Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

zwischen dem Lizenznehmer der Software "fetchtax" (nachfolgend "Verantwortlicher") und der HeyPragmatic GmbH, Kolonnenstr. 8, 10827 Berlin (nachfolgend "Auftragnehmer"), gemeinsam nachfolgend als "Parteien" bezeichnet

Präambel

Der Auftragnehmer erbringt für den Verantwortlichen Leistungen im Zusammenhang mit der Software "fetchtax" auf Grundlage der zwischen den Parteien geschlossenen Allgemeinen Geschäftsbedingungen (nachfolgend "Hauptvertrag"). Im Rahmen dieser Leistungserbringung verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag des Verantwortlichen im Sinne von Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, nachfolgend "DSGVO"). Dieser Vertrag zur Auftragsverarbeitung (nachfolgend "AVV") regelt die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dieser Verarbeitung.

Der AVV wird mit Abschluss des Hauptvertrages zwischen den Parteien automatisch Vertragsbestandteil, ohne dass es einer gesonderten Annahme durch den Verantwortlichen bedarf.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

(1) Gegenstand, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten sowie die Kategorien betroffener Personen ergeben sich aus Anlage 1 dieses AVV.

(2) Die Dauer der Auftragsverarbeitung (Laufzeit) entspricht der Laufzeit des Hauptvertrages, sofern sich aus den Regelungen dieses AVV keine darüber hinausgehenden Verpflichtungen ergeben.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen. Dies umfasst Tätigkeiten, die im Hauptvertrag und in Anlage 1 konkretisiert sind.

(2) Der Verantwortliche ist im Rahmen dieses AVV allein verantwortlich für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenübermittlung an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung ("Verantwortlicher" im Sinne des Art. 4 Nr. 7 DSGVO).

(3) Die Weisungen des Verantwortlichen werden anfänglich durch den Hauptvertrag und diesen AVV festgelegt und können vom Verantwortlichen danach in schriftlicher Form oder in Textform an die vom Auftragnehmer benannte Kontaktstelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierten Weisungen des Verantwortlichen, es sei denn, er ist durch das Recht der Europäischen Union oder eines ihrer Mitgliedstaaten, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragnehmer dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Der Auftragnehmer wird den Verantwortlichen unverzüglich informieren, wenn er der Auffassung ist, dass eine Weisung des Verantwortlichen gegen datenschutzrechtliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

(3) Der Auftragnehmer sichert zu, dass die mit der Datenverarbeitung betrauten Personen zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung besteht auch nach Beendigung der Tätigkeit fort.

(4) Der Auftragnehmer setzt die Maßnahmen gemäß § 6 dieses AVV um.

(5) Der Auftragnehmer unterstützt den Verantwortlichen im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gemäß Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten.

(6) Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt bzw. geprüft, dass eine Bestellpflicht nicht besteht. Die Kontaktdaten werden dem Verantwortlichen auf Anfrage mitgeteilt.

(7) Die Verarbeitung personenbezogener Daten findet grundsätzlich innerhalb des Gebiets der Europäischen Union oder des Europäischen Wirtschaftsraums statt. Jegliche Verlagerung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

§ 4 Pflichten des Verantwortlichen

(1) Der Verantwortliche hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten in Bezug auf datenschutzrechtliche Bestimmungen feststellt.

(2) Der Verantwortliche ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Pflicht gilt auch nach Beendigung dieses Vertrages fort.

(3) Der Verantwortliche benennt dem Auftragnehmer auf Anforderung einen Ansprechpartner für datenschutzrechtliche Angelegenheiten.

§ 5 Anfragen und Rechte betroffener Personen

(1) Der Auftragnehmer wird dem Verantwortlichen, soweit dies möglich ist, mit geeigneten technischen und organisatorischen Maßnahmen dabei helfen, seinen Pflichten nach Art. 12 bis 22 sowie Art. 32 und 36 DSGVO nachzukommen.

(2) Wendet sich eine betroffene Person mit Ansprüchen auf Berichtigung, Löschung, Auskunft, Einschränkung der Verarbeitung oder Datenübertragbarkeit unmittelbar an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Verantwortlichen verweisen, soweit eine Zuordnung zum Verantwortlichen möglich ist.

(3) Der Auftragnehmer darf Auskünfte über im Auftrag verarbeitete personenbezogene Daten nur nach vorheriger Weisung oder Zustimmung des Verantwortlichen erteilen.

