle. Der Betrieb erfolgt auf einem virtuellen Server der STRATO AG, Berlin, in einem Rechenzentrum der STRATO AG in Deutschland. Der physische Zutritt liegt in der Verantwortung des Rechenzentrumsbetreibers. Eigene Hardware des Auftragnehmers verarbeitet keine Daten des Auftraggebers im Produktivbetrieb.

Zugangskontrolle. Der Zugang zur Anwendung setzt eine persönliche Anmeldung voraus. Passwörter werden ausschließlich als Hash mit dem Verfahren bcrypt gespeichert. Sitzungsdaten werden verschlüsselt abgelegt. Auf Wunsch kann die Anmeldung über eine vom Auftraggeber betriebene SSO-Verbindung erfolgen und für dessen Konto erzwungen werden. Der administrative Zugang zum Server ist auf den Auftragnehmer beschränkt und erfolgt ausschließlich über Schlüsselauthentifizierung; die Anmeldung mit Passwort ist abgeschaltet. Zusätzlich ist der Zugang auf eine festgelegte Liste von IP-Adressen begrenzt, sodass eine Anmeldung von beliebigen Netzen aus auch mit gültigem Schlüssel nicht möglich ist.

Zugriffskontrolle. Innerhalb der Anwendung besteht eine rollenbasierte Rechteverwaltung. Zugriffe sind auf das Team des Auftraggebers begrenzt; ein teamübergreifender Lesezugriff ist nicht vorgesehen. Für Entwicklung, Wartung und Fehleranalyse setzt der Auftragnehmer ein KI-gestütztes Programmierwerkzeug ein, dessen Datenbankzugriff über ein eigenes Konto mit spaltengenau vergebenen Leserechten technisch beschränkt ist. Personenbezogene Felder sind diesem Konto entzogen; ein vorgeschalteter Filter weist Abfragen auf solche Felder zusätzlich ab. Die Einzelheiten sind im Verzeichnis von Verarbeitungstätigkeiten zum Entwicklungszugriff dokumentiert.

Trennungskontrolle. Die Daten aller Auftraggeber liegen in einer gemeinsamen Datenbank und werden logisch über eine Mandantenkennung getrennt. Die Trennung ist in der Anwendung durchgesetzt und durch automatisierte Tests abgesichert.

Verschlüsselung besonders kritischer Zugangsdaten. Die Zugangs- und Aktualisierungstoken für vom Auftraggeber verbundene Fremdkonten (Google Search Console, Google Analytics 4, Matomo) werden nicht im Klartext gespeichert. Sie werden auf Anwendungsebene mit AES-256 verschlüsselt in der Datenbank abgelegt; der Schlüssel liegt außerhalb der Datenbank in der Anwendungskonfiguration. Ein Lesezugriff auf die Datenbank allein gibt diese Token daher nicht preis.

Pseudonymisierung und Datenminimierung. An die in Anlage 3 genannten Anbieter werden nur die für die jeweilige Abfrage erforderlichen Angaben übermittelt: Markenname, Domain, Keywords, Wettbewerbernamen sowie weitere vom Auftraggeber hinterlegte Freitextangaben wie Nischenbeschreibungen. Kontakt-, Zugangs- und Zahlungsdaten der Nutzenden werden nicht übermittelt. Auswertungen über mehrere Auftraggeber hinweg erfolgen ausschließlich aggregiert und unter Anwendung von k-Anonymitätsschwellen. Ob das Ergebnis anonym ist, bewertet der Auftragnehmer bezogen auf den jeweiligen Veröffentlichungskontext und den Empfängerkreis; die Schwelle allein wird nicht als Beleg der Anonymität behandelt.

2. Integrität

Weitergabekontrolle. Der Zugriff auf die Anwendung ist ausschließlich über TLS möglich; unverschlüsselte Aufrufe werden auf die verschlüsselte Adresse umgeleitet. Der Dienst sendet HTTP Strict Transport Security mit einer Gültigkeit von sechs Monaten einschließlich Subdomains sowie eine Content Security Policy. Datenbank, Warteschlange und Zwischenspeicher sind ausschließlich lokal auf dem Server erreichbar und nicht aus dem Netz aufrufbar. Ausgehende Abrufe unterliegen einer Prüfung gegen interne Netzbereiche.

