# Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO für die Social Media Management CRM „Vibie“

Schwertfels Consulting GmbH
Leopoldstraße 150
80804 München

(nachfolgend „***Auftraggeber***“)

Kunde gemäß Hauptvertrag

(nachfolgend „***Auftragnehmer***“)

(Auftragnehmer und Auftraggeber nachfolgend jeweils „***Partei***“, gemeinsam „***Parteien***“)

## 1. Parteien und Vertragsgegenstand

Die Parteien haben einen Vertrag über die Bereitstellung der Web-basierten Social Media Management Plattform Vibie (nachfolgend „***Hauptvertrag***“) geschlossen. Der Auftragnehmer verarbeitet dabei im Auftrag des Auftraggebers personenbezogene Daten. Der Auftragnehmer ist Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO, und der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Mit dem vorliegenden Auftragsverarbeitungsvertrag legen die Parteien ihre Pflichten und Rechte nach Art. 28 DSGVO fest.

## 2. Geltung der EU-Standardvertragsklauseln gemäß Art. 28 Abs. 7 DSGVO

Die Parteien vereinbaren hiermit die Geltung der Standardvertragsklauseln zwischen Verantwortlichem und Auftragsverarbeitern gemäß **Art. 28 Abs. 7** der Europäischen Datenschutz-Grundverordnung („***DSGVO***“) ((EU) 2021/915 vom 4. Juni 2021) („***Standardvertragsklauseln***“). Die Standardvertragsklauseln sind im Amtsblatt der Europäischen Union L 199/18 veröffentlicht und können unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32021D0915 abgerufen werden. Sie sind Bestandteil dieses Auftragsverarbeitungsvertrags.
In den Klauseln 1 lit. a, 8 lit. c Nr. 4, 9.1 lit. b und lit. c sowie 9.2 Abs. 3 der Standardvertragsklauseln wählen die Parteien hiermit Option 1.
Die fakultative Klausel 5 der Standardvertragsklauseln (Kopplungsklausel) gilt nicht.
Folgende Klauseln der Standardvertragsklauseln gelten nicht: Klausel 2 (Unabänderbarkeit) und Klausel 7.7 lit. e (Drittbegünstigtenklausel in Verträgen mit Unterauftragsverarbeitern).
Die Informationen zur Vervollständigung der Anhänge I-IV der Standardvertragsklauseln sind in den Anhängen I-IV dieses Auftragsverarbeitungsvertrags enthalten.

## 3. Unterauftragsverarbeiter

In Klausel 7.7 lit. a der Standardvertragsklauseln (Einsatz von Unterauftragsverarbeitern) vereinbaren die Parteien Option 2 (**allgemeine schriftliche Genehmigung**). Die Frist für die Benachrichtigung über neue oder geänderte Unterauftragsverarbeiter beträgt 30 Tage. Widerspricht der Auftraggeber einem neuen Unterauftragsverarbeiter, werden die Parteien nach Treu und Glauben verhandeln, um eine gütliche Einigung zu finden. Kommt eine solche binnen 14 Tagen nicht zustande, so ist der Auftragnehmer zur (Teil-)Kündigung des Vertrags berechtigt, soweit der neue Unterauftragsverarbeiter für die Erbringung der Vertragsleistungen benötigt wird. Etwaig im Voraus bezahlte Vergütungen für die gekündigten Leistungen werden vom Auftraggeber in diesem Fall anteilig erstattet.

## 4. Kontrollrechte

Die Beantwortung von Anfragen nach Klausel 7.6.b und die zur Verfügungstellung von Informationen nach Klausel 7.6.c Satz 1 der Standardvertragsklauseln erfolgt, indem der Auftragnehmer dem Auftraggeber vorliegende Dokumentationen, Zertifizierungen, Berichte und Unterlagen betreffend die Datenverarbeitung und Sicherheitsmaßnahmen bereitstellt („***Sicherheitsdokumentation***"). Sollte die Sicherheitsdokumentation nicht ausreichen, um die Einhaltung der Standardvertragsklauseln durch den Auftragnehmer zu bewerten (z.B. beim konkreten Hinweisen der Nichteinhaltung), wird der Auftragnehmer zusätzliche schriftliche Anfragen des Auftraggebers beantworten. Wenn und soweit auch diese nicht ausreichen, gestattet der Auftragnehmer Prüfungen vor Ort, insbesondere wenn eine zuständige Aufsichtsbehörde eine solche Prüfung verlangt.

