Vereinbarung zur Auftragsverarbeitung (AVV)

gemäß Art. 28 DSGVO

Diese Vereinbarung ergänzt den zwischen dem Auftragnehmer und dem Auftraggeber geschlossenen Vertrag bzw. die bestehende Geschäftsbeziehung (nachfolgend „Hauptvertrag") und konkretisiert die datenschutzrechtlichen Pflichten der Parteien. Sie gilt für alle Leistungen, bei denen der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers verarbeitet.

§ 1 Gegenstand und Dauer

1.1 Der Auftragnehmer verarbeitet im Rahmen des Hauptvertrages personenbezogene Daten im Auftrag des Auftraggebers. Art, Umfang und Zweck der Verarbeitung ergeben sich aus dem Hauptvertrag sowie aus Anlage 1 dieser Vereinbarung.

1.2 Diese Vereinbarung gilt für alle zum Zeitpunkt des Abschlusses bestehenden und zukünftigen Einzelverträge zwischen den Parteien, bei denen der Auftragnehmer personenbezogene Daten im Auftrag verarbeitet. Kommen neue Leistungen hinzu, die Datenverarbeitung beinhalten, sind diese in Anlage 1 zu ergänzen.

1.3 Die Dauer der Verarbeitung entspricht der Laufzeit des jeweiligen Hauptvertrages. Nach Beendigung gelten die Regelungen dieser Vereinbarung fort, bis alle personenbezogenen Daten gelöscht oder zurückgegeben sind.

§ 2 Weisungsrecht

2.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist durch EU-Recht oder das Recht eines Mitgliedstaats zur Verarbeitung verpflichtet. In diesem Fall informiert der Auftragnehmer den Auftraggeber vorab, sofern das betreffende Recht dies nicht verbietet.

2.2 Weisungen werden in der Regel in Textform (z. B. per E-Mail) erteilt. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

2.3 Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, weist er den Auftraggeber unverzüglich darauf hin. Der Auftragnehmer darf die Durchführung dieser Weisung aussetzen, bis der Auftraggeber sie bestätigt oder ändert.

§ 3 Pflichten des Auftragnehmers

3.1 Der Auftragnehmer gewährleistet, dass die mit der Verarbeitung beauftragten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

3.2 Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Anfragen betroffener Personen (Art. 15–22 DSGVO).

3.3 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der Pflichten nach Art. 32–36 DSGVO (Sicherheit der Verarbeitung, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzung).

3.4 Nach Beendigung des Hauptvertrages löscht der Auftragnehmer alle personenbezogenen Daten des Auftraggebers, sofern keine gesetzliche Aufbewahrungspflicht besteht. Auf Wunsch werden die Daten stattdessen herausgegeben. Löschung oder Herausgabe wird auf Verlangen bestätigt.

3.5 Der Auftragnehmer stellt dem Auftraggeber alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten nach Art. 28 DSGVO erforderlich sind.

§ 4 Technische und organisatorische Maßnahmen

4.1 Der Auftragnehmer trifft die erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO. Die konkreten Maßnahmen sind in Anlage 2 beschrieben.

4.2 Der Auftragnehmer darf alternative Maßnahmen umsetzen, sofern das Sicherheitsniveau nicht unterschritten wird. Wesentliche Änderungen werden dokumentiert.

§ 5 Unterauftragsverarbeiter

5.1 Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, Unterauftragsverarbeiter im Sinne des Art. 28 Abs. 2 DSGVO einzusetzen. Die aktuell eingesetzten Unterauftragsverarbeiter sind in Anlage 3 aufgeführt.

5.2 Der Auftragnehmer informiert den Auftraggeber in Textform über jede beabsichtigte Änderung bei den Unterauftragsverarbeitern. Der Auftraggeber kann innerhalb von 14 Tagen aus sachlichen Gründen Einspruch erheben.

5.3 Kann bei Einspruch keine Einigung erzielt werden, steht dem Auftraggeber ein Sonderkündigungsrecht für den betreffenden Hauptvertrag mit einer Frist von 4 Wochen zu.

5.4 Der Auftragnehmer stellt vertraglich sicher, dass die Unterauftragsverarbeiter die

Datenschutzpflichten dieser Vereinbarung einhalten. Der Auftragnehmer bleibt dem Auftraggeber gegenüber verantwortlich.