Eingabekontrolle. Sicherheitsrelevante Vorgänge im Konto des Auftraggebers werden mit Zeitpunkt, handelndem Nutzerkonto, IP-Adresse und User-Agent in einem Audit-Log protokolliert. Änderungen an der Anwendung selbst sind über die Versionsgeschichte des Quellcodes nachvollziehbar.

3. Verfügbarkeit und Belastbarkeit

Wiederherstellbarkeit. Der Auftragnehmer sichert die Daten täglich. Die Sicherungen werden verschlüsselt auf einem Speicherdienst der Hetzner Online GmbH in Deutschland abgelegt und liegen damit räumlich getrennt vom Produktivsystem. Die Aufbewahrungsdauer der Sicherungen beträgt zwei Monate. Aus der täglichen Sicherung folgt ein maximal tolerierter Datenverlust (RPO) von 24 Stunden. Als Zielwert für die Wiederherstellungszeit (RTO) nennt der Auftragnehmer vier Stunden; die Herleitung und ihre Grenzen stehen im Nachweis unten.

Nachweis der Wiederherstellung. Die ausgelagerte Sicherung wurde vollständig zurückgelesen und wiederhergestellt. Der Test lief am 18.08.2026 von 11:30 bis 12:05 Uhr (MESZ) und dauerte damit 35 Minuten von der Entschlüsselung bis zur geprüften Verfügbarkeit der Daten. Die wiederhergestellten Daten waren vollständig. Zuvor war bereits eine Wiederherstellung der Datenbank aus einer lokal vorgehaltenen Sicherung im Ernstfall erfolgreich verlaufen.

Damit ist die Wiederherstellbarkeit im Sinne von Art. 32 Abs. 1 lit. c DSGVO nicht nur eingerichtet, sondern für die ausgelagerte Kette nachgewiesen. Nachgewiesen ist damit die Wiederherstellung des Datenbestands. Ein vollständiger Ausfalltest einschließlich Ersatzserver, Betriebssystem, Anwendung und Konfiguration ist noch nicht erfolgt. Der Auftragnehmer nennt daher als Zielwert für die Wiederherstellungszeit (RTO) vier Stunden. Dieser Zielwert ist keine vertragliche Zusage; er wird überprüft, sobald ein vollständiger Ausfalltest durchgeführt wurde.

Wiederkehrende Überprüfung. Der Test wird vierteljährlich wiederholt und mit Datum, Dauer, Umfang und Ergebnis in der folgenden Übersicht vermerkt. Damit besteht ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit nach Art. 32 Abs. 1 lit. d DSGVO. Nächster Test: spätestens 18.11.2026.

Datum	Quelle	Dauer	Ergebnis
18.08.2026	Ausgelagerte, verschlüsselte Sicherung bei der Hetzner Online GmbH	35 Minuten	Vollständig wiederhergestellt

Belastbarkeit. Verarbeitungen erfolgen über eine Warteschlange mit definierten Zeitüberschreitungen und Wiederholungen, sodass die Störung eines externen Anbieters nicht zum Verlust bereits erhobener Daten führt. Ausfälle einzelner KI-Anbieter führen zu einer Lücke in der Messreihe, nicht zum Ausfall des Dienstes.

Protokollierung. Anwendungsfehler werden protokolliert und ausgewertet.

4. Verfahren zur regelmäßigen Überprüfung

- Die datenschutzrelevanten Zugriffsbeschränkungen sind durch automatisierte Tests abgesichert, die bei jedem Testlauf mitlaufen.
- Nach jeder Datenbankmigration wird automatisch geprüft, ob die vergebenen Leserechte des eingeschränkten Datenbankkontos noch zum Schema passen, und zwar in beide Richtungen.
- Der Auftragnehmer führt ein Verzeichnis von Verarbeitungstätigkeiten und dokumentiert Verletzungen des Schutzes personenbezogener Daten nach Art. 33 Abs. 5 DSGVO.

5. Auftragskontrolle

Die Einbindung von Unterauftragsverarbeitern erfolgt nach § 5 dieses Vertrages. Der aktuelle Stand ist in Anlage 3 dokumentiert. Der Auftragnehmer prüft vor der Einbindung, ob der Unterauftragsverarbeiter hinreichende Garantien im Sinne von Art. 28 Abs. 1 DSGVO bietet.

