Vereinbarung
über eine
Auftragsverarbeitung nach Art 28 DSGVO

Der Verantwortliche:

Kunde
von
FALZEDER Consulting

(im Folgenden Auftraggeber)

Der Auftragsverarbeiter:

FALZEDER Consulting
Vera Falzeder
Fleckendorf 7
4052 Ansfelden

(im Folgenden Auftragnehmer)

1. Allgemeine Bestimmungen und Auftragsgegenstand

1.1. Mit diesem Vertrag soll sichergestellt werden, dass die Anforderungen der Datenschutz-Grundverordnung) bei der Übermittlung personenbezogener Daten an einen Auftragnehmer eingehalten werden Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er allein ist für Beurteilung der Zulässigkeit der Datenverarbeitungsvorgänge nach Art. 6 DSGVO und die Wahrung der Betroffenenrechte verantwortlich.

1.2. Dieser Vertrag gilt für die Übermittlung personenbezogener Daten gemäß Anhang 1. Die Anlage zu diesem Vertrag mit den darin enthaltenen Anhängen ist Bestandteil dieses Vertrages

1.3. Dieser Vertrag enthält geeignete Garantien, einschließlich durchsetzbarer Rechte betroffener Personen und wirksamer Rechtsbehelfe gemäß Artikel 46 Absatz 1 und Artikel 46 Absatz 2 Buchstabe c der DSGVO.

1.4. Dieser Vertrag gilt unbeschadet der Verpflichtungen, denen der Auftraggeber gemäß der DSGVO unterliegt.

1.5. Die Einzelheiten der Datenübermittlung(en), insbesondere die Kategorien der übermittelten personenbezogenen Daten und der/die Zweck(e), zu dem/denen sie übermittelt werden, sind in Anhang 1 aufgeführt.

1.6. Der Auftraggeber versichert, sich im Rahmen des Zumutbaren davon überzeugt zu haben, dass der Auftragnehmer – durch die Umsetzung geeigneter technischer und organisatorischer Maßnahmen – in der Lage ist, seinen Pflichten aus diesem Vertrag nachzukommen.

1.7. Die Verarbeitung der Daten durch den Auftragnehmer findet ausschließlich auf dem Gebiet des Staates Österreich, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des EWR- Abkommens statt. Die Verarbeitung außerhalb dieser Staaten erfolgt nur unter den Voraussetzungen von Kapitel 5 der DSGVO (Art. 44 ff.) und mit vorheriger Zustimmung des Auftraggebers.

1.8. Die Vergütung wird außerhalb dieses Vertrags vereinbart.

2. Vertragslaufzeit und Kündigung

Diese Vereinbarung ist als Ergänzung zum jedem Vertrag zwischen FALZEDER Consulting und dessen Kunden zu verstehen und beginnt mit dem Zeitpunkt, ab dem FALZEDER Consulting als Auftragsverarbeiter für den Kunden tätig wird. DieVereinbarung wird auf unbestimmte Zeit geschlossen und kann von jeder Vertragspartei mit einer Frist von einem Monaten ordentlich gekündigt werden. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. Weisungen des Auftraggebers

3.1. Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung ggü. dem Auftragnehmer zu. In dieser Rolle kann er insbesondere die unverzügliche Löschung, Berichtigung, Sperrung oder Herausgabe der vertragsgegenständlichen Daten verlangen. Der Auftragnehmer ist verpflichtet, den Weisungen des Auftraggebers Folge leisten, sofern keine berechtigten vertraglichen oder gesetzlichen Interessen entgegenstehen.

3.2. Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit der Auftragnehmer substantiiert anzweifelt, ist der Auftragnehmer berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert.

3.3. Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z.B. per E-Mail) zu erteilen. Mündliche Weisung sind auf Verlangen des Auftragnehmers schriftlich oder

in einem elektronischen Format durch den Auftraggeber zu bestätigen. Der Auftragnehmer hat Person, Datum und Uhrzeit der mündlichen Weisung in angemessener Form zu protokollieren.

3.4. Der Auftraggeber benennt auf Verlangen des Auftragnehmers eine oder mehrere weisungsberechtigte Personen. Änderungen sind dem Auftragnehmer unverzüglich mitzuteilen.

4. Kontrollbefugnisse des Auftraggebers

4.1. Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch von ihm 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.

4.2. Der Auftraggeber hat dafür zu sorgen, dass die Kontrollmaßnahmen verhältnismäßig sind und den Betrieb des Auftragnehmers nicht mehr als erforderlich beeinträchtigen. Insbesondere sollen Vorortkontrollen grundsätzlich zu den üblichen Geschäftszeiten und nach Terminvereinbarung mit angemessener Vorlauffrist erfolgen, sofern der Kontrollzweck einer vorherigen Ankündigung nicht widerspricht.

