

Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

zwischen

[Kunde / Unternehmen des Nutzers]

– nachfolgend Verantwortlicher –

und

FFH Enterprises GmbH

Lindenallee 5

57577 Hamm (Sieg)

Deutschland

vertreten durch die Geschäftsführung

– nachfolgend Auftragsverarbeiter –

gemeinsam Parteien".

§ 1 Gegenstand des Vertrages

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen die Software Pitflow als cloudbasierte SaaS-Lösung zur Verfügung.

(2) Im Rahmen der Nutzung verarbeitet der Auftragsverarbeiter personenbezogene Daten ausschließlich im Auftrag und nach Weisung des Verantwortlichen.

(3) Dieser Vertrag konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien gemäß Art. 28 DSGVO.

§ 2 Art und Zweck der Verarbeitung

Die Verarbeitung erfolgt zum Zweck der Bereitstellung der Software Pitflow und umfasst insbesondere:

- Kundenverwaltung
- Fahrzeugverwaltung
- Auftragsverwaltung
- Terminverwaltung
- Rechnungserstellung
- Dokumentenverwaltung
- E-Mail-Kommunikation
- WhatsApp-Kommunikation
- KI-gestützte Assistenzfunktionen
- Datenspeicherung und Datensicherung

§ 3 Art der personenbezogenen Daten

Je nach Nutzung können insbesondere folgende Daten verarbeitet werden:

Unternehmensdaten

- Firmenname
- Anschrift
- Telefonnummer
- E-Mail-Adresse
- Bankverbindung
- Umsatzsteuerdaten

Kundendaten

- Vorname
- Nachname
- Anschrift
- Telefonnummer
- E-Mail-Adresse

Fahrzeugdaten

- Kennzeichen
- Fahrzeugmarke
- Fahrzeugmodell
- Fahrzeuginformationen

Auftragsdaten

- Leistungen
- Preise
- Termine
- Statusinformationen
- Notizen

Rechnungsdaten

- Rechnungsnummern
- Rechnungsinhalte
- Steuerdaten
- Zahlungsinformationen

Kommunikationsdaten

- WhatsApp-Nachrichten
- E-Mails
- Anhänge
- Kommunikationsverläufe

§ 4 Kategorien betroffener Personen

Von der Verarbeitung können insbesondere betroffen sein:

- Kunden des Verantwortlichen
- Interessenten des Verantwortlichen
- Mitarbeiter des Verantwortlichen
- Geschäftspartner des Verantwortlichen
- Nutzer der Software

§ 5 Weisungsrecht des Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen.

(2) Weisungen können insbesondere in Textform (z. B. E-Mail) erfolgen.

(3) Erkennt der Auftragsverarbeiter, dass eine Weisung gegen Datenschutzrecht verstößt, wird er den Verantwortlichen hierauf unverzüglich hinweisen.

§ 6 Vertraulichkeit

(1) Der Auftragsverarbeiter verpflichtet sämtliche mit der Verarbeitung beschäftigten Personen zur Vertraulichkeit.

(2) Die Verpflichtung besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 7 Technische und organisatorische Maßnahmen (TOM)

Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO.

Hierzu gehören insbesondere:

Zugangskontrolle

- Passwortschutz
- Mehrstufige Authentifizierung (soweit verfügbar)
- Rollenbasierte Benutzerverwaltung

Zugriffskontrolle

- Berechtigungssysteme
- Trennung von Kundendaten

Übertragungskontrolle

- TLS-/SSL-Verschlüsselung
- Verschlüsselte Datenübertragung

Speicherkontrolle

- Verschlüsselte Datenspeicherung
- Regelmäßige Sicherheitsupdates

Verfügbarkeitskontrolle

- Datensicherungen

- Backup-Systeme
- Monitoring

Wiederherstellbarkeit

- Regelmäßige Sicherungen
- Wiederanlaufverfahren

§ 8 Unterstützungspflichten

Der Auftragsverarbeiter unterstützt den Verantwortlichen angemessen bei:

- Auskunftersuchen
- Berichtigungen
- Löschungen
- Einschränkungen der Verarbeitung
- Datenübertragbarkeit
- Datenschutz-Folgenabschätzungen
- Meldungen von Datenschutzverletzungen

soweit dies technisch möglich und wirtschaftlich zumutbar ist.

§ 9 Meldung von Datenschutzverletzungen

(1) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über bekannt gewordene Verletzungen des Schutzes personenbezogener Daten.