5.5 Bei einzelnen Leistungen nutzt der Auftraggeber selbst Plattformen Dritter (z. B. Shopify, Amazon Seller Central, Make.com), auf denen der Auftragnehmer im Auftrag des Auftraggebers tätig wird. Diese Plattformbetreiber sind eigenständige Auftragsverarbeiter oder Verantwortliche gegenüber dem Auftraggeber – nicht Unterauftragsverarbeiter des Auftragnehmers. Die AVV zwischen dem Auftraggeber und diesen Plattformbetreibern liegt in der Verantwortung des Auftraggebers.

§ 6 Datenübermittlung in Drittländer

6.1 Eine Verarbeitung in einem Drittland (außerhalb EU/EWR) erfolgt nur, sofern die Voraussetzungen der Art. 44–49 DSGVO erfüllt sind.

6.2 Soweit Unterauftragsverarbeiter in Drittländern ansässig sind oder Daten dorthin übermitteln, stellt der Auftragnehmer sicher, dass geeignete Garantien vorliegen (z. B. Standardvertragsklauseln, Angemessenheitsbeschluss, verbindliche interne Datenschutzvorschriften). Details finden sich in Anlage 3.

§ 7 Kontrollrechte des Auftraggebers

7.1 Der Auftraggeber hat das Recht, die Einhaltung dieser Vereinbarung zu überprüfen. Der Auftragnehmer stellt die erforderlichen Informationen zur Verfügung.

7.2 Kontrollen vor Ort sind nach angemessener Vorankündigung (mindestens 14 Tage) zu üblichen Geschäftszeiten möglich. Der Auftragnehmer wirkt aktiv mit.

7.3 Alternativ kann der Auftragnehmer aktuelle Prüfberichte, Zertifikate oder Testate unabhängiger Prüfer vorlegen.

7.4 Für Kontrollen, die nicht durch einen Verstoß des Auftragnehmers veranlasst sind, kann eine angemessene Vergütung verlangt werden.

§ 8 Meldepflicht bei Datenschutzverletzungen

8.1 Der Auftragnehmer informiert den Auftraggeber unverzüglich, in der Regel innerhalb von 24 Stunden nach Kenntnisnahme, über jede Verletzung des Schutzes personenbezogener Daten.

8.2 Die Meldung enthält mindestens: Art der Verletzung, betroffene Kategorien und ungefähre Anzahl betroffener Personen und Datensätze, wahrscheinliche Folgen sowie ergriffene oder vorgeschlagene Maßnahmen.

8.3 Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung seiner Meldepflichten gegenüber der Aufsichtsbehörde (Art. 33 DSGVO) und den betroffenen Personen (Art. 34 DSGVO).

§ 9 Schlussbestimmungen

9.1 Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform.

9.2 Sollte eine Bestimmung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien ersetzen die unwirksame Bestimmung durch eine, die dem Zweck am nächsten kommt.

9.3 Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist, soweit gesetzlich zulässig, der Sitz des Auftragnehmers.

Anlage 1 – Angaben zur Verarbeitung

Die nachfolgenden Module beschreiben die möglichen Verarbeitungstätigkeiten. Im jeweiligen Einzelvertrag wird festgelegt, welche Module Anwendung finden.

Modul 1: WordPress Hosting & Wartung
Beschreibung der Verarbeitung: Der Auftragnehmer betreibt die WordPress-Website des Auftraggebers auf einem eigenen Server (VPS) und führt optional technische Wartungsarbeiten durch. Dies umfasst die Speicherung und Bereitstellung aller Website-Daten, Zugriff auf die Datenbank im Rahmen von Updates und Wartung, Erstellung und Verwaltung von Backups (lokal und/oder extern), Einsicht in Server-Logdateien zur Fehlerbehebung und Sicherheitsanalyse. Kategorien betroffener Personen: Besucher und Nutzer der Website, Kunden des Auftraggebers (z. B. bei Bestellungen, Buchungen, Anfragen), Newsletter-Abonnenten, Kontaktpersonen über Formulare, ggf. Mitarbeiter oder Geschäftspartner des Auftraggebers. Kategorien personenbezogener Daten: Stammdaten (Name, Firma), Kontaktdaten (E-Mail, Telefon, Adresse), Nutzungsdaten (IP-Adressen, Zugriffszeiten, Browser-Infos), Inhaltsdaten (Formulareingaben, Kommentare), ggf. Zahlungs- und Vertragsdaten (bei WooCommerce oder vergleichbar).
Modul 2: Backup-Speicherung (Cloud)
Beschreibung der Verarbeitung: Der Auftragnehmer erstellt regelmäßige Backups der Website und/oder Systeme des Auftraggebers und speichert diese verschlüsselt bei einem Cloud-Anbieter. Art und Häufigkeit der Backups ergeben sich aus dem Hauptvertrag. Kategorien betroffener Personen: Alle Personen, deren Daten in den gesicherten Systemen gespeichert sind (identisch mit dem jeweiligen Quell-Modul).

