Vereinbarung über eine Auftragsverarbeitung gemäß Art. 28 DSGVO

Abgeschlossen zwischen

Dem Verantwortlichen (im Folgenden ‚Auftraggeber')

_____

_____

_____

_____

_____

Und

dem Auftragsverarbeiter (im Folgenden ‚Auftragnehmer')

Hochzeit.Management GmbH

Geschäftsführer: Andreas Schwarzlmüller

Linzerstraße 200 Stock 1, 4600 Wels,

Tel.: +43 664 264 629 7

E-Mail: support@hochzeit.management

1. **Gegenstand der Vereinbarung**

    a. **Gegenstand**

Der Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

- Verarbeitung der vom Auftraggeber in den Dienst https://app.hochzeit.management eingepflegten (personenbezogenen) Daten seiner Kunden, wobei seitens des Auftraggebers insbesondere die folgenden Verarbeitungshandlung auf dem Dienst https://app.hochzeit.management gesetzt werden können:
    - Speicherung und Verwaltung der Stammdaten der Kunden (Brautpaare)
    - Kalenderverwaltung
    - To-Do-Listen-Verwaltung
    - Mail-Kommunikation mit den Kunden über ein Mail-Postfach
    - Erstellung und Verwaltung von Angeboten und Rechnungen
    - Tracking der Mails, welche an Kunden versandt wurden (hierfür holt der Auftraggeber bei den Kunden eine Einwilligung nach Art 7 DSGVO vorab ein)

Die genannten Verarbeitungen ergeben sich überdies aus den dem Geschäftsverhältnis zugrundeliegenden AGB des Dienstes https://app.hochzeit.management.

    b. **Art und Zweck der Verarbeitung von Daten**

Nähere Beschreibung des Auftrages in Hinblick auf Art und Zweck der vorgesehenen Verarbeitung durch den Auftragnehmer:

Gegenstand des Vertrages ist **nicht die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragnehmer.** Im Zuge der Leistungserbringung des Auftragnehmers im Bereich des Auftraggebers kann ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden.

    c. **Art der Daten**

Folgende Datenkategorien werden verarbeitet:

Personenstammdaten, Kontaktdaten, Vertragsdaten, Verrechnungsdaten, Kommunikationsdaten, IP Adressen und alle weiteren Datenkategorien, welche durch den Auftraggeber zur Erfüllung seiner (vor)vertraglichen Pflichten gegenüber seinen Kunden verarbeitet werden müssen oder deren Verarbeitung und Speicherung durch dessen Kunden ausdrücklich zugestellt wurde.

    d. **Kategorien betroffener Personen**

Folgende Kategorien betroffener Personen unterliegen der Verarbeitung:

Kunden, Lieferanten, Mitarbeiter, Ansprechpartner, und alle weiteren Kategorien betroffener Personen, welche durch den Auftraggeber zur Erfüllung seiner (vor)vertraglichen Pflichten gegenüber seinen Kunden verarbeitet werden müssen oder deren Verarbeitung und Speicherung durch dessen Kunden ausdrücklich zugestellt wurde.

2. Dauer der Vereinbarung

Die Vereinbarung ist auf unbestimmte Zeit geschlossen und bleibt aufrecht, so lange ein unter Punkt (1) Gegenstand definiertes Vertragsverhältnis zwischen dem Auftraggeber und Auftragnehmer aufrecht bleibt.

Der Auftragnehmer kann diese Vereinbarung aus technischer oder organisatorischer Notwendigkeit anpassen. Diese Anpassung (Versionierung) wird dem Auftraggeber mindestens 4 Wochen vor Inkrafttreten der neuen Version in geeigneter Weise, analog oder digital, zur Kenntnis gebracht.

Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. Pflichten des Auftragnehmers

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers 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) Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

(3) Wahrung der Vertraulichkeit und Verschwiegenheit: Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung im Sinne von § 6 DSG (2018) und § 11 UWG unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

(4) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32ff DSGVO ergriffen hat. Konkret handelt es sich hierbei um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Einzelheiten hierzu finden sich im Anhang (Technisch-organisatorische Maßnahmen).

(5) Mitwirkungspflicht bei Betroffenenrechten: Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Betroffenenrechte nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen. Für die Erbringung dieser Leistungen kann der Auftragnehmer eine angemessene Vergütung zur Abrechnung bringen.

(6) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer durchzuführen (sicherzustellen). Für die Erbringung dieser Leistungen kann der Auftragnehmer eine angemessene Vergütung zur Abrechnung bringen.

(7) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten. Dazu gehören Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation.
Für die Erbringung dieser Leistungen kann der Auftragnehmer eine angemessene Vergütung zur Abrechnung bringen.

(8) Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu erstellen hat.

(9) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind. Diese Kontrollen sind rechtzeitig anzukündigen und so durch zu führen, dass der laufende Geschäftsbetrieb nicht gestört wird. Diese Kontrollen haben während der gewöhnlichen Geschäftstätigkeit zu

erfolgen. Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

(10) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, sämtliche in seinem Besitz gelangten Unterlagen, erstellte Verarbeitungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber zu übergeben oder in dessen Auftrag zu vernichten. Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.
Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.
Gleiches gilt für Test- und Ausschussmaterial bzw. Test- und Ausschussdaten.
Für die Erbringung dieser Leistungen kann der Auftragnehmer eine angemessene Vergütung zur Abrechnung bringen.

(11) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

(12) Für Unterstützungsleistungen, die nicht in der ggf. vereinbarten Leistungsvereinbarung enthalten sind oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

4. Technisch-organisatorische Maßnahmen

Die technischen und organisatorischen Maßnahmen (TOMs) unterliegen dem technischen Fortschritt und der Weiterentwicklung. Es ist dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen, soweit das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

Einzelheiten sind dem Anhang zu entnehmen.