## 5. Vergütung

Aufwände des Auftragnehmers für folgende Leistungen sind vom Auftraggeber nach tatsächlich angefallenem Aufwand gesondert zu vergüten: Aufwände, die im Rahmen von Kontrollen des Auftraggebers beim Auftragnehmer vor Ort entstehen, sowie Aufwände für das Erstellen von Dokumentationen, Zertifizierungen, Berichten und Unterlagen zu Sicherheitsmaßnahmen, die über das hinausgehen, was beim Auftragnehmer bereits vorliegt.
Vor Entstehen entsprechender Kosten wird der Auftragnehmer den Auftraggeber hierauf hinweisen. Die Höhe der Vergütung für Arbeitsaufwände entspricht den zwischen den Parteien vereinbarten Sätzen, hilfsweise einer branchen- und ortsüblichen Vergütung.

## 6. Schlussbestimmungen

Sollten einzelne Bestimmungen dieses Auftragsverarbeitungsvertrags unwirksam sein oder werden, so wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. Statt der unwirksamen Bestimmung gilt dasjenige, was die Parteien nach dem ursprünglich angestrebten Zweck unter wirtschaftlicher Betrachtungsweise redlicherweise vereinbart hätten. Das Gleiche gilt im Falle einer Vertragslücke.

In Bezug auf Formerfordernisse, anwendbares Recht und Gerichtsstand gelten die Bestimmungen des Hauptvertrags.

* * *

## ANHANG I: LISTE DER PARTEIEN

### Verantwortlicher

Verantwortlicher ist der auf der ersten Seite des Auftragsverarbeitungsvertrags angegebene Auftraggeber.
Ist der Auftraggeber in Bezug auf den Vertragsgegenstand seinerseits Auftragsverarbeiter für einen Dritten, so gilt der Auftraggeber im Verhältnis zum Auftragnehmer für die Zwecke dieses Auftragsverarbeitungsvertrags als Verantwortlicher.

### Auftragsverarbeiter

Auftragsverarbeiter ist der auf der ersten Seite des Auftragsverarbeitungsvertrags angegebene Auftragnehmer.
Ansprechpartner beim Auftragnehmer: Ertug Kilickaya, Geschäftsführer, Leopoldstraße 150, 80804 München; Tel: 089 / 217 04 90 20 E-Mail: privacy@vibie.de

**ANHANG II: BESCHREIBUNG DER VERARBEITUNG**

## 1. Kategorien von betroffenen Personen, deren personenbezogene Daten verarbeitet werden:

Nutzer des Vibie-Dienstes (Kunden des Auftraggebers): Personen, die im Auftrag des Auftraggebers die Vibie-Plattform nutzen, um Social-Media-Aktivitäten zu verwalten (z.B. Mitarbeiter des Auftraggebers, Marketing-Teams).

Endnutzer der Social-Media-Profile des Auftraggebers: Personen, die mit den Social-Media-Profilen interagieren, die der Auftraggeber über Vibie verwaltet (z.B. Follower, Kommentatoren, Personen, die Nachrichten senden).
Kontakte des Auftraggebers: Personen, deren Daten im Rahmen der Nutzung von Vibie durch den Auftraggeber eingegeben oder verarbeitet werden (z.B. in Nachrichten, Posts, Erwähnungen).

## 2. Kategorien der verarbeiteten personenbezogenen Daten

Nutzerdaten des Vibie-Dienstes:

- Identifikationsdaten: Vorname, Nachname, E-Mail-Adresse, Passwort (gehasht).
- Rechnungsdaten: Adresse, ggf. USt-ID Nr.
- Zugriffstoken für die angebundenen Social-Media-APIs (LinkedIn, Pinterest, Meta (Instagram / Facebook), TikTok, Youtube etc.).
- Nutzungspräferenzen: z.B. Tonalität, Beitragslänge, Hashtagnutzung, Emoji-Verwendung, Persona (vom User individuell definierte Beitragspräferenzen in Form einer Persona) Formulierungswünsche, Beispielbeiträge (im Rahmen der User-Personalisierung).
- Protokolldaten: Log-Daten über die Nutzung des Services.

**Daten von Endnutzern der Social-Media-Profile:**

- Öffentlich zugängliche Profildaten von Social-Media-Nutzern
- Interaktionsdaten: Daten über Reaktionen, Kommentare, Shares, Direct Messages.