Kategorien personenbezogener Daten: Sämtliche Daten, die zum Zeitpunkt des Backups in den gesicherten Systemen gespeichert waren.

Eingesetzter Dienst: Amazon Web Services (AWS) S3, Region eu-central-1 (Frankfurt am Main). Backups werden per TLS übertragen und serverseitig verschlüsselt gespeichert (AES-256).

Modul 3: E-Commerce-Plattform – Wartung & Verwaltung (z. B. Shopify)
Plattform: Shopify / WooCommerce / andere

Beschreibung der Verarbeitung: Der Auftragnehmer greift im Rahmen der vereinbarten Wartungs- und Verwaltungsleistungen auf das Backend der E-Commerce-Plattform des Auftraggebers zu. Dies kann umfassen: Pflege von Produktdaten und Shop-Einstellungen, Bearbeitung oder Einsicht von Bestellungen und Kundendaten, technische Anpassungen, Plugin-/App-Verwaltung, Fehlerbehebung.

Kategorien betroffener Personen: Kunden und Besteller des Online-Shops, Besucher des Shops, ggf. Mitarbeiter des Auftraggebers mit Backend-Zugang.

Kategorien personenbezogener Daten: Stamm- und Kontaktdaten der Shopkunden (Name, Adresse, E-Mail, Telefon), Bestelldaten (Produkte, Mengen, Preise), Zahlungsinformationen (Zahlungsart, ggf. letzte Ziffern der Kartennummer – soweit über die Plattform sichtbar), Versanddaten (Lieferadressen, Tracking), Nutzungsdaten (IP-Adressen, Browser-Infos).

Hinweis: Die E-Commerce-Plattform selbst (z. B. Shopify Inc.) ist eigenständiger Auftragsverarbeiter gegenüber dem Auftraggeber. Der Abschluss einer AVV zwischen dem Auftraggeber und der Plattform liegt in der Verantwortung des Auftraggebers (vgl. § 5.5).

Modul 4: Automatisierungen
Plattform: Make.com / Zapier / n8n / andere

Beschreibung der Verarbeitung: Der Auftragnehmer erstellt, konfiguriert und/oder verwaltet automatisierte Workflows, die personenbezogene Daten zwischen verschiedenen Systemen des Auftraggebers übertragen und verarbeiten. Dies kann umfassen: Synchronisation von Kundendaten zwischen Systemen (z. B. Shop → CRM → E-Mail-Marketing), automatisierte Benachrichtigungen und E-Mail-Versand, Datenaufbereitung und -weiterleitung, Anbindung von Drittdiensten im Auftrag des Auftraggebers.

Kategorien betroffener Personen: Abhängig von den konkreten Workflows – typischerweise: Kunden, Leads/Interessenten, Newsletter-Abonnenten, Besteller, ggf. Mitarbeiter des Auftraggebers.

Kategorien personenbezogener Daten: Abhängig von den konkreten Workflows – typischerweise: Stamm- und Kontaktdaten, Bestelldaten, Nutzungsdaten, E-Mail-Inhalte und -Metadaten, CRM-Daten.

Hinweis: Die Automatisierungsplattform selbst (z. B. Make.com / Celonis SE) ist eigenständiger Auftragsverarbeiter gegenüber dem Auftraggeber. Der Abschluss einer AVV zwischen dem Auftraggeber und der Plattform liegt in der Verantwortung des Auftraggebers (vgl. § 5.5). Gleiches gilt für alle Drittdienste, die über die Automatisierung angebunden werden.

Modul 5: Marketplace-/Plattform-Setup und -Verwaltung
Plattform: Amazon Seller Central / eBay / andere

Beschreibung der Verarbeitung: Der Auftragnehmer richtet im Auftrag des Auftraggebers ein Verkäufer-/Geschäftskonto auf einer Marktplatz-Plattform ein und/oder verwaltet dieses laufend. Dabei kann der Auftragnehmer Zugriff auf personenbezogene Daten haben, insbesondere auf: Kontodaten des Auftraggebers (Geschäftsadresse, Bankverbindung, Steuerdaten), Bestellungen inkl. Kundenadressen und Zahlungsinformationen (soweit über die Plattform sichtbar), Käuferkommunikation.