§ 6 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft die technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau sicherzustellen. Die zum Zeitpunkt des Vertragsschlusses umgesetzten Maßnahmen sind in Anlage 2 beschrieben.

(2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Das Sicherheitsniveau der festgelegten Maßnahmen darf dabei nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

§ 7 Unterauftragsverhältnisse

(1) Der Verantwortliche erteilt dem Auftragnehmer die allgemeine Genehmigung zur Hinzuziehung weiterer Auftragsverarbeiter (nachfolgend "Unterauftragnehmer") im Sinne von Art. 28 Abs. 2 Satz 1 DSGVO. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragnehmer sind in Anlage 3 aufgeführt.

(2) Der Auftragnehmer wird den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern in angemessener Form, spätestens 30 Tage vor Beauftragung bzw. Änderung, informieren. Der Verantwortliche hat das Recht, gegen derartige Änderungen innerhalb von 14 Tagen nach Zugang der Information in Textform Einspruch zu erheben. Der Einspruch darf nur aus einem wichtigen datenschutzrechtlichen Grund erfolgen, der dem Auftragnehmer gegenüber zu begründen ist.

(3) Erhebt der Verantwortliche fristgerecht einen begründeten Einspruch, sind die Parteien verpflichtet, eine einvernehmliche Lösung zu suchen. Gelingt dies nicht, ist jede Partei berechtigt, den Hauptvertrag und diesen AVV mit der im Hauptvertrag vorgesehenen Frist zu kündigen.

(4) Der Auftragnehmer verpflichtet den Unterauftragnehmer zu denselben datenschutzrechtlichen Pflichten, die in diesem AVV festgelegt sind. Bei

Unterauftragsverhältnissen in einem Drittland wird der Auftragnehmer die Voraussetzungen gemäß Art. 44 ff. DSGVO sicherstellen, insbesondere durch Abschluss der Standardvertragsklauseln der EU-Kommission.

(5) Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung gelten Nebenleistungen, die der Auftragnehmer bei Dritten in Anspruch nimmt (z. B. Telekommunikationsleistungen, Post- und Transportdienste, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder Entsorgung von Datenträgern). Der Auftragnehmer stellt jedoch sicher, dass auch bei diesen Nebenleistungen angemessene Schutzvorkehrungen zur Gewährleistung der Vertraulichkeit getroffen werden.

(6) Die Zahlungsabwicklung durch Stripe (Stripe Payments Europe, Ltd.) stellt keine Auftragsverarbeitung im Sinne dieses AVV dar. Stripe verarbeitet Zahlungsdaten als eigenständig Verantwortlicher. Der Auftragnehmer ist für diese Verarbeitung nicht im Auftrag des Verantwortlichen tätig.

§ 8 Nachweis- und Kontrollrechte

(1) Der Auftragnehmer weist dem Verantwortlichen die Einhaltung der in diesem AVV niedergelegten Pflichten mit geeigneten Mitteln nach. Dies kann insbesondere durch die Vorlage aktueller Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung) oder durch eine geeignete Zertifizierung gemäß Art. 42 DSGVO erfolgen.

(2) Sofern im Einzelfall Prüfungen durch den Verantwortlichen oder einen von diesem beauftragten Prüfer erforderlich sind, werden diese während der üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach rechtzeitiger Vorankündigung mit einer angemessenen Frist von mindestens 30 Tagen durchgeführt. Der Auftragnehmer kann diese von der vorherigen Anmeldung mit angemessener Frist und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen.

(3) Der Auftragnehmer kann für die Unterstützung bei Prüfungen, die über einmal pro Kalenderjahr hinausgehen oder die erheblichen Aufwand erfordern, eine angemessene Vergütung verlangen. Dies gilt nicht bei konkretem Anlass, insbesondere bei Vorliegen einer Datenschutzverletzung.

(4) Sollte eine Datenschutzaufsichtsbehörde oder eine andere staatliche Aufsichtsbehörde des Verantwortlichen eine Prüfung vornehmen, gelten grundsätzlich dieselben Regeln wie in Absatz 2. Eine Verschwiegenheitserklärung muss nicht unterschrieben werden, sofern die Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt.

§ 9 Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Verantwortlichen bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherigen Konsultationen.

