Vertrag zur Auftragsverarbeitung (AVV)

nach Art. 28 Datenschutz-Grundverordnung (DSGVO) · Stand: 20. November 2026

Auftraggeber (Verantwortlicher)	Auftragnehmer (Auftragsverarbeiter)
Der Kunde laut Angebot bzw. Auftrag (Name, Firma, Anschrift wie im Angebot angegeben)	Marius Herr, webautomation.media Brüder-Grimm-Straße 10, 36088 Hünfeld webautomation.media@gmail.com · +49 157 52766440

Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien bei der Verarbeitung personenbezogener Daten im Auftrag. Er wird Bestandteil des Hauptvertrags, sobald der Auftraggeber eine Leistung beauftragt, bei der der Auftragnehmer personenbezogene Daten in seinem Auftrag verarbeitet (insbesondere Webseite im Abo mit Kontaktformular, KI-Telefonassistent, Chatbot oder Automatisierung).

§ 1 Gegenstand und Dauer

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen auf Grundlage des Hauptvertrags (Angebot und Auftrag einschließlich der AGB von webautomation.media). Dazu gehören insbesondere die Bereitstellung von Webseiten im Abo einschließlich Kontaktformularen, die Einrichtung und der Betrieb von KI-Telefonassistenten, Chatbots und Automatisierungen sowie deren Betreuung. Dabei verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers im Sinne von Art. 28 DSGVO.

(2) Dieser Vertrag gilt für die Dauer des Hauptvertrags. Er endet nicht, solange der Auftragnehmer noch personenbezogene Daten des Auftraggebers verarbeitet.

§ 2 Art, Zweck und Umfang der Verarbeitung

(1) Art und Zweck der Verarbeitung ergeben sich aus dem Hauptvertrag und Anlage 1. Typisch sind: Entgegennahme, Speicherung und Weiterleitung von Anfragen aus Kontaktformularen; Annahme von Anrufen durch einen KI-Assistenten, Transkription, Zusammenfassung und Weiterleitung als Auftragsnotiz; automatische Übergabe von Anfragen, Auftragsdaten und Terminen an Systeme des Auftraggebers (zum Beispiel Microsoft 365 oder Google Workspace); Beantwortung von Fragen durch einen Chatbot.

(2) Kategorien betroffener Personen und Arten personenbezogener Daten sind in Anlage 1 beschrieben.

(3) Die Verarbeitung findet grundsätzlich in der Europäischen Union bzw. im Europäischen Wirtschaftsraum statt. Eine Verarbeitung in einem Drittland (zum Beispiel in den USA) erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere auf Grundlage eines Angemessenheitsbeschlusses (zum Beispiel EU-US Data Privacy Framework) oder der Standardvertragsklauseln der EU-Kommission.

§ 3 Weisungsrecht des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist durch das Recht der Union oder eines Mitgliedstaats zur Verarbeitung verpflichtet; in diesem Fall teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht verbietet.

(2) Die Weisungen ergeben sich zunächst aus dem Hauptvertrag und diesem Vertrag. Weitere Weisungen erteilt der Auftraggeber in Textform (zum Beispiel per E-Mail).

(3) Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, weist er den Auftraggeber unverzüglich darauf hin. Er darf die Ausführung

der Weisung aussetzen, bis der Auftraggeber sie bestätigt oder ändert.

§ 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet die Daten nur im Rahmen dieses Vertrags und nicht für eigene Zwecke. Kopien werden nur erstellt, soweit dies für die Leistung, zur Datensicherung oder aufgrund gesetzlicher Pflichten erforderlich ist.

(2) Der Auftragnehmer gewährleistet, dass sich alle Personen, die zur Verarbeitung befugt sind, zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Derzeit verarbeitet ausschließlich der Inhaber Marius Herr die Daten.

(3) Der Auftragnehmer trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in Anlage 2 beschrieben sind. Er darf sie weiterentwickeln, solange das Schutzniveau nicht unterschritten wird.

(4) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten Maßnahmen bei der Erfüllung der Rechte betroffener Personen (Art. 12 bis 23 DSGVO). Wendet sich eine betroffene Person direkt an den Auftragnehmer, leitet er die Anfrage unverzüglich an den Auftraggeber weiter.