6. Bekanntes Restrisiko: keine Verschlüsselung ruhender Daten

Sachverhalt. Auf dem Produktivserver ist keine Verschlüsselung des Datenträgers auf Betriebssystemebene eingerichtet. Datenbank und Dateiablage liegen unverschlüsselt auf dem virtuellen Datenträger. Die Datensicherungen sind davon nicht betroffen; sie werden verschlüsselt abgelegt.

Abwägung. Der Auftragnehmer hat die Einrichtung geprüft und bewusst davon abgesehen. Tragend sind folgende Erwägungen: Der Datenträger liegt in einem Rechenzentrum mit Zutrittskontrolle durch den Betreiber. Datenbank, Warteschlange und Zwischenspeicher sind ausschließlich lokal erreichbar. Der administrative Zugang ist auf Schlüsselauthentifizierung aus festgelegten Netzen beschränkt. Eine Verschlüsselung auf Betriebssystemebene schützt in dieser Aufstellung im Wesentlichen gegen den physischen Zugriff auf den Datenträger, während der Schlüssel im laufenden Betrieb ohnehin im Arbeitsspeicher des Systems vorliegt; gegen die realistischen Angriffswege, nämlich den unbefugten Zugriff über das Netz oder über ein kompromittiertes Konto, wirkt sie nicht.

Bewertung. Der Auftragnehmer stuft das verbleibende Risiko nach Art. 32 Abs. 1 DSGVO als vertretbar ein. Die Maßnahme steht nach seiner Einschätzung nicht im Verhältnis zu dem Schutz, den sie über die bereits getroffenen Maßnahmen hinaus bewirkt. Der Auftraggeber ist auf diesen Umstand hiermit ausdrücklich hingewiesen. Bei der Außerbetriebnahme von Datenträgern ist der Auftragnehmer auf die Löschverfahren des Rechenzentrumsbetreibers angewiesen.

Anlage 3: Unterauftragsverarbeiter

Stand: 18.08.2026

1. Betrieb der Anwendung

Gesellschaft	Dienst	Verarbeitungsort	Rolle
STRATO AG, Berlin	Virtueller Server, Rechenzentrum der STRATO AG	Deutschland	Auftragsverarbeiter
Hetzner Online GmbH, Gunzenhausen	Speicherdienst für die verschlüsselten Datensicherungen	Deutschland	Auftragsverarbeiter

2. KI-Anbieter für die Sichtbarkeitsmessung

Übermittelt werden ausschließlich Markenname, Keyword und Domain sowie die vom Auftraggeber in Freitextfeldern eingegebenen Angaben.

Der Auftragnehmer nutzt bei allen Anbietern die regulären Zugänge ohne individuell verhandelte Vereinbarung und ist in Deutschland niedergelassen. Maßgeblich sind daher die veröffentlichten Standardbedingungen der Anbieter für Kundinnen und Kunden im EWR. Die folgenden Angaben geben deren Stand am 18.08.2026 wieder.