(2) Die Mitteilung erfolgt ohne schuldhaftes Zögern.

(3) Die Meldung enthält alle verfügbaren Informationen, die zur Erfüllung der gesetzlichen Meldepflichten erforderlich sind.

§ 10 Unterauftragsverarbeiter

(1) Der Verantwortliche stimmt dem Einsatz folgender Unterauftragsverarbeiter zu:

Dienstleister	Zweck	Standort
Supabase	Datenbank und Authentifizierung	EU
Vercel	Hosting (Serverless Functions)	EU (Frankfurt)
360dialog	WhatsApp Business API	EU
Resend	E-Mail-Versand	EU
OpenAI	KI-Funktionen	USA
Anthropic	KI-Funktionen	USA

(2) Der Auftragsverarbeiter darf weitere Unterauftragsverarbeiter einsetzen, sofern:

- der Verantwortliche vorab informiert wird,
- ein gleichwertiges Datenschutzniveau sichergestellt wird.

(3) Der Verantwortliche kann innerhalb von 14 Tagen nach Mitteilung aus wichtigem datenschutzrechtlichem Grund widersprechen.

§ 11 Drittstaatenübermittlung

(1) Der Auftragsverarbeiter hostet seine Anwendung auf Servern in der Europäischen Union (Frankfurt, Deutschland). Eine Verarbeitung personenbezogener Daten außerhalb der EU kann bei folgenden Unterauftragsverarbeitern erfolgen:

(2) Dies betrifft insbesondere:

- OpenAI
- Anthropic

(3) Die Übermittlung erfolgt ausschließlich auf Grundlage geeigneter Garantien gemäß Art. 44 ff. DSGVO.

Hierzu zählen insbesondere:

- EU-Standardvertragsklauseln (SCC)
- Zusätzliche technische Schutzmaßnahmen

§ 12 Kontrollrechte

(1) Der Verantwortliche ist berechtigt, die Einhaltung dieses Vertrages nach angemessener Vorankündigung zu überprüfen.

(2) Der Nachweis kann insbesondere erfolgen durch:

- Selbstauskünfte
- Zertifikate
- Sicherheitsberichte
- Auditreports

(3) Vor-Ort-Kontrollen dürfen nur erfolgen, soweit berechtigte Interessen anderer Kunden nicht beeinträchtigt werden.

§ 13 Löschung und Rückgabe von Daten

(1) Nach Beendigung des Vertragsverhältnisses werden personenbezogene Daten auf Weisung des Verantwortlichen gelöscht oder zurückgegeben.

(2) Gesetzliche Aufbewahrungspflichten bleiben unberührt.

(3) Rechnungs- und steuerrechtlich relevante Daten können aufgrund gesetzlicher Verpflichtungen bis zu 10 Jahre gespeichert werden.

(4) Nach Ablauf gesetzlicher Fristen werden die Daten gelöscht.

§ 14 Haftung

(1) Die Haftung richtet sich nach den gesetzlichen Bestimmungen der DSGVO.

(2) Im Übrigen gelten die Haftungsregelungen der zwischen den Parteien vereinbarten AGB.

§ 15 Laufzeit

(1) Dieser Vertrag wird mit Abschluss des Hauptvertrages wirksam.

(2) Er endet automatisch mit Beendigung des SaaS-Vertrages, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

§ 16 Schlussbestimmungen

(1) Änderungen dieses Vertrages bedürfen der Textform.

(2) Sollten einzelne Bestimmungen unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(3) Es gilt das Recht der Bundesrepublik Deutschland.

Anlage 1 – Technische und organisatorische Maßnahmen (TOM)

Der Auftragsverarbeiter setzt insbesondere folgende Sicherheitsmaßnahmen ein:

- Verschlüsselte Datenübertragung (TLS/SSL)
- Passwortgeschützte Benutzerkonten
- Rollen- und Berechtigungssysteme
- Regelmäßige Sicherheitsupdates
- Backup- und Wiederherstellungssysteme
- Protokollierung sicherheitsrelevanter Ereignisse
- Zugriffsbeschränkung auf berechtigte Mitarbeiter
- Datentrennung zwischen Mandanten
- Monitoring und Angriffserkennung
- Regelmäßige Überprüfung der Sicherheitsmaßnahmen

Ort, Datum: _____

Verantwortlicher

Name/Firma: _____

Unterschrift: _____

Auftragsverarbeiter

FFH Enterprises GmbH

Unterschrift: _____