

Fabian Digital Services

Auftragsverarbeitungsvertrag (AVV)

Vertrag zur Auftragsverarbeitung gemaess Art. 28 DSGVO

Vertragspartner

Rolle	Angaben
Auftraggeber / Verantwortlicher	Name/Firma: _____ Anschrift: _____ E-Mail: _____ Vertreten durch: _____
Auftragnehmer / Auftragsverarbeiter	Dennis Fabian Fabian Digital Services Speckstrasse 67 76744 Woerth am Rhein E-Mail: dennis@fabian-digital-services.de Website: https://fabian-digital-services.de Datenschutz-Ansprechpartner: Dennis Fabian, E-Mail wie oben Ein Datenschutzbeauftragter ist derzeit nicht benannt, sofern keine gesetzliche Benennungspflicht besteht.

nachfolgend gemeinsam „Parteien“ genannt.

1. Begriffsbestimmungen

Begriffe wie „personenbezogene Daten“, „Verarbeitung“, „Verantwortlicher“, „Auftragsverarbeiter“, „besondere Kategorien personenbezogener Daten“ und „Verletzung des Schutzes personenbezogener Daten“ werden im Sinne der Datenschutz-Grundverordnung (DSGVO), insbesondere Art. 4, Art. 9 und Art. 10 DSGVO, verwendet.

2. Gegenstand, Anwendungsbereich und Rangfolge

2.1 Dieser Vertrag regelt die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers nach Art. 28 DSGVO.

2.2 Der konkrete Leistungsumfang ergibt sich aus dem jeweiligen Hauptvertrag, Dienstleistungsvertrag, Werkvertrag, Angebot, Pflegevertrag oder Einzelauftrag zwischen den Parteien (nachfolgend „Hauptvertrag“). Dieser AVV gilt nur, soweit der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers verarbeitet.

2.3 Nicht unter diesen AVV fallen Datenverarbeitungen, bei denen der Auftragnehmer selbst Verantwortlicher ist, insbesondere eigene Vertragsverwaltung, Rechnungslegung, Buchhaltung, Steuer- und Nachweispflichten, eigene Kundenkommunikation und eigene Rechtsverfolgung oder Rechtsverteidigung.

2.4 Bei Widerspruechen gehen die datenschutzrechtlichen Regelungen dieses AVV fuer die Auftragsverarbeitung den Regelungen des Hauptvertrags vor.

3. Art, Zweck und Umfang der Verarbeitung

3.1 Die Verarbeitung erfolgt zur Erbringung digitaler Dienstleistungen, insbesondere Website-/WordPress-Pflege, Fehleranalyse, Formularpruefung, Datenaufbereitung, Excel-/CSV-Bearbeitung, IT-Hilfe, PC-/Software-Einrichtung, Remote-Support und damit zusammenhaengenden Supportleistungen.

3.2 Art, Zweck, Dauer, Datenkategorien, betroffene Personen und Systeme werden in Anlage 1 sowie bei Bedarf in Anlage 4 konkretisiert.

3.3 Besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO, insbesondere Gesundheitsdaten, sind nicht Bestandteil des Standardauftrags. Eine Verarbeitung erfolgt nur, wenn sie vorab ausdruuecklich in Textform vereinbart, in Anlage 4 dokumentiert und die hierfuer erforderlichen rechtlichen Voraussetzungen sowie angemessenen Schutzmassnahmen geklaert wurden.

3.4 Eine Verarbeitung zu eigenen Zwecken des Auftragnehmers findet im Rahmen der Auftragsverarbeitung nicht statt.

4. Dauer der Verarbeitung

4.1 Dieser AVV beginnt mit Unterzeichnung oder mit Beginn der ersten beauftragten Verarbeitung personenbezogener Daten, je nachdem, welcher Zeitpunkt frueher liegt.