(5) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation).

(6) Der Auftragnehmer meldet dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich, möglichst innerhalb von 24 Stunden nach Bekanntwerden, und stellt die Informationen nach Art. 33 Abs. 3 DSGVO bereit, soweit sie ihm vorliegen.

(7) Der Auftragnehmer ist als Kleinunternehmen mit weniger als 20 mit der Verarbeitung beschäftigten Personen nicht zur Benennung eines Datenschutzbeauftragten verpflichtet. Ansprechpartner für den Datenschutz ist Marius Herr, webautomation.media@gmail.com.

§ 5 Pflichten und Verantwortung des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO und für die Rechtmäßigkeit der Verarbeitung verantwortlich. Er stellt insbesondere sicher, dass betroffene Personen ordnungsgemäß informiert werden – zum Beispiel durch einen Hinweis zu Beginn eines Anrufs, dass ein KI-Assistent das Gespräch führt und transkribiert, und durch eine passende Datenschutzerklärung auf seiner Webseite.

(2) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

(3) Stellt der Auftraggeber Zugänge zu eigenen Systemen bereit (zum Beispiel Microsoft 365 oder Google Workspace), ist er für deren Vertragsverhältnis mit dem jeweiligen Anbieter verantwortlich. Der Auftragnehmer nutzt solche Zugänge nur im erforderlichen Umfang.

§ 6 Unterauftragsverarbeiter

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

(2) Der Auftragnehmer informiert den Auftraggeber mindestens 14 Tage vorab in Textform über beabsichtigte Änderungen (Hinzuziehung oder Ersetzung). Der Auftraggeber kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen. Kann keine Einigung erzielt werden, sind beide Parteien berechtigt, die betroffene Leistung zum Zeitpunkt der Änderung zu kündigen.

(3) Der Auftragnehmer verpflichtet Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die denen dieses Vertrags entsprechen (Art. 28 Abs. 4 DSGVO). Bei großen Anbietern geschieht dies über deren Auftragsverarbeitungsbedingungen.

§ 7 Kontrollrechte

(1) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung, insbesondere eine Beschreibung der technischen und organisatorischen Maßnahmen und, soweit vorhanden, Zertifikate oder Prüfberichte der Unterauftragsverarbeiter.

(2) Der Auftraggeber kann Überprüfungen einschließlich Inspektionen nach vorheriger Anmeldung mit angemessener Frist (in der Regel 14 Tage), während der üblichen Geschäftszeiten und ohne Störung des Betriebs selbst durchführen oder durch einen zur Verschwiegenheit verpflichteten Prüfer durchführen lassen. Für Kontrollen, die über eine jährliche Überprüfung hinausgehen und nicht durch eine Datenschutzverletzung veranlasst sind, kann der Auftragnehmer eine angemessene Vergütung verlangen.

§ 8 Löschung und Rückgabe

(1) Nach Ende der Leistungen löscht der Auftragnehmer nach Wahl des Auftraggebers alle personenbezogenen Daten oder gibt sie ihm zurück, sofern keine Pflicht zur Speicherung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats besteht. Trifft der Auftraggeber innerhalb von 30 Tagen nach Vertragsende keine Wahl, werden die Daten gelöscht.

(2) Gesprächsaufzeichnungen, Transkripte und Formulardaten werden während der Laufzeit nur so lange gespeichert, wie es für die Weiterleitung an den Auftraggeber erforderlich ist, sofern der Auftraggeber keine längere Speicherung anweist. Die Löschung in den Systemen der Unterauftragsverarbeiter richtet sich nach deren technischen Möglichkeiten.

(3) Auf Verlangen bestätigt der Auftragnehmer die Löschung in Textform.

§ 9 Haftung

Für die Haftung gilt Art. 82 DSGVO. Im Übrigen gelten die Haftungsregelungen des Hauptvertrags, soweit sie mit Art. 82 DSGVO vereinbar sind.

§ 10 Schlussbestimmungen

(1) Bei Widersprüchen gehen in Fragen des Datenschutzes die Regelungen dieses Vertrags denen des Hauptvertrags und der AGB vor.