**Vom Auftraggeber erstellte und verwaltete Inhalte:**

- Beiträge und Kampagnen: Texte, Bilder, Videos, Links.
- Planungsdaten: Zeitpunkte für Veröffentlichungen.
- Analytics-Daten: Performance-Daten der Beiträge und Kampagnen (Reichweite, Engagement, Follower-Zahlen, Profilansichten etc., soweit über die APIs der Plattformen zugänglich und vom Auftraggeber über Vibie abgerufen).
- Daten aus der Mediathek: Hochgeladene oder KI-generierte Bilder und Videos.
- Daten aus der Research- & Brainstorming-Funktion: Suchanfragen, gebookmarkte Inhalte.

## 3. Sensible verarbeitete Daten (falls zutreffend)

Es werden keine sensiblen Daten verarbeitet.

## 4. Art der Verarbeitung

Gegenstand der Auftragsverarbeitung ist: Bereitstellung von Vibie, ein Content-Management-System (CMS), das die zentrale Verwaltung verschiedener Social-Media-Profile (Instagram, TikTok, Facebook, LinkedIn, Pinterest) ermöglicht.
Der Auftragnehmer führt folgende Verarbeitungen durch: Bereitstellung von Vibie, einem Content-Management-System (CMS), zur zentralen Verwaltung und Optimierung von Social-

Media-Profilen auf Plattformen wie Instagram, TikTok, Facebook, LinkedIn und Pinterest gemäß Hauptvertrag/Leistungsvereinbarung.
Wartung und Betrieb der zugehörigen Server.

## 5. Zweck(e), für den/die die personenbezogenen Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet werden

Bereitstellung und Betrieb der Vibie-Plattform als Content-Management-System (CMS) zur zentralen Verwaltung, Erstellung, Planung, Veröffentlichung, Analyse und Optimierung von Social-Media-Aktivitäten auf Plattformen wie Instagram, TikTok, Facebook, LinkedIn und Pinterest.
Soweit der Auftragnehmer die Daten für nachfolgende eigene Zwecke nutzt, ist dies nicht Gegenstand der Auftragsverarbeitung, sondern der Auftragnehmer ist eigenständiger Verantwortlicher:

- Produktverbesserung
- Entwicklung neuer Produkte
- Tracking der App/Website-Nutzung

## 6. Dauer der Verarbeitung

Die Laufzeit der Vereinbarung entspricht der Laufzeit des Hauptvertrags..

## ANHANG III: TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN ZUR GEWÄHRLEISTUNG DER DATENSICHERHEIT

### 1. Vertraulichkeit

Unter dem nachfolgenden Kapitel „Vertraulichkeit“, sind Maßnahmen darzustellen, die dem Schutz personenbezogener Daten vor unbefugter oder unbeabsichtigter Preisgabe dienen. Dies umfasst Schutz vor externen wie internen Angreifern (z.B. Hacker, frustrierte oder neugierige Mitarbeiter) sowie Schutz vor strukturellen Gefährdungen (z.B. ungeschulte Mitarbeiter, mangelhafte Rollen-/Rechtekonzepte, Mängel in der Datenschutzorganisation).

#### 1.1 Zutrittskontrolle

- Videoüberwachung
- Alarmanlage
- Sicherheitsschlösser
- Chipkartensystem

#### 1.2 Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten benutzt werden können.

- Zugangsschutz zu Systemen durch Authentifizierung (Benutzerkennung mit Passwort)
- Verfahren für die Erteilung und den Entzug von Berechtigungen einschließlich Protokollierung
- Passwortrichtlinie (Mindestpasswortlänge, Komplexität, Einmaligkeit, Erzwingung durch das System)
- Schutz von IT-Systemen vor Viren und sonstiger Schadsoftware mit Updates
- Erhöhte Auth-Sicherheitsmechanismen wie Tokenisierung der Authentifizierung inklusiver Token-Refresh-Systemen

#### 1.3 Zugriffskontrolle

Maßnahmen zur Sicherstellung, dass die zur Benutzung von Datenverarbeitungssystemen berechtigten Nutzer nur auf solche Daten zugreifen können, für die sie berechtigt sind, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt kopiert, verändert oder gelöscht werden können.

- Schriftliche dokumentiertes Berechtigungskonzept
- Regelmäßige Prüfung von Rollen, Berechtigungen und Zuweisung von Rollen zu Personen
- Protokollierung von Änderungen bei Rollen, Berechtigungen und bei der Zuweisung von Rollen zu Personen
- Schriftliche Anweisung zum Umgang mit ausscheidenden Mitarbeitern
- Beschränkung des Admin-Zugriffs (z.B. Anzahl der Admins)
- Protokollierung von Änderungen, Löschungen und Datenexporten
- Dokumentierte Datenträgerverwaltung
- Anweisung zum Sicheren Löschen von Datenträgern
- Anweisung zur sicheren Vernichtung von Unterlagen mit personenbezogenen Daten (Aktenvernichter)

#### 1.4 Trennung

Maßnahmen zur Sicherstellung, dass personenbezogene Daten, die für unterschiedliche Auftraggeber oder für unterschiedliche Zwecke erhoben wurden, getrennt verarbeitet werden können.