4.2 Der AVV gilt fuer die Dauer des jeweiligen Hauptvertrags oder Einzelauftrags und endet, wenn alle personenbezogenen Daten nach Weisung des Auftraggebers zurueckgegeben oder geloescht wurden, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

5. Weisungen des Auftraggebers

5.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschliesslich auf dokumentierte Weisung des Auftraggebers. Die anfaenglichen Weisungen ergeben sich aus dem Hauptvertrag, diesem AVV, Anlage 1 und projektbezogenen Weisungen nach Anlage 4.

5.2 Weisungen werden grundsaeztlich in Textform erteilt, insbesondere per E-Mail. Muendliche Weisungen sind unverzueglich in Textform zu bestaetigen.

5.3 Soweit der Auftragnehmer durch Recht der Europaeischen Union oder eines Mitgliedstaats zu einer Verarbeitung verpflichtet ist, informiert er den Auftraggeber vor der Verarbeitung ueber diese rechtliche Anforderung, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen oeffentlichen Interesses verbietet.

5.4 Der Auftragnehmer informiert den Auftraggeber unverzueglich, wenn er der Ansicht ist, dass eine Weisung gegen Datenschutzrecht verstoesst. Die Ausfuehrung der betroffenen Weisung kann bis zur Klaerung ausgesetzt werden.

6. Pflichten des Auftragnehmers

6.1 Der Auftragnehmer waehrt Vertraulichkeit und stellt sicher, dass Personen, die mit der Verarbeitung befasst sind, zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

6.2 Der Auftragnehmer trifft geeignete technische und organisatorische Massnahmen gemaess Anlage 2 und darf diese weiterentwickeln, sofern das Schutzniveau nicht unterschritten wird.

6.3 Der Auftragnehmer unterstuetzt den Auftraggeber angemessen bei der Erfuellung von Betroffenenrechten, bei Datenschutzverletzungen, Datenschutz-Folgenabschaetzungen und Anfragen von Aufsichtsbehoerden, soweit dies die Auftragsverarbeitung betrifft und im Rahmen des Auftrags zumutbar ist.

6.4 Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, insbesondere mit einem Auskunfts-, Berichtigungs-, Loeschungs- oder sonstigen Betroffenenersuchen, leitet der Auftragnehmer dieses Ersuchen unverzueglich an den Auftraggeber weiter, soweit eine Zuordnung zum Auftraggeber moeglich ist. Eine inhaltliche Beantwortung erfolgt nur nach Weisung des Auftraggebers.

6.5 Der Auftragnehmer fuehrt, soweit gesetzlich erforderlich, ein Verzeichnis der Kategorien von Verarbeitungstaetigkeiten nach Art. 30 Abs. 2 DSGVO oder stellt dem Auftraggeber die hierfuer erforderlichen Informationen im angemessenen Umfang zur Verfuegung.

6.6 Der Auftragnehmer unterstuetzt den Auftraggeber im gesetzlich erforderlichen Umfang bei Nachweisen zur Einhaltung dieses AVV.

7. Pflichten und Verantwortlichkeit des Auftraggebers

7.1 Der Auftraggeber ist Verantwortlicher im Sinne der DSGVO. Er ist fuer die Rechtmassigkeit der Datenverarbeitung, die Rechtsgrundlagen, Informationspflichten, Betroffenenrechte, Datenschutz-Folgenabschaetzungen und die Richtigkeit seiner Weisungen verantwortlich.

7.2 Der Auftraggeber stellt sicher, dass dem Auftragnehmer nur solche personenbezogenen Daten bereitgestellt werden, die fuer die beauftragte Leistung erforderlich sind.

7.3 Der Auftraggeber informiert den Auftragnehmer vorab, wenn besondere Risiken bestehen, z. B. besondere Kategorien personenbezogener Daten, Berufsgeheimnisse, Patientendaten, Mitarbeiterdaten, Bewerberdaten oder gesetzliche Sonderanforderungen.

