Auftragsverarbeitungsvertrag (AVV) – Vorlage

Vereinbarung gemäß Art. 28 DSGVO zwischen Auftraggeber und Fly & Froth Grafik- & Webdesign · Stand: Juli 2026

Parteien

Verantwortlicher (Auftraggeber):

Firma/Name: _____

Anschrift: _____

Vertreten durch: _____

Auftragsverarbeiter (Auftragnehmer):

Fly & Froth Grafik- & Webdesign · Inhaber: Mehmet Genco · Röderweg 19, 61184 Karben · info@fly-froth.com

§ 1 Gegenstand und Dauer der Verarbeitung

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers im Rahmen des Hauptvertrags über die Einrichtung und Betreuung von KI-Agenten bzw. weiterer digitaler Services (nachfolgend „Hauptvertrag“). Die Dauer dieses AVV entspricht der Laufzeit des Hauptvertrags.

§ 2 Art und Zweck der Verarbeitung

Betrieb von KI-Agenten (Website-Chat, WhatsApp, E-Mail, Telefon) und zugehörigen Workflows: Entgegennahme und Beantwortung von Anfragen, Lead-Erfassung, Terminvereinbarung, Erstellung von Gesprächszusammenfassungen sowie Übergabe der Daten an den Auftraggeber. Hosting, Wartung und Monitoring der eingesetzten Systeme.

§ 3 Kategorien betroffener Personen

- Kunden und Interessenten des Auftraggebers
- Mitarbeiter des Auftraggebers (soweit sie mit den Systemen arbeiten)
- Sonstige Kontaktpersonen, die die Kommunikationskanäle des Auftraggebers nutzen

§ 4 Kategorien personenbezogener Daten

- Kontaktdaten (Name, Telefonnummer, E-Mail-Adresse)
- Kommunikationsinhalte (Chat-Verläufe, Nachrichten, E-Mails, Gesprächstranskripte/-zusammenfassungen)
- Termin- und Anfragedaten (Wunschtermine, Anliegen, Angebotsdaten)
- Technische Daten (Zeitstempel, Kanal, ggf. Telefonnummer des Anrufers)

Besondere Kategorien (Art. 9 DSGVO) sind nicht Gegenstand der beauftragten Verarbeitung; sollten Betroffene solche Daten unaufgefordert übermitteln, werden sie nicht gezielt ausgewertet.

§ 5 Pflichten des Auftragnehmers

- Verarbeitung ausschließlich auf dokumentierte Weisung des Auftraggebers (Art. 28 Abs. 3 lit. a DSGVO); der Hauptvertrag gilt als Weisung
- Vertraulichkeitsverpflichtung aller mit der Verarbeitung befassten Personen (lit. b)
- Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO (lit. c, siehe Anlage 1)
- Unterstützung des Auftraggebers bei Betroffenenrechten (Auskunft, Löschung, Berichtigung u. a.) und bei den Pflichten aus Art. 32–36 DSGVO (lit. e, f)

- Unverzügliche Meldung von Verletzungen des Schutzes personenbezogener Daten an den Auftraggeber, spätestens innerhalb von 48 Stunden nach Kenntnis
- Nach Vertragsende: Löschung oder Rückgabe aller personenbezogenen Daten nach Wahl des Auftraggebers, sofern keine gesetzliche Aufbewahrungspflicht besteht (lit. g)
- Bereitstellung aller erforderlichen Informationen zum Nachweis der Pflichten sowie Ermöglichung von Überprüfungen (lit. h)

§ 6 Unterauftragsverarbeiter

Der Auftraggeber erteilt die allgemeine Genehmigung zum Einsatz der in Anlage 2 aufgeführten Unterauftragsverarbeiter. Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen (Hinzuziehung oder Ersetzung) in Textform; der Auftraggeber kann innerhalb von 14 Tagen aus wichtigem Grund widersprechen. Mit jedem Unterauftragsverarbeiter werden Verpflichtungen entsprechend diesem AVV vereinbart; bei Verarbeitung außerhalb der EU/des EWR werden geeignete Garantien (Art. 44 ff. DSGVO, insb. EU-Standardvertragsklauseln oder Angemessenheitsbeschluss) sichergestellt.