Kategorien betroffener Personen: Auftraggeber selbst (Geschäftsdaten), Kunden/Käufer des Auftraggebers auf der Plattform.

Kategorien personenbezogener Daten: Geschäftsdaten des Auftraggebers (Firmenname, Adresse, Bankverbindung, USt-IdNr.), Kundendaten (Name, Lieferadresse, E-Mail), Bestelldaten, ggf. Zahlungsdaten (soweit sichtbar).

Hinweis: Bei einmaligen Setup-Leistungen ohne laufenden Zugriff auf Endkundendaten liegt in der Regel keine Auftragsverarbeitung vor. Dieses Modul ist nur bei laufender Verwaltung mit regelmäßigem Datenzugriff anzukreuzen. Die Plattform selbst (z. B. Amazon) ist eigenständiger Verantwortlicher oder Auftragsverarbeiter gegenüber dem Auftraggeber.

Modul 6: Sonstige Leistungen mit Datenzugriff

Beschreibung der Leistung: [Freitext – z. B. Verwaltung eines CRM-Systems, E-Mail-Marketing-Setup, Analytics-Konfiguration etc.]

Kategorien betroffener Personen: [individuell festlegen]

Kategorien personenbezogener Daten: [individuell festlegen]

Eingesetzte Dienste/Plattformen: [individuell festlegen]

Allgemeiner Hinweis zu besonderen Datenkategorien

Besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1 DSGVO, z. B. Gesundheitsdaten, biometrische Daten, Daten zur politischen Meinung) sind nicht Gegenstand der regulären Verarbeitung. Sollte der Auftraggeber solche Daten über seine Systeme erheben, hat er den Auftragnehmer vorab darüber zu informieren.

Anlage 2 – Technische und organisatorische Maßnahmen (TOMs)

Der Auftragnehmer hat folgende Maßnahmen gemäß Art. 32 DSGVO implementiert. Die Maßnahmen gelten übergreifend für alle in Anlage 1 genannten Module, soweit jeweils anwendbar.

1 – Zutrittskontrolle

(Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen)

- Soweit der Auftragnehmer eigene Server betreibt (z. B. IONOS VPS): Diese stehen in professionellen Rechenzentren mit physischer Zutrittskontrolle (biometrisch, Videoüberwachung, Sicherheitspersonal) durch den Rechenzentrumsbetreiber.
- Der Auftragnehmer arbeitet remote; ein physischer Zutritt zu den Servern findet nicht statt.
- Arbeitsgeräte des Auftragnehmers werden durch Passwort/PIN, ggf. biometrische Sperre und Festplattenverschlüsselung gesichert.

2 – Zugangskontrolle

(Schutz vor unbefugter Nutzung der Systeme)

- Server-Zugang nur über SSH-Schlüssel-Authentifizierung (kein Passwort-Login)
- Admin-Zugänge zu allen Systemen mit starken, einzigartigen Passwörtern
- Zwei-Faktor-Authentifizierung (2FA), soweit die jeweilige Plattform dies unterstützt
- Automatische Sperrung nach fehlgeschlagenen Login-Versuchen (z. B. Fail2Ban, Login-Limiter)
- Passwort-Management über mit einen verschlüsselten Passwort-Manager von 1Passwort mit EU-Region
- Regelmäßige Überprüfung und Aktualisierung von Zugangsdaten

3 – Zugriffskontrolle

(Berechtigte greifen nur auf die ihrem Profil unterliegenden Daten zu)

- Berechtigungskonzept nach dem Prinzip der minimalen Rechte (Least Privilege)
- Getrennte Benutzerkonten für verschiedene Kunden und Projekte
- Keine gemeinsame Nutzung von Zugangsdaten zwischen Kunden
- Bei WordPress: separate Installationen und Datenbanken je Kunde
- API-Schlüssel und Automatisierungs-Zugänge mit geringstmöglichen Berechtigungen

4 – Weitergabekontrolle

(Schutz bei Übertragung und Speicherung)

- SSL/TLS-Verschlüsselung für alle Websites und Schnittstellen (HTTPS)
- Verschlüsselte Verbindungen bei Serverzugriff (SSH, SFTP)
- Backups werden verschlüsselt übertragen und serverseitig verschlüsselt gespeichert (AES-256)
- Cloud-Speicher (z. B. AWS S3) mit aktiviertem „Block Public Access"
- Automatisierungs-Plattformen (z. B. Make.com) kommunizieren ausschließlich über verschlüsselte Verbindungen (HTTPS/TLS)
- E-Mail-Kommunikation mit sensiblen Daten nach Möglichkeit verschlüsselt oder über sichere Übertragungswege