Gesellschaft	Dienst	Rolle	Vertragsgrundlage und Transfermechanismus
OpenAI Ireland Ltd., Irland	OpenAI API (Chat- und Responses-Endpunkte)	Auftragsverarbeiter	Für Kundinnen und Kunden im EWR ist OpenAI Ireland Ltd. Vertragspartner. Das Data Processing Addendum gilt für API-Kunden; Weiterübermittlungen an Konzerngesellschaften außerhalb des EWR erfolgen auf Grundlage von EU-Standardvertragsklauseln oder eines Angemessenheitsbeschlusses. Der Auftragnehmer ruft die Endpunkte /v1/chat/completions und /v1/responses auf und setzt dabei `store: false`, sodass OpenAI keinen abrufbaren Anwendungszustand vorhält. Davon unabhängig führt OpenAI Protokolle zur Missbrauchserkennung, die in der Regel bis zu 30 Tage aufbewahrt und aus rechtlichen oder Sicherheitsgründen im Einzelfall länger gespeichert werden können
Google Cloud EMEA Limited, Velasco, Clanwilliam Place, Dublin 2, Irland	Gemini Developer API (generativelanguage.googleapis.com), kostenpflichtiger Tarif über Cloud Billing	Auftragsverarbeiter	Vertragspartner ist ausweislich der Rechnungsstellung die Google Cloud EMEA Limited mit Sitz in Irland. Es gilt das "Data Processing Addendum for Products Where Google is a Data Processor". Eingaben und Antworten werden im kostenpflichtigen Tarif nicht zur Produktverbesserung genutzt; für Kundinnen und Kunden im EWR erstrecken die Bedingungen diese Datenregeln auch auf kostenlose Kontingente
Anthropic Ireland, Limited, Irland	Anthropic Messages API	Auftragsverarbeiter	Für den EWR ist Anthropic Ireland, Limited Vertragspartner. Das Data Processing Addendum ist durch Verweis Bestandteil der Commercial Terms und enthält EU-Standardvertragsklauseln; es gilt irisches Recht
Perplexity AI, Inc., USA	Perplexity API	Auftragsverarbeiter	Das Data Processing Addendum ist Bestandteil der API-Bedingungen. Perplexity ist unter dem EU-US Data Privacy Framework zertifiziert; ergänzend sind EU-Standardvertragsklauseln (Modul 2 und 3) einbezogen
X.AI LLC, USA	xAI API (nur in den Tarifen Pro und Enterprise)	Auftragsverarbeiter	Das Data Processing Addendum bezieht die EU-Standardvertragsklauseln (Modul 2 und 3) ein; es gilt irisches Recht
Mistral AI SAS, Frankreich	Mistral API (nur in den Tarifen Pro und Enterprise)	Auftragsverarbeiter	Data Processing Addendum nach DSGVO. Mistral speichert die Daten standardmäßig in der Europäischen Union, schließt je nach Funktion und eingesetztem Unterauftragnehmer vorübergehende Übermittlungen in Drittländer jedoch nicht aus; dafür gelten die Garantien des Addendums

3. Weitere Datenquellen

Gesellschaft	Dienst	Rolle	Vertragsgrundlage und Transfermechanismus
Brave Software, Inc., USA	Brave Search API, Abfrage von Suchergebnissen zu Keywords des Auftraggebers	siehe Hinweis unten	Brave stellt für die Brave Search API ein Data Processing Addendum bereit, ordnet sich hinsichtlich der übermittelten Suchanfragen jedoch ausdrücklich nicht die Rolle eines Auftragsverarbeiters zu und weist die Verantwortung für die Rechtmäßigkeit der Anfragen dem Kunden zu. Für Unternehmenskunden bietet Brave einen Betrieb ohne Speicherung der Anfragen (Zero Data Retention) an

Hinweis zu openrouteservice. Für die Darstellung des Einzugsgebiets einer Marke ruft der Auftragnehmer beim Dienst openrouteservice der HeiGIT gGmbH, Heidelberg, ein Erreichbarkeitspolygon ab. Übermittelt werden dabei ausschließlich das Koordinatenpaar des vom Auftraggeber angegebenen Standorts der Marke, die Fortbewegungsart und eine Zeitspanne in Minuten. Weder Name, Kennung, Anschrift, Keyword noch sonstige Angaben zum Auftraggeber oder zu betroffenen Personen werden übermittelt. Ein Koordinatenpaar kann für sich genommen einen Personenbezug aufweisen, etwa wenn es die Wohn- oder Praxisanschrift eines Einzelunternehmens bezeichnet. Ohne Namen, Kennung oder sonstige Zusatzangabe ist dem Empfänger eine Zuordnung zu einer bestimmten Person nach Einschätzung des Auftragnehmers nicht möglich; HeiGIT selbst behandelt Standortdaten allgemein als möglicherweise personenbezogen. Die Verarbeitung findet in Deutschland statt.

Bewertung des Auftragnehmers: Das Koordinatenpaar stammt aus der vom Auftraggeber selbst angegebenen, regelmäßig veröffentlichten Geschäftsadresse der Marke. Es wird ohne Namen, Kennung oder sonstige Zusatzangabe übermittelt, sodass dem Empfänger eine Zuordnung zu einer bestimmten Person nicht möglich ist. Auch wenn die Koordinate im Einzelfall auf die Wohnanschrift eines Einzelunternehmens verweisen kann, bleibt der Eingriff auf das beschränkt, was der Markeninhaber ohnehin veröffentlicht hat. Der Empfänger sitzt in Deutschland, eine Drittlandübermittlung findet nicht statt.

