RheinMainTech GmbH
Wilhelm-Theodor-Römheld-Str. 14
55130 Mainz Deutschland
Tel: 06131 - 26 58 333
E-Mail: office@rheinmaintech.com

Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 Abs. 3 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung - DSGVO)

Zwischen

Unternehmen / Name	
Strasse, Hausnummer	
PLZ, Ort	
Vertreten durch	

(nachfolgend **„Verantwortlicher“**)

und

RheinMainTech GmbH
Wilhelm-Theodor-Römheld-Str. 14, 55130 Mainz
Vertreten durch: Sven Kessel (nachfolgend **„Auftragsverarbeiter“**)

Präambel

Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten im Rahmen des zwischen ihnen geschlossenen Webhosting-Vertrags (nachfolgend „Hauptvertrag“). Er findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragsverarbeiters oder durch ihn beauftragte Dritte mit personenbezogenen Daten des Verantwortlichen in Berührung kommen können.

§ 1 Gegenstand, Dauer, Art und Ort der Verarbeitung

(1) Gegenstand: Der Gegenstand der Auftragsverarbeitung ist die Erbringung der im Hauptvertrag spezifizierten Webhosting-Leistungen. Dies umfasst die Speicherung von Daten und Inhalten der vom Verantwortlichen betriebenen Website(s) sowie die Zurverfügungstellung dieser Daten zum Abruf über das Internet.

(2) Dauer: Die Dauer dieses AVV richtet sich nach der Laufzeit des Hauptvertrags.

(3) Art und Zweck der Verarbeitung:

- **Art:** Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Bereitstellung, Sicherung (Backup) und Löschung von Daten.
- **Zweck:** Technischer Betrieb, Wartung und Ermöglichung der Erreichbarkeit der Website(s) und E-Mail-Postfächer des Verantwortlichen über das Internet.

(4) Ort der Verarbeitung: Die Verarbeitung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Eine Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

§ 2 Art der personenbezogenen Daten und Kategorien betroffener Personen

(1) Art der personenbezogenen Daten: Die Verarbeitung kann insbesondere die folgenden Arten von personenbezogenen Daten umfassen, die durch die vom Verantwortlichen auf dem Webspace gespeicherten Inhalte bestimmt werden:

- **Stammdaten von Endnutzern:** z.B. Name, E-Mail-Adresse, Telefonnummern, Adressdaten, Benutzernamen.
- **Kommunikationsdaten:** z.B. Inhalte von E-Mails, Eingaben in Kontaktformularen, Kommentare.
- **Nutzungs-/Verkehrsdaten:** z.B. IP-Adressen der Website-Besucher, Logfiles, Zeitstempel, Browser-Informationen.
- **Vertragsdaten von Endnutzern:** z.B. Bestelldaten in einem Onlineshop, Historie, Zahlungsinformationen (sofern verarbeitet).
- **Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO):** Dem Auftragsverarbeiter ist nicht bekannt, ob der Verantwortliche besondere Kategorien personenbezogener Daten auf dem Webspace verarbeitet. Der Verantwortliche ist allein dafür verantwortlich, die rechtlichen Voraussetzungen für eine solche Verarbeitung zu schaffen.

(2) Kategorien der betroffenen Personen:

- Besucher der Website(s) des Verantwortlichen.
- Kunden, Mitglieder und Interessenten des Verantwortlichen.
- Mitarbeiter des Verantwortlichen.
- Ansprechpartner und Nutzer, die mit dem Verantwortlichen per E-Mail oder Kontaktformular kommunizieren.

§ 3 Technische und Organisatorische Massnahmen (TOMs)

(1) Einhaltung: Der Auftragsverarbeiter verpflichtet sich zur Einhaltung der in Art. 32 DSGVO geforderten technischen und organisatorischen Massnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(2) Dokumentation: Die konkret umgesetzten Massnahmen sind in **Anlage 1** dieses Vertrages detailliert beschrieben. Diese Massnahmen gewährleisten insbesondere die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste.