- Physische Trennung von Datenbeständen unterschiedlicher Auftraggeber (anderer Server, andere Festplatte)
- Logische Trennung von Datenbeständen unterschiedlicher Auftraggeber (Zuordnung von Datensätzen zu Auftraggebern, unterschiedliche Dateiordner/Datenbanken/Tabellen).
- Trennung von Produktiv-, Test- und Entwicklungssystemen
- Mandantenfähigkeit (z. B. unterschiedliche Einstellungen je Mandant möglich, etwa zur Speicherdauer)

#### 1.5 Verschlüsselung (Art 32 Abs. 1 lit. a) DSGVO)

Maßnahmen zur Verschlüsselung von Daten.

- Automatisches Passworthashing via bcrypt (Salt-Faktor: 10) inklusive sicherer Passwort-Verifikation mit bcrypt.compare
- IAM-basierte Zugriffskontrolle mit granulare Berechtigungen
- Automatische Rotation von Keys
- Refresh-Tokens nur serverseitig zugänglich
- CORS-Protection (strikte Origin-Validierung)
- Request-Size-Limits

- Header Buffer Protection (Schutz vor Header-Overflow-Angriffen)
- Verschlüsselte Connection-Strings

**Kryptographische Token-Generierung:**

- E-Mail-Verifikation: SHA256-Hashing + randomBytes (32)
- Passwort-Reset: Sichere Tokengenerierung mit zeitlicher Begrenzung (24h)
- OAuth State Parameter für CSRF-Schutz

**JWT-Token-Verschlüsselung:**

- Access-Tokens: 15-minütige Gültigkeitsdauer, signiert
- Refresh-Tokens: 30 Tage Gültigkeitsdauer für sichere Token-Erneuerung
- Token-Validierung: Strikte Typ-Prüfung (access vs. Refresh tokens)
- Secret Management: JWT über AWS Secrets Manager verwaltet
- Kryptographische Validierung mit HMAC-SHA256 für Webhooks
- Timing-Safe Comparison: Verhinderung von Timing-Angriffen

**mTLS für erhöhte Webhook-Sicherheit:**

- Client Certificate Validation
- Expected CN
- AWS ALB Integration
- DigiCert Root CA

#### 1.6 Pseudonymisierung (Art 32 Abs. 1 lit. a) DSGVO)

Maßnahmen zu Pseudonymisierung, d.h., dem Ersetzen von Identifikationsmerkmalen wie z.B. eines Namens, einer Anschrift oder einer E-Mail-Adresse durch eindeutige Kennung, dem Pseudonym. Die Identifikationsmerkmale (und die Zuordnung zum Pseudonym) werden getrennt von den Inhaltsdaten aufbewahrt und besonders gesichert. Bei der Pseudonymisierung ist eine Re-Identifikation möglich, es liegen damit personenbezogene Daten vor (keine Anonymisierung!).

- Ersetzung durch Codes: Eindeutige Identifikationsmerkmale wie Namen oder E-Mail-Adressen werden durch zufällig generierte Codes ersetzt (ObjectIDs)
- Kreierte Inhalte auf der Plattform werden via User-IDs verwaltet, nicht mit den echten Identifikationsmerkmalen
- Zugriffskontrollen: Nur ein begrenzter Personenkreis erhält Zugang zu den Zuordnungsinformationen

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

Unter dem Kapitel „Integrität“, sind Maßnahmen darzustellen, die dazu dienen, personenbezogene Daten vollständig und richtig bereitzustellen. Die Maßnahmen zielen darauf ab, unzulässige Änderungen an den Daten zu erkennen und Verfahren zur Berichtigung vorzuhalten.

#### 2.1 Eingabekontrolle

Maßnahmen zur Sicherstellung, dass überprüft werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder gelöscht worden sind.