5 – Eingabekontrolle

(Nachvollziehbarkeit von Datenveränderungen)

- Server-Logdateien mit Zugriffs- und Fehlerprotokollen
- Versionierung und Änderungsprotokolle, soweit die eingesetzten Systeme dies unterstützen
- Automatisierungen: Ausführungsprotokolle in der jeweiligen Plattform (z. B. Make.com Scenario Logs)
- WordPress: Aktivitätsprotokoll (sofern im Wartungsumfang enthalten)

6 – Auftragskontrolle

(Verarbeitung nur gemäß Weisungen)

- Vertragliche Regelung durch diese AVV
- Weisungen des Auftraggebers werden dokumentiert
- Mitarbeiter und Auftragnehmer sind auf Vertraulichkeit verpflichtet und im Datenschutz unterwiesen

7 – Verfügbarkeitskontrolle

(Schutz gegen Zerstörung oder Verlust)

- Regelmäßige automatisierte Backups (Art und Häufigkeit gemäß Hauptvertrag)
- Backup-Speicherung räumlich getrennt vom Primärsystem (z. B. AWS S3, EU-Region)
- Rechenzentrum (IONOS) gewährleistet USV, redundante Stromversorgung und Brandschutz
- Server-/Website-Monitoring mit Benachrichtigung bei Ausfällen

8 – Trennungsgebot

(Daten verschiedener Auftraggeber werden getrennt verarbeitet)

- Logische Trennung der Kundendaten (separate Verzeichnisse, Datenbanken, Konten)
- Separate WordPress-Installationen je Kunde
- Separate Zugänge und Projekte je Kunde in Drittplattformen
- Kein gegenseitiger Zugriff zwischen Kundenprojekten

Anlage 3 – Unterauftragsverarbeiter

Der Auftragnehmer setzt die nachfolgend genannten Unterauftragsverarbeiter ein. Nicht jeder Unterauftragsverarbeiter kommt bei jedem Kunden zum Einsatz:

1 – IONOS SE

- Anschrift: Elgendorfer Str. 57, 56410 Montabaur, Deutschland
- Leistung: Server-Infrastruktur (VPS-Hosting) für WordPress-Websites
- Verarbeitungsort: Rechenzentren in Deutschland
- Datenschutzgarantie: AVV mit IONOS SE gem. Art. 28 DSGVO abgeschlossen. IONOS unterliegt als deutsches Unternehmen der DSGVO.
- Infos: https://www.ionos.de/hilfe/datenschutz/

2 – Amazon Web Services EMEA SARL (AWS)

- Anschrift: 38 Avenue John F. Kennedy, L-1855 Luxemburg, Luxemburg
- Leistung: Cloud-Speicher (Amazon S3) für verschlüsselte Backups
- Verarbeitungsort: EU-Region eu-central-1 (Frankfurt am Main)
- Datenschutzgarantie: AWS GDPR DPA ist automatisch Bestandteil der AWS Service Terms. Für eventuelle Datenübermittlungen in Drittländer gelten die darin enthaltenen Standardvertragsklauseln (SCCs) gem. Art. 46 Abs. 2 lit. c DSGVO.

- Infos: https://aws.amazon.com/de/compliance/gdpr-center/

Hinweis zu Plattformen des Auftraggebers

Folgende Plattformen werden nicht als Unterauftragsverarbeiter des Auftragnehmers eingesetzt, sondern sind Dienste, die der Auftraggeber selbst nutzt und auf denen der Auftragnehmer im Auftrag tätig wird. Die AVV mit diesen Anbietern liegt in der Verantwortung des Auftraggebers:

Plattform	**Anbieter**	**AVV/DPA des Anbieters**
Shopify	Shopify International Ltd., Irland	https://www.shopify.com/legal/dpa
Make.com	Celonis SE, Deutschland	https://www.make.com/en/dpa
Amazon Seller Central	Amazon Services Europe S.à r.l., Luxemburg	https://sellercentral.amazon.de (unter Datenschutz)

Der Auftraggeber ist dafür verantwortlich, mit diesen Plattformbetreibern eigene AVVs abzuschließen, soweit er über diese Plattformen personenbezogene Daten verarbeitet.

Änderungen

Der Auftraggeber wird über jede beabsichtigte Änderung der Unterauftragsverarbeiter vorab in Textform informiert (vgl. § 5 dieser Vereinbarung).