(3) Anpassung: Der Auftragsverarbeiter behält sich das Recht vor, die Massnahmen der technischen Entwicklung anzupassen, solange das definierte Schutzniveau hierdurch nicht unterschritten wird. Wesentliche Änderungen sind dem Verantwortlichen mitzuteilen.

§ 4 Rechte und Pflichten des Verantwortlichen

(1) Zuständigkeit: Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der betroffenen Personen ist allein der Verantwortliche zuständig (Art. 4 Nr. 7 DSGVO).

(2) Weisungen: Der Verantwortliche erteilt alle Aufträge und Weisungen in der Regel schriftlich oder in Textform (z.B. E-Mail). Mündliche Weisungen sind unverzüglich vom Verantwortlichen schriftlich oder in Textform zu bestätigen.

(3) Kontrolle: Der Verantwortliche hat das Recht, die Einhaltung der in diesem Vertrag getroffenen Vereinbarungen und der TOMs durch den Auftragsverarbeiter zu kontrollieren.

(4) Meldepflicht: Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er in den Auftragsergebnissen Fehler oder Unregelmässigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

§ 5 Pflichten des Auftragsverarbeiters

(1) Weisungsgebundene Verarbeitung: Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschliesslich im Rahmen der getroffenen Vereinbarungen und nach dokumentierten Weisungen des Verantwortlichen. Sofern der Auftragsverarbeiter durch Unionsrecht oder das Recht des Mitgliedstaats, dem er unterliegt, zu einer Verarbeitung verpflichtet ist, teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Vertraulichkeit: Der Auftragsverarbeiter stellt sicher, dass sich alle Personen, die befugt sind, personenbezogene Daten zu verarbeiten (Mitarbeiter und Beauftragte), zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(3) Unterstützung des Verantwortlichen: Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Massnahmen bei der Erfüllung seiner Pflichten, insbesondere:

- bei der Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten (z. B. Auskunft, Löschung).
- bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit, Meldungen, Folgenabschätzung).

(4) Kontrollrechte: Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen (Inspektionen), die vom Verantwortlichen oder einem beauftragten Prüfer durchgeführt werden.

(5) Meldung von Datenschutzverletzungen: Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten unverzüglich, möglichst binnen 48 Stunden nach Bekanntwerden.

(6) Rückgabe und Löschung: Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen entweder alle personenbezogenen Daten oder gibt sie zurück, sofern keine gesetzliche Speicherpflicht besteht.

§ 6 Unterauftragsverhältnisse

(1) Genehmigung: Der Verantwortliche erteilt hiermit die allgemeine schriftliche Genehmigung für die Beauftragung von weiteren Auftragsverarbeitern (Unterauftragsverarbeiter).

(2) Liste der Unterauftragnehmer: Die aktuell eingesetzten Unterauftragsverarbeiter sind in **Anlage 2** aufgeführt.

(3) Änderungen: Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von anderen Auftragsverarbeitern. Der Verantwortliche kann gegen derartige Änderungen binnen einer Frist von 2 Wochen nach Zugang der Information Einspruch erheben.

(4) Vertragskette: Schaltet der Auftragsverarbeiter einen weiteren Auftragsverarbeiter ein, so hat er diesem dieselben Datenschutzpflichten aufzuerlegen, die in diesem Vertrag festgelegt sind.

Anlage 1: Technische und Organisatorische Massnahmen (TOMs)

gemäß Art. 32 DSGVO

Der Auftragsverarbeiter gewährleistet die Sicherheit der Verarbeitung durch die Umsetzung der folgenden Massnahmen. Soweit die Verarbeitung in Rechenzentren von Unterauftragnehmern stattfindet, gelten ergänzend die dort implementierten Sicherheitskonzepte (z.B. ISO 27001 Zertifizierung).