7.4 Der Auftraggeber ist fuer Backups seiner Systeme und Daten verantwortlich, soweit nicht im Hauptvertrag ausdruendlich etwas anderes vereinbart ist. Vor Arbeiten an Live-Systemen, Datenbestaenden oder PCs soll ein aktuelles, funktionsfaehiges Backup vorliegen oder der Auftraggeber bestaetigt, dass er bewusst ohne Backup arbeiten laesst.

8. Zugangsdaten, Remote-Zugriff und Geheimhaltung

8.1 Zugangsdaten sind dem Auftragnehmer nur im erforderlichen Umfang und moeglichst ueber sichere Wege bereitzustellen.

8.2 Der Auftragnehmer behandelt Zugangsdaten vertraulich, gibt sie nicht unbefugt weiter und nutzt sie nur fuer den vereinbarten Auftrag.

8.3 Remote-Zugriffe erfolgen nur nach Zustimmung des Auftraggebers oder berechtigter Ansprechpartner. Der Auftraggeber kann Remote-Zugriffe beobachten und beenden, soweit dies technisch moeglich ist.

8.4 Der Auftraggeber sollte Passwoerter nach Abschluss eines Auftrags aendern, soweit dies sinnvoll und zumutbar ist.

9. Technische und organisatorische Massnahmen

9.1 Die technischen und organisatorischen Massnahmen richten sich nach Art, Umfang, Umstaenden und Zwecken der Verarbeitung sowie nach dem Risiko fuer die Rechte und Freiheiten betroffener Personen.

9.2 Die bei Vertragsschluss vorgesehenen Massnahmen sind in Anlage 2 beschrieben. Der Auftragnehmer darf Massnahmen anpassen und weiterentwickeln, sofern das vereinbarte Schutzniveau nicht unterschritten wird.

9.3 Bei Auftraegen mit besonderen Risiken koennen ergaenzende Massnahmen in Anlage 4 oder im Hauptvertrag vereinbart werden.

10. Unterauftragsverarbeiter

10.1 Der Auftraggeber erteilt eine allgemeine Genehmigung zum Einsatz von Unterauftragsverarbeitern, soweit diese fuer die Leistungserbringung erforderlich sind und ein angemessenes Datenschutzniveau gewaehren.

10.2 Der Auftragnehmer informiert den Auftraggeber ueber neue oder ersetzte Unterauftragsverarbeiter. Der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund innerhalb von 14 Kalendertagen nach Information widersprechen.

10.3 Der Auftragnehmer verpflichtet Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die den Pflichten dieses AVV im Wesentlichen entsprechen.

10.4 Die bei Vertragsschluss bekannten Unterauftragsverarbeiter bzw. Kategorien sind in Anlage 3 aufgefuehrt. Nicht jeder dort genannte Dienstleister wird in jedem Auftrag eingesetzt.

10.5 Vom Auftraggeber bereitgestellte Hosting-, Cloud- oder SaaS-Dienste sind grundsatzlich Systeme bzw. Dienstleister des Auftraggebers, sofern der Auftraggeber selbst Vertragspartner des jeweiligen Anbieters ist. Die datenschutzrechtliche Verantwortung fuer Auswahl, Zulaessigkeit und erforderliche Vereinbarungen mit diesen Anbietern liegt grundsatzlich beim Auftraggeber.

10.6 Die Einbindung sonstiger technischer Dienstleister nach dem jeweiligen Hauptvertrag, Dienstleistungsvertrag, Werkvertrag oder Einzelauftrag bleibt unberuehrt. Soweit ein Dritter personenbezogene Daten im Auftrag des Auftragnehmers verarbeitet, gelten die vorstehenden Regelungen zu Unterauftragsverarbeitern.

11. Datenuebermittlung in Drittlaender

11.1 Eine Uebermittlung personenbezogener Daten in Laender ausserhalb der Europaeischen Union oder des Europaeischen Wirtschaftsraums erfolgt durch den Auftragnehmer nur, wenn die datenschutzrechtlichen Voraussetzungen erfuellt sind, insbesondere durch Angemessenheitsbeschluss, Standardvertragsklauseln oder eine sonstige zulaessige Grundlage.