(2) Änderungen und Ergänzungen bedürfen der Textform. Dieser Vertrag kann auch elektronisch geschlossen werden (Art. 28 Abs. 9 DSGVO), zum Beispiel durch Annahme des Angebots, das auf diesen Vertrag verweist.

(3) Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An die Stelle der unwirksamen Bestimmung tritt die gesetzliche Regelung.

(4) Es gilt deutsches Recht. Gerichtsstand ist, soweit gesetzlich zulässig, der Sitz des Auftragnehmers.

Anlage 1 – Gegenstand der Verarbeitung

Welche Leistungen im Einzelfall gelten, ergibt sich aus dem Angebot.

Leistung	Betroffene Personen	Datenarten
Webseite im Abo mit Kontaktformular	Interessenten und Kunden des Auftraggebers, die das Formular nutzen	Name, Kontaktdaten (E-Mail, Telefon), Inhalt der Anfrage, Zeitpunkt, technische Daten (z. B. IP-Adresse in Server-Logs)
KI-Telefonassistent	Anrufende (Kunden, Interessenten, Lieferanten)	Telefonnummer, Name, Anliegen, Gesprächsaufzeichnung bzw. -transkript, Zusammenfassung, Terminwünsche, Zeitpunkt und Dauer des Anrufs
Automatisierungen	Kunden, Interessenten und Ansprechpartner des Auftraggebers	Kontaktdaten, Anfrage- und Auftragsdaten, Termine, Inhalte von E-Mails und Dokumenten, soweit sie Gegenstand der Automatisierung sind
KI-Chatbot	Besucher der Webseite des Auftraggebers	Eingegebene Nachrichten und Fragen; der Auftraggeber weist darauf hin, keine sensiblen Daten einzugeben

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

• **Zugangs- und Zugriffskontrolle:** Nutzung von Konten mit starken, einzigartigen Passwörtern und Zwei-Faktor-Anmeldung, wo verfügbar; Zugriff ausschließlich durch den Inhaber; Arbeitsgeräte mit Bildschirmsperre und aktuellem Betriebssystem.

• **Übertragungskontrolle:** Verschlüsselte Übertragung (HTTPS/TLS) für Webseiten, Formulare und Schnittstellen.

• **Trennungskontrolle:** Getrennte Projekte, Formulare und Abläufe je Auftraggeber.

• **Eingabekontrolle:** Protokollierung durch die eingesetzten Plattformen (zum Beispiel Ausführungsverläufe von Automatisierungen, Formular-Eingänge).

• **Verfügbarkeit:** Hosting bei etablierten Anbietern mit Redundanz; regelmäßige Sicherung von Projektdateien.

• **Datensparsamkeit:** Verarbeitung nur der für den Zweck nötigen Daten; Demos mit Beispieldaten; Löschung nach Zweckerfüllung.

• **Auswahl von Dienstleistern:** Einsatz von Anbietern mit eigenen Auftragsverarbeitungsbedingungen und, bei Drittlandbezug, geeigneten Garantien nach Art. 44 ff. DSGVO.

Anlage 3 – Unterauftragsverarbeiter

Je nach gebuchter Leistung werden die folgenden Unterauftragsverarbeiter eingesetzt:

Anbieter	Zweck	Ort / Garantie
Netlify, Inc., San Francisco, USA	Hosting von Webseiten, Formular-Verarbeitung (Netlify Forms)	USA; Standardvertragsklauseln der EU-Kommission

Anbieter	Zweck	Ort / Garantie
Google Ireland Limited, Dublin, Irland	E-Mail-Postfach (Gmail), Zustellung von Formular-Eingängen und Auftragsnotizen; ggf. KI-Funktionen (Gemini API) für Chatbots	EU; Verarbeitung in den USA möglich: EU-US Data Privacy Framework / Standardvertragsklauseln
Celonis SE (Make), München, Deutschland	Automatisierungen (nur bei gebuchter Automatisierung)	EU; Unterauftragsverarbeiter gemäß den Bedingungen von Make
Anbieter des KI-Telefonassistenten	Telefonie, Spracherkennung, Gesprächsführung (nur bei gebuchtem KI-Telefonassistenten)	Wird im Angebot konkret benannt; Server in der EU bevorzugt

Hinweis: Dieser Vertrag ist eine Vorlage von webautomation.media. Er ersetzt keine Rechtsberatung.