

Auftragsverarbeitungsvertrag

gemäß Art. 28 DSGVO (AVV) · Muster · Stand: August 2026

Dies ist die als Muster veröffentlichte Standardfassung des Auftragsverarbeitungsvertrages zur Vorabinformation. Die individuellen Angaben zum Auftraggeber sowie zum zugrundeliegenden Haupt- und Wartungsvertrag werden bei Vertragsschluss ergänzt und von beiden Parteien unterzeichnet.

Auftraggeber (Verantwortlicher)

Name / Firma:

Adresse:

E-Mail:

Weisungsberechtigte Person:

(nachfolgend „Auftraggeber“ genannt)

Auftragnehmer (Auftragsverarbeiter)

Marcel Ulbrich, Ulbrich Digital Solutions, tätig unter der Marke Webwerk.ai

Körnerstraße 9, 09130 Chemnitz, Deutschland

kontakt@webwerk.ai · webwerk.ai · USt-IdNr.: DE351141921

(nachfolgend „Auftragnehmer“ genannt)

§1 Gegenstand und Dauer der Verarbeitung

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers im Rahmen der vereinbarten digitalen Dienstleistungen gemäß dem zugrundeliegenden Hauptvertrag.
- (2) Die Verarbeitung beginnt mit Wirksamwerden dieses Vertrages und endet mit Beendigung sämtlicher zugrundeliegender Hauptverträge. Sie umfasst insbesondere auch den Zeitraum des laufenden Hostings sowie der Wartung und Pflege über die Abnahme des Werks hinaus.
- (3) Ort der Verarbeitung ist die Bundesrepublik Deutschland. Eine Verarbeitung in Drittländern findet ausschließlich nach Maßgabe des §5 statt.

§2 Art und Zweck der Verarbeitung

- (1) Gegenstand der Verarbeitung sind folgende Datenkategorien:

- Kontaktdaten der Website-Besucher (Name, E-Mail, Telefon, über Kontaktformulare)

- Zugangsdaten für Server, CMS und Hosting-Systeme
- Technische Daten (IP-Adressen, Log-Dateien des Webserver)
- Domain- und Registrierungsdaten (Name, Anschrift, E-Mail des Domaininhabers)
- Geschäftsdaten des Auftraggebers (z. B. Kundenlisten, Prozessdaten) bei Automatisierungsprojekten
- KI-verarbeitete Daten (Eingaben, Ausgaben) bei KI-Integration
- Sonstige vom Auftraggeber bereitgestellte Inhalte und Daten

(2) Zweck der Verarbeitung ist die Erstellung, Pflege und technische Betreuung der Website, der Betrieb des Hostings und der Domainverwaltung sowie die Umsetzung digitaler Automatisierungs- und KI-Lösungen des Auftraggebers.

(3) Betroffene Personen sind Website-Besucher, Kunden und Interessenten des Auftraggebers sowie Mitarbeiter des Auftraggebers, soweit deren Daten im Rahmen von Automatisierungs- oder KI-Lösungen verarbeitet werden.

(4) Eine gezielte Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO ist nicht Gegenstand dieses Vertrages. Soweit im Einzelfall, insbesondere bei Kontaktformularen von Angehörigen der Heilberufe, gesundheitsbezogene Angaben durch betroffene Personen freiwillig übermittelt werden können, trifft der Auftraggeber die erforderlichen Maßnahmen zur Datenminimierung, insbesondere durch Verzicht auf Freitextfelder zu Beschwerden oder Diagnosen. Der Auftragnehmer setzt in diesen Fällen ergänzende Schutzmaßnahmen um (verschlüsselte Formularübertragung, verkürzte Speicherfristen, restriktive Zugriffsrechte).

(5) Sofern nicht abweichend vereinbart, gelten folgende Löschfristen:

- Anfragen über Kontaktformulare: Löschung 6 Monate nach abschließender Bearbeitung
- Server- und Zugriffs-Logfiles: Löschung nach 7 Tagen
- Backups: Überschreibung nach 30 Tagen

Gesetzliche Aufbewahrungspflichten des Auftraggebers bleiben unberührt und sind von diesem mitzuteilen.

§3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verpflichtet sich, personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers zu verarbeiten, sich selbst zur Vertraulichkeit zu verpflichten und hinzugezogene Dritte entsprechend zu verpflichten, alle erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO umzusetzen, den Auftraggeber unverzüglich zu informieren, wenn eine erteilte Weisung gegen die DSGVO oder andere datenschutzrechtliche Vorschriften verstößt, den Auftraggeber bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO zu unterstützen, insbesondere bei Datenschutz-Folgenabschätzungen und der Meldung von Datenschutzverletzungen, unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen, alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO festgelegten Pflichten zur Verfügung zu stellen sowie Überprüfungen des Auftraggebers oder eines von diesem beauftragten Prüfers zu ermöglichen und dazu beizutragen.