11.2 Soweit der Auftraggeber selbst Tools, Cloud-Dienste, Hosting-Anbieter oder sonstige Systeme vorgibt, bleibt er fuer deren datenschutzrechtliche Zulaessigkeit verantwortlich.

12. Kontrollrechte und Nachweise

12.1 Der Auftragnehmer stellt dem Auftraggeber auf angemessene Anfrage die erforderlichen Informationen zum Nachweis der Einhaltung dieses AVV zur Verfuegung.

12.2 Vor-Ort-Kontrollen sind nur nach vorheriger Abstimmung, zu ueblichen Geschaeftszeiten, mit angemessener Frist und unter Wahrung von Geheimhaltungsinteressen des Auftragnehmers und anderer Kunden moeglich.

12.3 Der Auftraggeber hat Kontrollen auf das erforderliche Mass zu beschraenken. Entstehender Zusatzaufwand kann nach vorheriger Ankuendigung angemessen verguetet werden, sofern kein vom Auftragnehmer zu vertretender Datenschutzverstoss Anlass der Kontrolle ist.

12.4 Nachweise koennen insbesondere durch Auskuenfte, Dokumentationen, TOM-Beschreibungen, Zertifikate oder sonstige geeignete Unterlagen erbracht werden, soweit diese verfuegbar und angemessen sind.

13. Meldung von Datenschutzverletzungen

13.1 Der Auftragnehmer informiert den Auftraggeber unverzueglich, wenn ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die im Zusammenhang mit der Auftragsverarbeitung steht.

13.2 Die Meldung enthaelt, soweit verfuegbar, Art der Verletzung, betroffene Datenkategorien, betroffene Personengruppen, moegliche Folgen, ergriffene oder vorgeschlagene Massnahmen und Ansprechpartner.

13.3 Der Auftragnehmer unterstuetzt den Auftraggeber im angemessenen Umfang bei der Erfuellung etwaiger Melde- und Benachrichtigungspflichten, soweit die Verletzung die Auftragsverarbeitung betrifft.

14. Rueckgabe und Loeschung von Daten

14.1 Nach Abschluss der beauftragten Verarbeitung gibt der Auftragnehmer personenbezogene Daten nach Wahl des Auftraggebers zurueck oder loescht sie, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

14.2 Datentraeger, Dateien, Exporte, Backups oder lokale Arbeitskopien werden geloescht, sobald sie fuer den Auftrag nicht mehr erforderlich sind und keine gesetzlichen oder berechtigten Gruende fuer eine weitere Speicherung bestehen.

14.3 Der Auftragnehmer darf Nachweise ueber Leistungen, Kommunikation, Abrechnung und Vertragsdurchfuehrung im eigenen Verantwortungsbereich aufbewahren, soweit dies gesetzlich erforderlich oder zur Rechtsverfolgung bzw. Rechtsverteidigung erforderlich ist.

14.4 Loesch- oder Rueckgabeanweisungen koennen in Anlage 4 dokumentiert werden.

15. Verguetung fuer Zusatzaufwand

15.1 Unterstuetzungsleistungen, die ueber die normale Leistungserbringung hinausgehen, koennen nach vorheriger Abstimmung gesondert berechnet werden. Das betrifft insbesondere aufwaendige Auskunfts-, Kontroll-, Export-, Loeschungs- oder Dokumentationsaufgaben, soweit diese nicht durch einen vom Auftragnehmer zu vertretenden Verstoss verursacht wurden.

15.2 Gesetzlich zwingende Pflichten bleiben unberuehrt.

16. Schlussbestimmungen

16.1 Aenderungen und Ergaenzungen dieses AVV beduerfen mindestens der Textform, soweit keine strengere Form gesetzlich vorgeschrieben ist. Der Vertrag kann auch elektronisch abgeschlossen werden, soweit rechtlich zulaessig.

16.2 Sollte eine Bestimmung dieses AVV unwirksam sein oder werden, bleibt die Wirksamkeit der uebrigen Bestimmungen unberuehrt. Anstelle der unwirksamen Bestimmung gelten die gesetzlichen Regelungen.

