Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DSGVO

Version 2.0

Präambel

Verantwortlicher (Auftraggeber): [Firma des Verantwortlichen] · [Anschrift]
Auftragsverarbeiter (Auftragnehmer): Dreambirds Productions GbR, vertreten durch Nico Briegel & Nadine Briegel, Hintere Straße 13, 76756 Bellheim — Betreiberin der Plattform flowerdesk (https://flowerdesk.de), info@flowerdesk.de
Die Parteien schließen den folgenden Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO. Sie werden im Folgenden gemeinsam "die Parteien" genannt.

§ 1 Gegenstand des Vertrages

(1) Gegenstand ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Rahmen der Bereitstellung der Online-Plattform flowerdesk (CRM- und Business-Management für Kreative: Kontakt-/Projektverwaltung, Angebote, Rechnungen, Verträge/Signaturen, E-Mail-Kommunikation, Terminplanung und Formulare/Buchungsstrecken).
(2) Die Verarbeitung erfolgt im Rahmen des bestehenden Nutzungsverhältnisses, das durch die Registrierung und Akzeptanz der AGB sowie dieses AVV zustande kommt.
(3) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Auftrag und nach Weisung des Auftraggebers.

§ 2 Umfang, Art und Zweck sowie Kreis der Betroffenen

(1) Art der Verarbeitung umfasst insbesondere: Speicherung und Hosting der eingegebenen Daten, Datenbankverarbeitung von Kontakt-, Projekt- und Auftragsdaten, Erstellung und Verwaltung von Angeboten/Rechnungen/Verträgen, Versand und Protokollierung von E-Mails, Termin-/Kalenderverwaltung sowie technische Analyse und Fehlerbehebung im Rahmen des Supports.
(2) Zweck ist die Bereitstellung, Verwaltung und Nutzung des CRM durch den Auftraggeber zur Abwicklung seiner Geschäftsbeziehungen gegenüber dessen Kund:innen und Interessent:innen.
(3) Datenarten: Stammdaten (Name, Anschrift, Telefon, E-Mail), Vertrags-/Projektdaten, Kommunikationsinhalte, Rechnungs-/Zahlungsdaten, Nutzerkennungen und IP-Adressen sowie Log- und Nutzungsdaten. Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind nicht Gegenstand der Verarbeitung und dürfen nicht eingestellt werden.
(4) Kreis der Betroffenen: Kund:innen, Interessent:innen und Kontakte des Auftraggebers sowie dessen Beschäftigte/Nutzer der Plattform.

§ 3 Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

(1) Die zum Zeitpunkt des Vertragsschlusses geltenden technischen und organisatorischen Maßnahmen (TOM) sind in der Anlage dargestellt. Der Auftragnehmer überprüft sie regelmäßig, passt sie bei Bedarf an und stellt sie dem Auftraggeber auf Anforderung zur Verfügung.
(2) Änderungen der TOM dürfen das vereinbarte Schutzniveau nicht unterschreiten.

§ 4 Berichtigung, Einschränkung und Löschung

Der Auftragnehmer berichtigt, schränkt die Verarbeitung ein oder löscht personenbezogene Daten nur nach dokumentierter Weisung des Auftraggebers. Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer wendet, leitet dieser das Anliegen unverzüglich an den Auftraggeber weiter. Funktionen zur Auskunft, zum Export und zur Löschung einzelner Betroffener stehen in der Anwendung zur Verfügung.

§ 5 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet Daten ausschließlich im Rahmen der Weisungen des Auftraggebers und unterrichtet diesen, wenn er eine Weisung für rechtswidrig hält.
(2) Die mit der Verarbeitung befassten Personen sind auf die Vertraulichkeit verpflichtet bzw. unterliegen einer angemessenen gesetzlichen Verschwiegenheit.