(2) Der Auftragnehmer informiert den Verantwortlichen unverzüglich, möglichst innerhalb von 48 Stunden, nachdem er Kenntnis von einer Verletzung des Schutzes personenbezogener Daten erlangt hat. Die Meldung enthält mindestens die Angaben gemäß Art. 33 Abs. 3 DSGVO, soweit dem Auftragnehmer bekannt.

(3) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen und stimmt sich hierzu mit dem Verantwortlichen ab.

§ 10 Weisungsbefugnis des Verantwortlichen

(1) Mündliche Weisungen bestätigt der Verantwortliche unverzüglich schriftlich oder in Textform.

(2) Der Auftragnehmer hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

§ 11 Löschung und Rückgabe personenbezogener Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Verantwortlichen – spätestens mit Beendigung des Hauptvertrages – wird der Auftragnehmer sämtliche in seinen Besitz gelangten personenbezogenen Daten gemäß den Regelungen des Hauptvertrages löschen. Die Löschung erfolgt gemäß § 15 Abs. 3 des Hauptvertrages innerhalb von 100 Tagen nach Vertragsende aus den produktiven Systemen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben.

§ 12 Haftung

(1) Für die Haftung der Parteien gelten die Regelungen des Art. 82 DSGVO.

(2) Im Übrigen gelten die Haftungsregelungen des Hauptvertrages entsprechend, soweit nicht zwingende gesetzliche Vorschriften entgegenstehen.

§ 13 Sonstiges

(1) Im Falle von Widersprüchen zwischen Regelungen dieses AVV und Regelungen des Hauptvertrages gehen die Regelungen dieses AVV vor, soweit es um die Verarbeitung personenbezogener Daten geht.

(2) Sollten einzelne Teile dieses AVV unwirksam sein, so berührt dies die Wirksamkeit des AVV im Übrigen nicht.

(3) Änderungen und Ergänzungen dieses AVV und aller seiner Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen der Textform und eines ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(4) Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts und der Verweisungsnormen des internationalen Privatrechts.

(5) Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem AVV ist Berlin, sofern der Verantwortliche Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.

(6) Dieser AVV wird in deutscher und englischer Sprache bereitgestellt. Bei Widersprüchen oder Abweichungen zwischen der deutschen und der englischen Fassung hat die deutsche Fassung Vorrang.

Anlage 1 – Beschreibung der Verarbeitung

1. Gegenstand und Zweck der Verarbeitung

Bereitstellung der Software "fetchtax" als Software-as-a-Service zur effizienten Verwaltung kaufmännischer Geschäftsvorfälle, insbesondere durch den Import von Daten aus Drittsystemen, die Bearbeitung und Aufbereitung dieser Daten sowie die Bereitstellung der Daten für Drittsysteme.

2. Art der Verarbeitung

Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen oder Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Abgleich oder Verknüpfung, Einschränken, Löschen oder Vernichten personenbezogener Daten im Rahmen der Bereitstellung und des Betriebs der Software.

3. Dauer der Verarbeitung

Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages. Nach dessen Beendigung erfolgt eine Löschung der Daten gemäß § 11 dieses AVV.

4. Art der personenbezogenen Daten

Die Verarbeitung umfasst insbesondere folgende Datenarten:

- Stammdaten (z. B. Name, Anschrift, Firmierung)
- Kontaktdaten (z. B. E-Mail-Adresse, Telefonnummer)
- Zugangsdaten (z. B. Benutzername, verschlüsselte Passwörter)
- Nutzungsdaten (z. B. Log-Daten, IP-Adressen, Zeitstempel)
- Daten zu Geschäftsvorfällen (z. B. Rechnungs- und Belegdaten, Zahlungsinformationen, Umsatzsteuerdaten)
- Sonstige im Rahmen der Geschäftsvorfälle verarbeitete Daten, soweit diese personenbezogen sind

Eine Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 DSGVO ist nicht Gegenstand des Auftrags und soll durch den Verantwortlichen nach Möglichkeit unterbleiben.

5. Kategorien betroffener Personen

- Mitarbeitende, Beauftragte und sonstige Nutzer des Verantwortlichen, die Zugriff auf den Arbeitsbereich haben
- Kunden, Lieferanten und sonstige Geschäftspartner des Verantwortlichen (bzw. der von diesem betreuten Unternehmen, z. B. Mandanten eines Steuerberaters)

- Sonstige Personen, deren Daten im Rahmen der Geschäftsvorfälle des Verantwortlichen verarbeitet werden (z. B. Rechnungsempfänger, Ansprechpartner)

Anlage 2 – Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Der Auftragnehmer trifft die nachfolgenden technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten. Die Angemessenheit der Maßnahmen wird regelmäßig überprüft und bei Bedarf an den Stand der Technik angepasst.