(2) Überprüfungen nach Absatz (1) sind mit einer Frist von 14 Tagen anzukündigen und erfolgen zu üblichen Geschäftszeiten ohne Störung des Betriebsablaufs. Der Auftragnehmer kann den Nachweis auch durch aktuelle Testate, Zertifizierungen oder Berichte unabhängiger Stellen erbringen. Der Aufwand für Überprüfungen, die über eine Überprüfung pro Kalenderjahr hinausgehen, wird nach dem im Hauptvertrag vereinbarten Satz für Zusatzleistungen vergütet.

(3) Der Auftragnehmer ist nicht berechtigt, personenbezogene Daten oder Datenträger des Auftraggebers im Falle von Zahlungsstreitigkeiten oder sonstigen Leistungsstörungen zurückzuhalten. Das zivilrechtliche Zurückbehaltungsrecht nach §273 BGB ist für personenbezogene Daten und die zugehörigen Datenträger ausdrücklich ausgeschlossen.

§4 Technische und organisatorische Maßnahmen (TOM)

(1) Der Auftragnehmer implementiert die in Anlage 1 zu diesem Vertrag beschriebenen technischen und organisatorischen Maßnahmen und hält diese während der gesamten Vertragslaufzeit aufrecht.

(2) Der Auftragnehmer ist berechtigt, die Maßnahmen an den technischen Fortschritt anzupassen, sofern das vereinbarte Schutzniveau dabei nicht unterschritten wird. Wesentliche Änderungen sind dem Auftraggeber in Textform mitzuteilen.

(3) Der Auftragnehmer überprüft die Wirksamkeit der Maßnahmen mindestens jährlich und dokumentiert die Überprüfung.

§5 Unterauftragsverhältnisse

(1) Der Auftraggeber genehmigt den Einsatz folgender Unterauftragsverarbeiter:

Anbieter	Zweck	Standort	Grundlage Drittland
Hetzner Online GmbH	Web-Hosting, Server, Backups	Deutschland (EU)	—
GoDaddy	Domainregistrierung und DNS-Verwaltung	USA	EU-US Data Privacy Framework
UptimeRobot	Verfügbarkeitsüberwachung, Störungsbenachrichtigung	Malta (EU)	EU-Standardvertragsklauseln bei Verarbeitung außerhalb der EU

(2) Der Auftraggeber erteilt seine allgemeine Genehmigung zum Einsatz weiterer Unterauftragsverarbeiter. Der Auftragnehmer informiert den Auftraggeber mindestens 30 Tage vor Beauftragung in Textform. Der Auftraggeber kann innerhalb von 14 Tagen nach Zugang der Information aus wichtigem datenschutzrechtlichen Grund widersprechen. Im Falle eines berechtigten Widerspruchs sind beide Parteien zur außerordentlichen Kündigung des Hauptvertrages berechtigt.

(3) Der Auftragnehmer verpflichtet Unterauftragsverarbeiter zu Datenschutzpflichten, die den Regelungen dieses Vertrages entsprechen, und haftet für deren Verhalten wie für eigenes.

(4) Soweit Unterauftragsverarbeiter personenbezogene Daten außerhalb der EU bzw. des EWR verarbeiten, stellt der Auftragnehmer ein angemessenes Datenschutzniveau sicher, insbesondere durch Zertifizierung nach dem EU-US Data Privacy Framework oder durch Abschluss der EU-Standardvertragsklauseln nebst ergänzenden Schutzmaßnahmen.

(5) Soweit im Rahmen von KI-Integrationen ein selbst gehostetes Sprachmodell auf dem Server des Auftragnehmers eingesetzt wird, erfolgt keine Weitergabe von Daten an externe KI-Anbieter. Der Einsatz externer KI-Dienste erfolgt nur nach vorheriger Information des Auftraggebers und Aufnahme des Anbieters in die Liste nach Absatz (1).

(6) Nicht als Unterauftragsverarbeitung im Sinne dieses Vertrages gelten Nebenleistungen, die der Auftragnehmer für eigene Zwecke in Anspruch nimmt (z. B. Buchhaltung, Signaturdienste, Telekommunikation), sofern dabei keine personenbezogenen Daten des Auftraggebers im Sinne des §2 verarbeitet werden.

§6 Betroffenenrechte

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung von Anfragen betroffener Personen (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch), soweit dies im Rahmen der technischen Möglichkeiten liegt.

(2) Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet dieser die Anfrage unverzüglich an den Auftraggeber weiter und beantwortet sie nicht selbst.

(3) Unterstützungsleistungen, die über den im Hauptvertrag vereinbarten Leistungsumfang hinausgehen, werden nach dem dort vereinbarten Satz für Zusatzleistungen vergütet.