(3) Der Auftragnehmer unterstützt den Auftraggeber bei der Wahrung der Betroffenenrechte (Art. 12–23), bei Meldungen nach Art. 33/34 sowie bei Datenschutz-Folgenabschätzungen (Art. 35/36).

§ 6 Unterauftragnehmer

(1) Der Auftraggeber genehmigt den Einsatz der in Anlage 2 genannten Unterauftragsverarbeiter. Der Auftragnehmer informiert über beabsichtigte Änderungen; der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund widersprechen.
(2) Mit Unterauftragnehmern werden gleichwertige Datenschutzpflichten vereinbart; bei Drittlandtransfer werden Standardvertragsklauseln bzw. ein Angemessenheitsbeschluss (EU-US Data Privacy Framework) zugrunde gelegt.
(3) Reine Empfänger mit eigener Verantwortlichkeit oder eigener Rechtsgrundlage (z. B. Zahlungs-/Versanddienstleister) gelten nicht als Unterauftragnehmer.

§ 7 Kontrollrechte des Auftraggebers

Der Auftragnehmer stellt dem Auftraggeber die zum Nachweis der Einhaltung erforderlichen Informationen zur Verfügung und ermöglicht angemessene Überprüfungen (Art. 28 Abs. 3 lit. h DSGVO). Vor-Ort-Kontrollen bedürfen grundsätzlich einer angemessenen Ankündigung und erfolgen höchstens einmal jährlich, sofern kein konkreter Anlass besteht.

§ 8 Mitteilung bei Verstößen

(1) Der Auftragnehmer meldet dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich nach Bekanntwerden und stellt die für Meldungen nach Art. 33/34 DSGVO erforderlichen Informationen bereit.
(2) Der Auftragnehmer ergreift unverzüglich angemessene Maßnahmen zur Sicherung der Daten und zur Eindämmung möglicher nachteiliger Folgen und dokumentiert den Vorfall.

§ 9 Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet Daten nur auf Weisung des Auftraggebers. Die Nutzung der Anwendung und ihrer Einstellungen gilt als dokumentierte Weisung.
(2) Auskünfte an Dritte oder Betroffene erteilt der Auftragnehmer nur nach Zustimmung des Auftraggebers, es sei denn, er ist gesetzlich dazu verpflichtet.

§ 10 Löschung und Rückgabe

Nach Beendigung des Auftragsverhältnisses löscht der Auftragnehmer die verarbeiteten Daten oder gibt sie nach Wahl des Auftraggebers zurück, soweit keine gesetzliche Aufbewahrungspflicht (z. B. § 147 AO, § 257 HGB) entgegensteht. Steuerrelevante Belege werden bis zum Ablauf der gesetzlichen Fristen aufbewahrt. Die Löschung wird auf Anforderung nachgewiesen.

§ 11 Vertragslaufzeit

(1) Diese Vereinbarung wird wirksam, sobald der Auftraggeber sie im Rahmen der Registrierung auf der Plattform flowerdesk durch aktives Setzen einer Checkbox akzeptiert (bzw. im Konto unter "Auftragsverarbeitung" bestätigt).
(2) Sie gilt für die Dauer des bestehenden Nutzungsverhältnisses und endet mit dessen Beendigung; § 10 bleibt unberührt.

§ 12 Sonderkündigungsrecht

Der Auftraggeber kann diese Vereinbarung aus wichtigem Grund außerordentlich kündigen, insbesondere wenn der Auftragnehmer trotz Abmahnung schwerwiegend gegen diese Vereinbarung oder geltende Datenschutzvorschriften verstößt, rechtmäßige Weisungen wiederholt nicht umsetzt oder Kontrollrechte erheblich verweigert.

§ 13 Haftung

Es gilt die gesetzliche Haftungsregelung, insbesondere Art. 82 DSGVO. Im Innenverhältnis trägt jede Partei die Verantwortung für die von ihr zu vertretenden Datenschutzverstöße; die Parteien arbeiten zur Klärung der

Verantwortlichkeit zusammen.