5. Ort der Durchführung der Datenverarbeitung

Ausschließliche Durchführung innerhalb der EU/des EWR
Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw des EWR durchgeführt.

6. Sub-Auftragsverarbeiter

Als Sub-Auftragsverarbeiter im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Fernwartungssysteme, Bereitstellung von Infrastruktur, Post/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit,

Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

Der Auftragnehmer kann Sub-Auftragsverarbeiter zur unmittelbaren Erbringung der Hauptdienstleistung hinzuziehen.

Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer dies dem Auftraggeber eine angemessene Zeit vorab schriftlich anzeigt und
- der Auftraggeber nicht gegenüber dem Auftragnehmer schriftlich Einspruch gegen die geplante Auslagerung erhebt und
- die erforderlichen Vereinbarungen zwischen dem Auftragnehmer und dem Sub-Auftragsverarbeiter gemäß des Art. 28 Abs. 4 DSGVO abgeschlossen werden.
  Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

Festgehalten wird, dass der Auftragnehmer bereits jetzt folgende Sub-Auftragnehmer verpflichtet hat, welche mit Abschluss dieser Vereinbarung als vom Auftraggeber genehmigt gelten:

corner4 Information Technology GmbH
Johann Roithner-Straße 131
4050 Traun
Österreich

sigmavista it consulting GmbH
Johann-Roithner-Straße 131
4050 Traun
Österreich

7. Vermittlung von Drittanbietern und Lizenzen

Es wird festgehalten, dass Lizenzgeber und dritte Cloud Anbieter (wie zBsp. Microsoft, Adobe, vmware, veeam, google, facebook, etc.), nicht als Sub-Auftragnehmer anzusehen sind, sondern es zu einem direkten, von dieser Vereinbarung unabhängigen, Vertragsverhältnis zwischen dem Auftraggeber und dem Lizenzgeber/Cloud Anbieter kommt. Der Auftragnehmer führt im Rahmen der Beauftragung durch den Auftraggeber zur Einrichtung derartiger Dienste die nötigen Schritte durch. Der Auftraggeber muss seinerseits für eine angemessene Vereinbarung zwischen ihm und dem Lizenzgeber/Cloud bzw. sonstigen Drittanbietern Sorge tragen.

8. Haftung

Auf Art. 82 DSGVO wird verwiesen. Im Übrigen wird folgendes ergänzend vereinbart:

(1) Der Auftragnehmer haftet dem Auftraggeber für Vorsatz und grobe Fahrlässigkeit unbeschränkt. Für leichte Fahrlässigkeit haftet er nur bei Verletzung einer wesentlichen Vertragspflicht (Kardinalpflicht), deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt

erst ermöglicht und auf deren Einhaltung der Auftraggeber regelmäßig vertrauen darf, sowie bei Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit.

(2) Die Haftung des Auftragnehmers ist im Falle leichter Fahrlässigkeit summenmäßig beschränkt auf die Höhe des vorhersehbaren Schadens, mit dessen Entstehung typischerweise gerechnet werden muss.

(3) Soweit die Haftung des Auftragnehmers nach den vorgenannten Vorschriften ausgeschlossen oder beschränkt wird, gilt dies auch für Erfüllungsgehilfen des Auftragnehmers.

9. Rechtsnachfolge

Diese Vereinbarung geht an allfällige Rechtsnachfolger des Auftragnehmers über und bleibt im Sinne von Punkt 2. dieser Vereinbarung weiterhin aufrecht.

10. Allgemeines

(1) Für Nebenabreden ist die Schriftform oder ein dokumentiertes elektronisches Format erforderlich. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.
(2) Der Auftraggeber nimmt zur Kenntnis, dass diese Vereinbarung über eine Auftragsverarbeitung jeweils Bezug auf die aktuellen technischen und rechtlichen Bestimmungen nimmt. Für den Fall, dass seitens des Auftragsnehmers diese Vereinbarung aktualisiert wird, gelten diese Änderungen als akzeptiert, wenn der Auftraggeber – nach Erhalt der aktualisierten Fassung – diesen Änderungen gesamt oder einzeln nicht binnen zwei Wochen widerspricht.
(3) Es gilt die Anwendung des österreichischen Rechts als vereinbart. Als Gerichtsstand wird das sachlich in Betracht kommende Gericht in Wels, Oberösterreich, vereinbart.

Anhang – Technisch-organisatorische Maßnahmen (TOMs)

Vertraulichkeit

- Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen: Schlüssel, Magnet- oder Chipkarten, Alarmanlagen;
- Zugangskontrolle: Schutz vor unbefugter Systembenutzung, Kennwörter (einschließlich entsprechender Policy), zT. automatische Sperrmechanismen;
- Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, Standard-Berechtigungsprofile auf „need to know-Basis“, Standardprozess für Berechtigungsvergabe, periodische Überprüfung der vergebenen Berechtigungen, insb. von administrativen Benutzerkonten;
- Klassifikationsschema für Daten: Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

Integrität

- Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, Verschlüsselung, Virtual Private Networks (VPN);

Verfügbarkeit und Belastbarkeit

- Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, Backup-Strategie (online und/oder offline; on-site und/oder off-site; je nach vereinbartem Leistungsumfang), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne; Mehrstufiges Sicherungskonzept (je nach vereinbartem Leistungsumfang), Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern;

- Löschungsfristen: Sowohl für Daten selbst als auch Metadaten wie Logfiles, udgl.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen in durch den Auftragnehmer erstellten Systemen;
- Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, wie formalisiertes Auftragsmanagement, Auswahl des Auftragsverarbeiters, Vorabüberzeugungspflicht, Nachkontrollen.