- Protokollierung von Erstellung, Eingabe, Änderung und Löschung und anderen relevanten Aktionen mit Daten (z.B. Export, Reports)
- Protokollierung des Benutzers, der eine Aktion durchgeführt hat

#### 2.2 Weitergabekontrolle

Maßnahmen zur Sicherstellung, dass personenbezogenen Daten bei der elektronischen Übertragung oder beim Transport auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

- Schriftliche Anweisung zum sicheren Datenträgertransport
- Sicherung bei elektronischer Übermittlung (Verschlüsselung, siehe oben)
- Regelungen für Tele- / Heimarbeiter, Fernwartung

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

Unter dem Kapitel „Verfügbarkeit“, sind Maßnahmen darzustellen, die sicherstellen, dass personenbezogene Daten dann zur Verfügung stehen, wenn sie benötigt werden. Dies umfasst auch Maßnahmen zur Wiederherstellung der Daten bei Verlust oder Vernichtung.

#### 3.2 Allgemeine Maßnahmen

Grundlegende Maßnahmen zur Sicherstellung der Verfügbarkeit.

- Verwendung von Industrie-Standards bei Cloud-Servern zur höchstmöglicher Sicherstellung der Verfügbarkeit
- Schriftliches Backup-Konzept (Backup-Strategie („3-2-1), Vollbackup/differenzielles Backup, Periodizität, Umfang, Aufbewahrungsdauer, Speicherorte und -methode)
- Datensicherungs- und Wiederherstellungskonzept
- Tests von Backup und Recovery Verfahren
- Virenschutz und Firewallnutzung
- Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)
- Aufbewahrung von Backups an räumlich getrenntem Ort

#### 3.3 Insbesondere: Wiederherstellbarkeit nach Zwischenfall (Art 32 Abs. 1 lit. c) DSGVO)

Maßnahmen, um die Verfügbarkeit von personenbezogenen Daten nach einem physischen oder technischen Zwischenfall rasch wieder herzustellen.

- Notfallplan zur Sicherstellung angemessener „Wiederanlaufzeiten“

#### 3.4 Insbesondere: Belastbarkeit (Art 32 Abs. 1 lit. b) DSGVO)

Maßnahmen, um datenverarbeitende Systeme widerstandsfähig zu machen, wenn nicht verhinderbare Störungen auf die Systeme einwirken.

- Aufbau von Redundanzen zum Abfang des Ausfalls von Netzknoten
- Backupkonzepte und Notfallkonzepte
- DDoS Abwehrmechanismen

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

Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit technischer und organisatorischer Maßnahmen.

- Festlegung von Verantwortlichkeiten und Prozessen, um angemessene Datensicherheitsmaßnahmen festzulegen und regelmäßig zu prüfen (Datensicherheitsrichtlinie)
- Verfahren zum Testen der Wirksamkeit der Maßnahmen (z.B. Simulation von Angriffen, Penetrationstest)

**5. Weitere organisatorische Maßnahmen / Auftragskontrolle**

Für Mitarbeiter des Auftragnehmers verbindliche Richtlinien zur Auftragsverarbeitung mit folgenden Regelungen:

- Rollen und Verantwortlichkeiten (Datenschutzbeauftragter, Datenschutz-Manager, Datensicherheits-Manager)
- Verantwortlichkeiten und Prozesse zum Abschluss von Unter-Auftragsverarbeitungs-Verträgen mit Unter-Auftragnehmern, einschließlich deren Prüfung
- Verantwortlichkeiten und Prozesse bei der Einschaltung von weiteren Auftragsverarbeitern (Unter-Auftragsverarbeitern), einschließlich der Kontrolle und Vertragsprüfung
- Verantwortlichkeiten und Prozesse zum Umgang mit Weisungen von Auftraggebern und zur Sicherstellung der Zweckbindung bei der Auftragsverarbeitung
- Rückgabe und Löschung von Daten bei Ende der Auftragsverarbeitung
- Verantwortlichkeiten und Prozesse für den Umgang mit Anträgen von Betroffenen
- Verantwortlichkeiten und Prozesse für die Führung eines Verzeichnisses der Verarbeitungstätigkeiten (als Auftragsverarbeiter)
- Erkennung von Datenschutzvorfällen und Meldung an den Auftraggeber
- Sicherstellung der Verpflichtung der Beschäftigten zur Vertraulichkeit
- Verfahren zur Überprüfung und Anpassung der Richtlinie zur Auftragsverarbeitung

## ANHANG IV: LISTE DER UNTERAUFTRAGSVERARBEITER

Die Liste der vom Auftragnehmer bei Vertragsschluss genehmigten Unterauftragsverarbeiter ist online abrufbar unter https://www.vibie.de/unterauftragsverarbeiter. Sofern der Auftragnehmer dem Auftraggeber Änderungen an der Liste der Unterauftragsverarbeiter mitzuteilen hat, wird der Auftragnehmer die Liste auf der genannten Webseite aktualisieren.