16.3 Es gilt deutsches Recht, soweit keine zwingenden datenschutzrechtlichen Vorschriften entgegenstehen.

Unterschriften

Auftraggeber / Verantwortlicher	Auftragnehmer / Auftragsverarbeiter
Ort/Datum: _____	Ort/Datum: _____
Name/Firma: _____	Dennis Fabian Fabian Digital Services
Unterschrift: _____	Unterschrift: _____

Anlagen

Anlage 1 - Beschreibung der Verarbeitung

Punkt	Beschreibung
Gegenstand	Digitale Dienstleistungen im Auftrag des Auftraggebers, insbesondere Website-/WordPress-Pflege, Formularpruefung, Datenaufbereitung, Excel-/CSV-Bearbeitung, IT-Hilfe, Remote-Support und PC-/Software-Einrichtung.
Zweck	Wartung, Pflege, Fehleranalyse, Datenbereinigung, technische Umsetzung, Support und Optimierung der vom Auftraggeber beauftragten Systeme oder Dateien.
Art der Verarbeitung	Einsehen, Erfassen, Ordnen, Strukturieren, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Uebermitteln, Bereitstellen, Abgleichen, Loeschen oder Vernichten personenbezogener Daten, soweit fuer den Auftrag erforderlich.
Dauer	Fuer die Dauer des Hauptvertrags bzw. Einzelauftrags; danach Rueckgabe oder Loeschung nach Weisung, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.
Betroffene Personen	Kunden, Interessenten, Mitarbeiter, Ansprechpartner, Websitebesucher, Vereinsmitglieder, Lieferanten, Bewerber, Newsletterempfaenger oder sonstige Kontakte des Auftraggebers.
Datenkategorien	Kontaktdaten, Kommunikationsdaten, Formularinhalte, Website-/Logdaten, Benutzerkonten, Kundenlisten, Tabellen-/Dateiinhalte, Projekt- und Supportdaten.
Besondere Datenkategorien	Nicht Bestandteil des Standardauftrags. Nur nach ausdruecklicher Weisung, Dokumentation in Anlage 4 und gesonderter Pruefung. Gesundheitsdaten sind besonders zu kennzeichnen.
Systeme/Dateien	Vom Auftraggeber benannte Websites, WordPress-Systeme, Hosting-/Adminbereiche, Kontaktformulare, Excel-/CSV-Dateien, Cloud-Ordner, E-Mail-/Supportdaten oder PC-/Softwareumgebungen.

Anlage 2 - Technische und organisatorische Massnahmen (TOM)

Bereich	Massnahmen
Zutritts-/Zugangsschutz	Arbeitsgeraete werden durch Benutzerkonto, Passwort/PIN und nach Moeglichkeit durch Mehrfaktor-Authentifizierung gesichert. Keine unbeaufsichtigte Nutzung durch unbefugte Dritte.
Zugriffskontrolle	Zugriff auf Kundensysteme nur fuer beauftragte Zwecke und im erforderlichen Umfang. Zugangsdaten werden vertraulich behandelt und nicht unbefugt weitergegeben.
Berechtigungskonzept	Nutzung von Least-Privilege-Grundsuetzen, soweit technisch moeglich. Projektbezogene Zugriffe werden nach Abschluss entfernt oder der Auftraggeber wird zur Entfernung aufgefordert.
Passwortschutz	Verwendung individueller Passwoerter; keine Weitergabe an unbefugte Dritte; Empfehlung zur Aenderung von Passwoertern nach Projektende. Passwortmanager oder vergleichbare sichere Ablage, soweit eingesetzt.
Verschluesselung/Uebertragung	Nutzung verschluesselter Verbindungen, soweit verfuegbar (z. B. HTTPS, SFTP, TLS). Sensible Zugangsdaten sollen moeglichst nicht ungeschuetzt per E-Mail uebermittelt werden.
Datensparsamkeit	Verarbeitung nur der Daten, die fuer den beauftragten Zweck erforderlich sind. Keine bewusste Uebernahme unnoetiger Datenbestaende.
Trennung	Kundendaten werden projektbezogen abgelegt und nicht mit anderen Kundendaten vermischt, soweit technisch und organisatorisch moeglich.
Eingabe-/Aenderungskontrolle	Wesentliche Weisungen, Freigaben und sicherheitsrelevante Vorgaenge koennen in Textform dokumentiert werden. Aenderungen erfolgen nur im Rahmen des Auftrags.