Einordnung: HeiGIT betreibt openrouteservice als öffentlich zugänglichen Dienst nach eigenen Zwecken und Mitteln und verarbeitet die abgerufenen Koordinaten nicht im Auftrag des Auftragnehmers. HeiGIT ist deshalb kein Unterauftragsverarbeiter, sondern eigenständig Verantwortlicher; die Abfrage ist eine Übermittlung an einen Dritten. Rechtsgrundlage der Übermittlung ist Art. 6 Abs. 1 lit. b DSGVO, weil die Darstellung des Einzugsgebiets Teil der vertraglich vereinbarten Leistung ist. Die Übermittlung ist in der Datenschutzerklärung ausgewiesen. Der Auftragnehmer prüft daneben den Eigenbetrieb des Dienstes, der die Übermittlung vollständig entfallen ließe.

Hinweis zu Brave. Übermittelt werden die vom Auftraggeber angelegten Keywords. Soweit diese im Einzelfall personenbezogene Daten enthalten, steht Braves Selbsteinordnung einer Verarbeitung im Auftrag entgegen.

In den regulären Tarifen speichert Brave Suchanfragen nach eigenen Angaben bis zu 90 Tage. Die angebotene Speicherfreiheit (Zero Data Retention) ist ausschließlich Kundinnen und Kunden mit individuellem Unternehmenstarif vorbehalten und wird auf Anfrage beim Support freigeschaltet.

Bewertung des Auftragnehmers: Übermittelt wird die Suchanfrage, also der Markenname oder ein Suchbegriff, ohne Konto-, Kontakt- oder Zahlungsdaten und ohne eine Kennung des Auftraggebers oder einer betroffenen Person. Trägt eine Marke den Namen einer natürlichen Person, bleibt dieser Name ein personenbezogenes Datum; das Risiko für die betroffene Person ist jedoch gering: Die Anfrage gibt nichts preis, was der Markeninhaber nicht selbst veröffentlicht hat, und sie entspricht der Abfrage, die jede Person bei einer Suchmaschine auslösen würde. Eine Zuordnung der Anfrage zu einer bestimmten Person ist Brave nach dessen Angaben nicht möglich.

Der Auftragnehmer hat den Wechsel in einen Unternehmenstarif mit Zero Data Retention sowie den Wechsel der Suchquelle geprüft und beides als unverhältnismäßig zum beschriebenen Risiko verworfen. Ergriffen wurde stattdessen die Beschränkung der zulässigen Eingaben nach § 6 Ziffer 5 nebst Hinweis an den Eingabefeldern. Der Auftragnehmer behält sich den Wechsel der Suchquelle vor, falls sich die Bedingungen von Brave oder die Art der eingegebenen Keywords wesentlich ändern.

4. Zahlungsabwicklung

Gesellschaft	Dienst	Rolle	Vertragsgrundlage und Transfermechanismus
Stripe Technology Company Limited, One Wilton Park, Wilton Place, Dublin 2, Irland	Abwicklung der Zahlungen des Auftraggebers	eigener Verantwortlicher beziehungsweise Auftragsverarbeiter des Auftragnehmers, nicht Unterauftragsverarbeiter für Kundendaten	Vertragspartner ist die in den Nutzungsbedingungen genannte irische Gesellschaft. Es gilt das Data Processing Agreement von Stripe als Bestandteil der Stripe-Vertragsbedingungen

Die Zahlungsabwicklung gehört nach § 1 Ziffer 2 lit. a zu den Verarbeitungen, die der Auftragnehmer in eigener Verantwortlichkeit vornimmt. Sie ist hier nur der Vollständigkeit halber aufgeführt und nicht Gegenstand dieses Vertrages. Vertragspartner ist die im Hauptvertrag genannte Gesellschaft.

5. Nicht eingesetzt

Für den Versand von E-Mails, die Dateiablage im laufenden Betrieb und die Reichweitenmessung setzt der Auftragnehmer keine externen Dienstleister ein. Mailversand, Dateiablage und die selbst betriebene Reichweitenmessung laufen auf eigener Infrastruktur. Ausgenommen ist die in Ziffer 1 genannte Ablage der Datensicherungen.