§7 Meldepflichten

(1) Der Auftragnehmer meldet dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich, spätestens jedoch innerhalb von 48 Stunden nach Bekanntwerden, damit der Auftraggeber seine Meldepflichten gemäß Art. 33, 34 DSGVO erfüllen kann.

(2) Die Meldung enthält, soweit verfügbar: eine Beschreibung der Art der Verletzung, die Kategorien und die ungefähre Zahl der betroffenen Personen und Datensätze, eine Beschreibung der wahrscheinlichen Folgen sowie die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung und Schadensminderung.

(3) Der Auftragnehmer dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich der ergriffenen Maßnahmen.

§8 Weisungsrecht

(1) Der Auftraggeber ist gegenüber dem Auftragnehmer weisungsbefugt hinsichtlich der Verarbeitung personenbezogener Daten.

(2) Weisungen sind in Textform zu erteilen. Mündlich erteilte Weisungen sind unverzüglich in Textform zu bestätigen.

(3) Weisungsberechtigt auf Seiten des Auftraggebers ist die im Vertragskopf benannte Person. Änderungen sind dem Auftragnehmer in Textform mitzuteilen.

(4) Der Auftragnehmer dokumentiert erteilte Weisungen und bewahrt die Dokumentation für die Dauer des Vertrages sowie drei Jahre darüber hinaus auf.

§9 Laufzeit, Kündigung und Löschung

(1) Dieser Vertrag ist auf unbestimmte Zeit geschlossen und endet automatisch mit Beendigung sämtlicher zugrundeliegender Hauptverträge.

(2) Der Auftraggeber kann diesen Vertrag außerordentlich kündigen, wenn der Auftragnehmer schwerwiegend gegen datenschutzrechtliche Vorschriften oder gegen die Bestimmungen dieses Vertrages verstößt und den Verstoß trotz Aufforderung nicht innerhalb angemessener Frist abstellt.

(3) Nach Beendigung löscht der Auftragnehmer alle personenbezogenen Daten innerhalb von 30 Tagen oder gibt sie nach Wahl des Auftraggebers in einem gängigen Format zurück, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht.

(4) Auf Anforderung des Auftraggebers legt der Auftragnehmer einen Löschnachweis vor. Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, werden entsprechend der gesetzlichen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahrt.

§10 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrages bedürfen der Textform.

(2) Bei Widersprüchen zwischen diesem Vertrag und den übrigen Vertragsdokumenten gehen in datenschutzrechtlichen Fragen die Regelungen dieses Vertrages vor.

(3) Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein, bleibt die Wirksamkeit des übrigen Vertrages unberührt.

(4) Es gilt das Recht der Bundesrepublik Deutschland.

(5) Bestandteil dieses Vertrages ist Anlage 1 (Technische und organisatorische Maßnahmen).

Ort, Datum · Auftraggeber (Name, Firma)

Ort, Datum · Auftragnehmer
Marcel Ulbrich, Webwerk.ai

Anlage 1: Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

Vertraulichkeit

- Verschlüsselung der Datenübertragung (SSL/TLS) für alle betreuten Websites
- Zugangskontrolle durch sichere Passwörter und Zwei-Faktor-Authentifizierung, wo vom Anbieter unterstützt
- Berechtigungskonzept nach dem Minimalzugriffsprinzip
- Verwendung verschlüsselter Kommunikationskanäle für den Austausch sensibler Daten und Zugangsdaten
- Verschlüsselung der Datenträger der eingesetzten Arbeitsgeräte

Integrität

- Regelmäßige automatisierte Datensicherungen
- Protokollierung von Zugriffen auf produktive Systeme
- Firewall und Sicherheitskonfiguration auf Serverebene
- Zeitnahe Einspielung sicherheitsrelevanter Updates

Verfügbarkeit

- Hosting auf Servern in Deutschland (Hetzner Online GmbH)
- Automatisiertes Monitoring der Verfügbarkeit mit Benachrichtigung bei Ausfällen
- Redundante Stromversorgung und Netzanbindung im Rechenzentrum des Hosting-Anbieters

Trennungskontrolle

- Getrennte Verarbeitung der Daten unterschiedlicher Auftraggeber durch separate Systemumgebungen und Zugriffsrechte
- Trennung von Entwicklungs-, Test- und Produktivumgebung

Belastbarkeit und Wiederherstellung

- Regelmäßige Tests der Datensicherungen auf Wiederherstellbarkeit
- Dokumentiertes Verfahren zur Wiederherstellung nach Datenverlust

Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

- Mindestens jährliche Überprüfung und Aktualisierung der technischen und organisatorischen Maßnahmen
- Dokumentation von Sicherheitsvorfällen und daraus abgeleiteten Maßnahmen
- Prüfung der Datenschutzkonformität eingesetzter Unterauftragsverarbeiter vor Beauftragung