§ 14 Schlussbestimmungen

(1) Es gilt deutsches Recht. Sind einzelne Bestimmungen unwirksam, bleibt die Wirksamkeit der übrigen unberührt; an die Stelle der unwirksamen Regelung tritt eine zulässige, die dem Zweck am nächsten kommt.
(2) Bei Widersprüchen zwischen diesem AVV und sonstigen Vereinbarungen gehen in Datenschutzfragen die Regelungen dieses AVV vor. Änderungen bedürfen der Textform.

Anlage – TOM, Teil I: Datenschutzgrundsätze (Art. 5 DSGVO)

Transparenz: klare Datenschutzinformationen, nachvollziehbare Datenflüsse, Unterstützung der Informationspflichten.
Zweckbindung & Datenminimierung: Verarbeitung nur für festgelegte Zwecke, "Privacy by Design/Default", Zugriff nach "Need to know", keine Speicherung über das Erforderliche hinaus.
Richtigkeit: Berichtigung unzutreffender Daten nach Kenntnis.
Vertraulichkeit, Integrität, Verfügbarkeit & Ausfallsicherheit: Verschlüsselung, sichere Übertragung, rollenbasierte Rechte, regelmäßige getestete Backups, Monitoring.
Rechenschaftspflicht: dokumentierte TOM, AV-Verträge, Verarbeitungsverzeichnis, regelmäßige Überprüfung.

Anlage – TOM, Teil II: Maßnahmen (Art. 32 DSGVO)

Zutrittskontrolle: Betrieb ausschließlich in professionellen Rechenzentren (EU/Frankfurt) mit Zutrittsschutz; Arbeitsplätze gesperrt/verschlüsselt.
Zugangskontrolle: persönliche Konten, scrypt-Passwort-Hashing, optionale Zwei-Faktor-Authentifizierung, Rate-Limiting/Brute-Force-Schutz, Security-Header (CSP/HSTS).
Zugriffskontrolle: rollenbasierte Rechte (owner/admin/Mitglied), strikte Mandantentrennung per Row-Level-Security, Verschlüsselung sensibler Daten at-rest (AES-256-GCM), Audit-Logging.
Weitergabekontrolle: TLS-Verschlüsselung in-transit, SSRF-Schutz bei serverseitigen Abrufen, limitierte Exporte.
Auftragskontrolle: AV-Verträge mit Unterauftragnehmern, vorherige Prüfung der Standards, gepflegte Unterauftragnehmerliste.
Verfügbarkeitskontrolle: tägliche, verschlüsselte Backups, getestete Wiederherstellung, redundante/abgesicherte Rechenzentren.
Trennungsgebot: logische Trennung der Mandanten- und Datenarten, zweckgebundene Verarbeitung.
Organisation: dokumentierte Verfahren, Datenschutz-Folgenabschätzung bei hohem Risiko, regelmäßige Überprüfung der TOM.

Anlage 2 — Unterauftragsverarbeiter

- Hostinger International Ltd. (Vilnius, Litauen) — Hosting der Anwendung & Datenbank; Rechenzentrum Digital Realty Germany GmbH, Frankfurt am Main (EU (Frankfurt am Main, Deutschland))
- Sendinblue GmbH (Brevo) — Versand von System-/Transaktions-E-Mails (EU)
- Ruby Foundry B.V. (ProductLift), Niederlande — Changelog/Roadmap (optional); Hosting Hetzner Online GmbH, Nürnberg (EU (Nürnberg, Deutschland))
- ThriveDesk — Support-Chat (optional); Hosting Hetzner Online GmbH (EU (Deutschland))
- Google Ireland Ltd. — Kalender/Meet (nur bei Verbindung) (EU/USA (SCC/DPF))
- Microsoft Ireland Ltd. — Outlook/Teams (nur bei Verbindung) (EU/USA (SCC/DPF))