4.3. Die Ergebnisse der Kontrollen und Weisungen sind von beiden Vertragsparteien in geeigneter Weise zu protokollieren.

5. Allgemeine Pflichten des Auftragnehmers

5.1. Die Verarbeitung der vertragsgegenständlichen Daten durch den Auftragnehmer erfolgt ausschließlich auf Grundlage der vertraglichen Vereinbarungen in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung ist nur aufgrund zwingender europäischer oder mitgliedsstaatlicher Rechtsvorschriften zulässig (z.B. im Falle von Ermittlungen durch Strafverfolgungs- oder Staatsschutzbehörden). Ist eine Verarbeitung aufgrund zwingenden Rechts erforderlich, teilt der Auftragnehmer dies dem Auftraggeber vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

5.2. Der Auftragnehmer hat bei der Auftragsdurchführung sämtliche gesetzlichen Vorschriften einzuhalten. Er hat insbesondere die nach Art. 32 DSGVO notwendigen technischen und organisatorischen Maßnahmen implementieren und das nach Art. 30 Abs. 2 DSGVO erforderliche Verzeichnis von Verarbeitungstätigkeiten zu führen, soweit dies gesetzlich vorgeschrieben ist.

5.3. Sofern der Auftragnehmer nach der DSGVO oder sonstigen gesetzlichen Vorschriften zur Benennung eines Datenschutzbeauftragten verpflichtet ist, bestätigt er, dass er einen solchen in Einklang mit den gesetzlichen Vorschriften ausgewählt hat und sichert dem Auftraggeber zu, diesen unter Angabe seiner Kontaktdaten zu benennen (z.B. per E-Mail). Änderungen über Person und / oder Kontaktdaten des Datenschutzbeauftragten sind dem Auftraggeber unverzüglich mitzuteilen.

5.4. Der Auftragnehmer hat zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Vor der Unterwerfung unter die Verschwiegenheitspflicht dürfen die betreffenden Personen keinen Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.

5.5. Auf Anfrage stellt der Auftraggeber der betroffenen Person eine Kopie dieses Vertrages, einschließlich der von den Parteien ausgefüllten Anlage, unentgeltlich zur Verfügung. Soweit

es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich der in Anhang II beschriebenen Maßnahmen und personenbezogener Daten, notwendig ist, kann der Auftraggeber Teile des Textes der Anlage zu diesem Vertrag vor der Weitergabe einer Kopie unkenntlich machen; er legt jedoch eine aussagekräftige Zusammenfassung vor, wenn die betroffene Person andernfalls den Inhalt der Anlage nicht verstehen würde oder ihre Rechte nicht ausüben könnte. Auf Anfrage teilen die Parteien der betroffenen Person die Gründe für die Schwärzungen so weit wie möglich mit, ohne die geschwärzten Informationen offenzulegen. Diese Klausel gilt unbeschadet der Pflichten des Auftraggebers gemäß den Artikeln 13 und 14 der DSGVO.

5.6. Der Auftragnehmer wird die Erfüllung seiner Pflichten regelmäßig und selbstständig kontrollieren und in geeigneter Weise dokumentieren.

6. Sensible Daten

Soweit die Übermittlung personenbezogene Daten umfasst, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragnehmer die in Anhang I.A beschriebenen speziellen Beschränkungen und/oder zusätzlichen Garantien an.

7. Technische und organisatorische Maßnahmen

7.1. Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen, um die Sicherheit der Daten zu gewährleisten, einschließlich des Schutzes vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu diesen Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und dem/den Zweck(en) der Verarbeitung sowie den mit der Verarbeitung verbundenen Risiken für die betroffenen Personen gebührend Rechnung. Zur Erfüllung seiner Pflichten gemäß diesem Absatz setzt der Auftragnehmer mindestens die in Anhang II aufgeführten technischen und organisatorischen Maßnahmen um. Der Auftragnehmer führt regelmäßige Kontrollen durch, um sicherzustellen, dass diese Maßnahmen weiterhin ein angemessenes Schutzniveau bieten.

7.2. Der Auftragnehmer gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Er gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.3. Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer gemäß dieses Vertrags ergreift der Auftragnehmer geeignete Maßnahmen zur Behebung der Verletzung, darunter auch Maßnahmen zur Abmilderung ihrer nachteiligen Auswirkungen. Zudem meldet der Auftragnehmer dem Auftraggeber die Verletzung unverzüglich, nachdem sie ihm bekannt wurde. Diese Meldung enthält die Kontaktdaten einer Anlaufstelle für weitere Informationen, eine Beschreibung der Art der Verletzung (soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen personenbezogenen Datensätze), die wahrscheinlichen Folgen der Verletzung und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung etwaiger nachteiliger Auswirkungen. Wenn und

soweit nicht alle Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

7.4. Unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen arbeitet der Auftragnehmer mit dem Auftraggeber zusammen und unterstützt ihn dabei, seinen Pflichten gemäß der DSGVO nachzukommen, insbesondere die zuständige Aufsichtsbehörde und die betroffenen Personen zu benachrichtigen.

8. Unterstützungspflichten des Auftragnehmers

8.1. Der Auftragnehmer wird den Auftraggeber gem. Art. 28 Abs. 3 lit. e DSGVO bei dessen Pflichten zur Wahrung der Betroffenenrechte aus Kapitel III, Art. 12 – 22 DSGVO unterstützen. Dies gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten. Die Reichweite der Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung.