§ 7 Kontrollrechte

Der Auftraggeber ist berechtigt, sich vor Beginn und während der Verarbeitung von der Einhaltung der technischen und organisatorischen Maßnahmen zu überzeugen – in der Regel durch Einholung von Auskünften und aktuellen Nachweisen/Zertifikaten der eingesetzten Rechenzentren. Vor-Ort-Kontrollen erfolgen nach angemessener Vorankündigung zu üblichen Geschäftszeiten.

§ 8 Haftung & Schlussbestimmungen

Für die Haftung gilt Art. 82 DSGVO sowie die Haftungsregelung des Hauptvertrags. Änderungen und Ergänzungen dieses AVV bedürfen der Textform. Es gilt deutsches Recht. Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Ort, Datum: _____

Unterschrift Auftraggeber: _____

Unterschrift Auftragnehmer (Fly & Froth, Mehmet Genco):

_____

Anlage 1 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

- Zutritts-/Zugangskontrolle: Hosting ausschließlich in zertifizierten Rechenzentren (ISO 27001) in der EU; Zugang zu Systemen nur über persönliche Konten mit starken Passwörtern und Zwei-Faktor-Authentifizierung
- Zugriffskontrolle: Zugriff auf Kundendaten nur durch den Auftragnehmer; rollenbasierte Beschränkung; keine Weitergabe von Zugangsdaten
- Weitergabekontrolle: Verschlüsselte Übertragung (TLS 1.2+); verschlüsselte Speicherung (at rest); keine Übermittlung an Dritte außerhalb der Anlage 2
- Eingabekontrolle: Protokollierung wesentlicher Änderungen an Konfiguration und Wissensbasis
- Verfügbarkeitskontrolle: Tägliche Backups, Monitoring, dokumentiertes Wiederanlaufverfahren
- Trennungskontrolle: Logische Trennung der Daten je Kunde (separate Konfigurationen/Instanzen)

- KI-spezifisch: Konversationsdaten werden nicht zum Training von KI-Modellen verwendet; LLM-Aufrufe erfolgen mit deaktivierter Trainingsnutzung (Zero-Data-Retention bzw. opt-out gemäß Anbietervereinbarung)

Anlage 2 – Genehmigte Unterauftragsverarbeiter

- Hetzner Online GmbH (Deutschland) – Server-Hosting, n8n-Workflows
- Vercel Inc. (EU-Region; USA/SCC) – Hosting Web-Anwendungen
- Anthropic / OpenAI (USA; EU-Endpunkte soweit verfügbar, SCC/EU-US Data Privacy Framework, keine Trainingsnutzung) – Sprachmodell-API für Agenten-Antworten
- Meta Platforms Ireland Ltd. / Business Solution Provider (z. B. 360dialog GmbH, Deutschland) – WhatsApp-Business-API (nur bei WhatsApp-Agent)
- Twilio Inc. / Telefonie-Anbieter (USA/SCC bzw. EU) – Telefonie-Infrastruktur, Rufnummern (nur bei KI-Telefon)
- ElevenLabs / Sprachsynthese-Anbieter (USA/SCC) – Sprachausgabe (nur bei KI-Telefon)
- Sendinblue GmbH (Brevo) (Deutschland/Frankreich) – E-Mail-Versand (nur bei E-Mail-Agent/Newsletter)
- Google Ireland Ltd. – Google-Business-Profil-Anbindung (nur bei Bewertungs-Agent)

Die konkret eingesetzten Unterauftragsverarbeiter richten sich nach dem gebuchten Paket und werden im Auftragsformular bestätigt. Nicht benötigte Dienste kommen nicht zum Einsatz.