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

Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z. B. durch Schließsysteme, Alarmanlagen, Videoüberwachung, Zutrittsberechtigungskonzepte und Besucheranmeldung bei Hostinganbietern mit entsprechender Zertifizierung (z. B. ISO 27001).

Zugangskontrolle: Schutz vor unbefugter Systembenutzung durch sichere Passwörter, Mehr-Faktor-Authentifizierung für administrative Zugänge, automatische Sperrmechanismen, Verschlüsselung der Datenträger, Firewall-Systeme.

Zugriffskontrolle: Rollen- und Berechtigungskonzepte, Beschränkung des Zugriffs auf Daten auf das für die jeweilige Aufgabe erforderliche Maß (Need-to-know-Prinzip), Protokollierung von Zugriffen, sichere Löschung nicht mehr benötigter Daten.

Trennungskontrolle: Logische und physische Trennung von Daten verschiedener Mandanten (Multi-Tenant-Architektur), Trennung von Produktions-, Test- und Entwicklungsumgebungen.

Pseudonymisierung: Einsatz von Pseudonymisierung und Verschlüsselung, soweit dies mit Blick auf den Verarbeitungszweck möglich ist.

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

Weitergabekontrolle: Transportverschlüsselung (TLS) bei der Übertragung personenbezogener Daten, Dokumentation der Empfänger, gesicherte Schnittstellen.

Eingabekontrolle: Protokollierung von Eingaben, Änderungen und Löschungen personenbezogener Daten, Nachvollziehbarkeit durch Audit-Logs.

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

Verfügbarkeitskontrolle: Regelmäßige Datensicherungen (Backups), redundante Systeme, unterbrechungsfreie Stromversorgung (USV) beim Hostinganbieter, Schutz vor Schadsoftware, Notfallpläne.

Rasche Wiederherstellbarkeit: Definierte Wiederherstellungsprozesse (Disaster Recovery) und regelmäßige Tests der Wiederherstellbarkeit.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Datenschutz-Management und IT-Sicherheits-Management

Incident-Response-Management und Dokumentation von Sicherheitsvorfällen

Datenschutzfreundliche Voreinstellungen (Privacy by Design / Default)

Regelmäßige Schulungen und Verpflichtung der Mitarbeitenden auf die Vertraulichkeit und die Einhaltung datenschutzrechtlicher Vorschriften

Regelmäßige Überprüfung und Aktualisierung dieser Maßnahmen

5. Auftragskontrolle

Klare und unmissverständliche Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl und regelmäßige Kontrolle von Unterauftragnehmern, schriftliche Weisungen, Verpflichtung der Mitarbeitenden auf die Vertraulichkeit.

Anlage 3 – Zugelassene Unterauftragnehmer

Zum Zeitpunkt des Vertragsschlusses setzt der Auftragnehmer folgende Unterauftragnehmer im Rahmen der Leistungserbringung ein:

Unterauftragsverarbeiter	Dienstleistung	Daten	Ort der Verarbeitung
Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxembourg	Cloud Hosting	Temporäre Verarbeitung von Kundendaten, keine dauerhafte Speicherung	EU
Lovable Labs AB, Box 190, 101 23 Stockholm, Sweden	Cloud Hosting	Rechenleistung und Cloud Speicherplatz für Kundendaten	EU
Supabase, Inc., 65 Chulia Street #38-02/03, OCBC Centre, Singapore 049513	Cloud Hosting	Rechenleistung und Cloud Speicherplatz für Kundendaten	EU
n8n GmbH, Novalisstr. 10, 10115 Berlin, Germany	Cloud Hosting	Verarbeitung von Geschäftsvorfällen des Kunden	EU
Mailgun Technologies, Inc., 112 E Pecan St #1135, San Antonio, TX 78205, USA	E-Mail-Versand	E-Mail-Adressen und Inhalte von System- und Benachrichtigungs-E-Mails	EU

Bei Änderungen informiert der Auftragnehmer den Verantwortlichen gemäß § 7 dieses AVV.