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

(1) Zutrittskontrolle: Massnahmen, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren. **Umsetzung:** Alarmanlagen, gesicherte Schlissanlagen, Schlüsselregelung, Sicherheitspersonal (im Rechenzentrum) sowie Besucherprotokollierung.

(2) Zugangskontrolle: Diese Massnahmen verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. **Umsetzung:** Einsatz sicherer Passwörter (unter Einhaltung von Komplexitätsvorgaben), Zwei-Faktor-Authentifizierung (2FA) für administrative Zugänge, automatische Sperrmechanismen bei Inaktivität sowie Verschlüsselung von Datenträgern.

(3) Zugriffskontrolle: Es werden Massnahmen ergriffen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschliesslich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. **Umsetzung:** Etablierung von Berechtigungskonzepten (Need-to-know-Prinzip), Verwaltung der Benutzerrechte durch Administratoren, Protokollierung von Zugriffen sowie sichere Löschung von Daten nach Vertragsende.

(4) Trennungskontrolle: Massnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. **Umsetzung:** Logische Mandantentrennung in der Software, getrennte Datenbanksysteme sowie die technische Trennung von Produktiv- und Testsystemen.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

(1) Weitergabekontrolle: Massnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. **Umsetzung:** Einsatz von Verschlüsselungsprotokollen (SSL/TLS/HTTPS) für den Webzugriff und E-Mail-Transport sowie Nutzung von VPN für administrative Wartungszugriffe.

(2) Eingabekontrolle: Massnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. **Umsetzung:** Protokollierung und Logging von Systemzugriffen und Änderungen (Server-Logfiles) sowie die Nachvollziehbarkeit von administrativen Eingaben.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

(1) Verfügbarkeitskontrolle: Massnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. **Umsetzung:** Regelmässige Backup-Konzepte (tägliche Sicherung),

Spiegelung von Festplatten (RAID-Systeme), unterbrechungsfreie Stromversorgung (USV) und Klimatisierung in den Rechenzentren sowie Brandschutzmassnahmen.

(2) Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO): Verfahren zur regelmässigen Überprüfung und Wiederherstellung von Daten. **Umsetzung:** Regelmässige Tests der Rückspielbarkeit von Backups (Disaster Recovery Tests).

4. Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

(1) Management: Es bestehen etablierte Datenschutz-Management-Prozesse sowie Prozesse zum Management von Datenschutzvorfällen (Incident-Response-Management).

(2) Evaluierung: Es erfolgt eine regelmässige Überprüfung und Aktualisierung der Sicherheitsmassnahmen. Zudem wird der Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Privacy by Design/Default) berücksichtigt.

Anlage 2: Genehmigte Unterauftragsverarbeiter

Der Verantwortliche genehmigt den Einsatz der folgenden Unterauftragnehmer für die Durchführung der Hosting-Leistungen. Der Auftragsverarbeiter bestätigt, dass mit diesen Dienstleistern Verträge zur Auftragsverarbeitung gemäss Art. 28 DSGVO geschlossen wurden.

Unternehmen	Anschrift	Leistungsbeschreibung	Ort der Verarbeitung
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen	Bereitstellung der Server- und Rechenzentrumsinfrastruktur	Deutschland
OVH GmbH	St. Johanner Str. 41-43, 66111 Saarbrücken	Bereitstellung der Server- und Rechenzentrumsinfrastruktur	Deutschland

§ 7 Schlussbestimmungen

(1) Schriftform: Änderungen und Ergänzungen dieses Vertrags und seiner Anlagen bedürfen der Schriftform.

(2) Salvatorische Klausel: Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, so wird die Wirksamkeit der übrigen Bestimmungen dadurch nicht berührt.

(3) Rechtswahl: Dieser Vertrag unterliegt deutschem Recht.

(4) Gerichtsstand: Ausschliesslicher Gerichtsstand ist Mainz, sofern der Verantwortliche Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.

Für den Verantwortlichen Ort, Datum, Name und Unterschrift	Für RheinMainTech GmbH Ort, Datum, Name und Unterschrift