Bereich	Massnahmen
Backups	Der Auftraggeber bleibt fuer Backups seiner Systeme verantwortlich, soweit nicht ausdruuecklich etwas anderes vereinbart ist. Vor Arbeiten an Live-Systemen soll ein aktuelles Backup vorliegen.
Verfuegbarkeit	Angemessene Sicherung eigener Arbeitsmittel; keine Garantie fuer Verfuegbarkeit von Kundensystemen, Drittanbieter-Diensten, Hosting oder Internetverbindungen.
Loeschung	Arbeitskopien, Exporte und Zugangsdaten werden geloeschet bzw. entfernt, sobald sie fuer den Auftrag nicht mehr erforderlich sind, soweit keine Aufbewahrungspflichten entgegenstehen.
Remote-Support	Remote-Zugriffe erfolgen nur nach Zustimmung des Auftraggebers bzw. berechtigter Ansprechpartner. Der Auftraggeber kann den Zugriff beobachten und beenden.
Incident Management	Bekannte Sicherheitsvorfaelle mit Bezug zur Auftragsverarbeitung werden bewertet, dokumentiert und dem Auftraggeber unverzueglich gemeldet.
Vertraulichkeit	Verpflichtung zur Vertraulichkeit; keine Offenlegung von Kundendaten gegenueber unbefugten Dritten.

Anlage 3 - Unterauftragsverarbeiter / Kategorien

Die folgende Liste ist vor Einsatz zu pruefen und bei Bedarf zu aktualisieren. Nicht jeder Dienstleister wird in jedem Auftrag eingesetzt. Vom Auftraggeber selbst beauftragte Systeme sind in der Regel keine Unterauftragsverarbeiter des Auftragnehmers.

Dienstleister/Kategorie	Zweck	Sitz/Region	Hinweis
E-Mail-/Webhosting des Auftragnehmers, z. B. limacity / zuständiger Hostinganbieter laut Kundenkonto	Kommunikation, Empfang von Anfragen, technische Bereitstellung eigener Website/E-Mail	Deutschland/EU, soweit vertraglich so bereitgestellt	Relevant, wenn Kundendaten ueber die E-Mail-/Websysteme des Auftragnehmers verarbeitet werden. Vor Einsatz Anbieterangaben pruefen.
Vom Auftraggeber bereitgestellte Hosting-, Cloud- oder SaaS-Dienste	Bearbeitung im System des Auftraggebers	Je nach Anbieter	Grundsaeztlich Dienstleister/Systeme des Auftraggebers, sofern der Auftraggeber selbst Vertragspartner ist. Verantwortung fuer Auswahl und AVV mit diesem Anbieter liegt grundsaeztlich beim Auftraggeber.
Weitere Dienstleister	Nur nach vorheriger Information bzw. Vereinbarung	Je nach Anbieter	Vor Einsatz konkret eintragen oder schriftlich bestaetigen.

Anlage 4 - Weisungsformular / projektbezogene Ergaenzung

Feld	Eintrag
Projekt/Auftrag	_____
Systeme/Dateien	_____
Erlaubte Verarbeitung	_____
Besondere Risiken/Sensibilitaet	_____
Besondere Kategorien personenbezogener Daten	Nein / Ja, naemlich: _____
Ansprechpartner Auftraggeber	_____
Loesch-/Rueckgabeanweisung nach Projektende	_____
Besondere Weisungen	_____