8.2. Der Auftragnehmer wird den Auftraggeber ferner gem. Art. 28 Abs. 3 lit. f DSGVO bei dessen Pflichten nach Art. 32 – 36 DSGVO (insb. Meldepflichten) unterstützen. Die Reichweite dieser Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen.

9. Einsatz von UnterAuftragnehmern (Subunternehmer)

9.1. In Übereinstimmung mit der Regelung des Art. 28 Abs. 2 S. 1 DSGVO nimmt der Auftragnehmer keinen weiteren Auftragnehmer (Unterauftragnehmer, Sub-Unterauftragnehmer) ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Auftraggebers in Anspruch, wobei die Bestimmungen zu Unterauftragsverhältnissen sowohl für den Unterauftragnehmer als auch für sämtliche in der Folge in Anspruch genommenen weiteren (Sub)-Unterauftragnehmer (entsprechende) Anwendung finden.

9.2. Der Auftraggeber stimmt hiermit der Beauftragung der in der unter **Anlage 3** aufgelisteten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2 und 4 DSGVO (gesondert) zu.

9.3. Überdies genehmigt der Auftraggeber hiermit in allgemeiner Weise die Inanspruchnahme weiterer durch den Auftragnehmer. Der Auftragnehmer wird den Auftraggeber über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragnehmer informieren. Dem Auftraggeber steht im Einzelfall ein Recht zu, schriftlich oder in Textform Einspruch gegen die Beauftragung eines potenziellen weiteren Auftragnehmers zu erheben. Ein Einspruch darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund erhoben werden. Soweit der Auftraggeber nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung.

9.4. Eine Beauftragung von Subunternehmern in Drittstaaten erfolgt nur, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

9.5. Der Auftragnehmer stellt sicher, dass der Auftraggeber gegenüber dem Unteraufragnehmer dieselben Weisungsrechte und Kontrollrechte wie gegenüber dem Auftragnehmer nach diesem Vertrag hat. Kommt ein Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Unterauftragnehmers.

9.6. Der Auftragnehmer stellt dem Auftraggeber auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich

personenbezogener Daten, notwendig ist, kann der Auftragnehmer den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

9.7. Der Auftragnehmer haftet gegenüber dem Auftraggeber in vollem Umfang dafür, dass der UnterAuftragnehmer seinen Pflichten gemäß dem mit dem Auftragnehmer geschlossenen Vertrag nachkommt. Der Auftragnehmer benachrichtigt den Auftraggeber, wenn der UnterAuftragnehmer seinen Pflichten gemäß diesem Vertrag nicht nachkommt.

10. Mitteilungspflichten des Auftragnehmers

10.1 Verstöße gegen diesen Vertrag, gegen die Weisungen des Auftraggebers oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen; das gleiche gilt bei Vorliegen eines entsprechenden begründeten Verdachts. Diese Pflicht gilt unabhängig davon, ob der Verstoß vom Auftragnehmer selbst, einer bei ihm angestellten Person, einem UnterAuftragnehmer oder einer sonstigen Person, die er zur Erfüllung seiner vertraglichen Pflichten eingesetzt hat, begangen wurde.

10.2 Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Erfüllung seiner gesetzlichen Informationspflichten nach Art. 33 und 34 DSGVO zu unterstützen. Eigenständige Meldungen an Behörden oder Betroffene nach Art. 33 und 34 DSGVO darf der Auftragnehmer erst nach vorheriger Weisung des Auftraggebers durchführen.

10.3 Ersucht ein Betroffener, eine Behörde oder ein sonstiger Dritter den Auftragnehmer um Auskunft, Berichtigung, Sperrung oder Löschung, wird der Auftragnehmer die Anfrage unverzüglich an den Auftraggeber weiterleiten; in keinem Fall wird der Auftragnehmer dem Ersuchen des Betroffenen ohne Zustimmung des Auftraggebers nachkommen.

10.4 Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn Aufsichtshandlungen oder sonstige Maßnahmen einer Behörde bevorstehen, von der auch die Verarbeitung, Nutzung oder Erhebung der durch den Auftraggeber zur Verfügung gestellten personenbezogenen Daten betroffen sein könnten. Darüber hinaus hat der Auftragnehmer den Auftraggeber unverzüglich über alle Ereignisse oder Maßnahmen Dritter zu informieren, durch die die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.

11. Vertragsbeendigung, Löschung und Rückgabe der Daten

Nach Abschluss der vertragsgegenständlichen Datenverarbeitung bzw. nach Beendigung dieses Vertrags hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers zu löschen oder zurückzugeben, sofern keine gesetzliche Verpflichtung zur Speicherung der betreffenden Daten mehr besteht (z.B. gesetzliche Aufbewahrungsfristen). Der Auftraggeber ist berechtigt, die Maßnahmen des Auftragnehmers in geeigneter Weise zu überprüfen. Hierzu ist er insbesondere berechtigt, die einschlägigen Löschprotokolle und die betroffenen Datenverarbeitungsanlagen vor Ort in Augenschein zu nehmen.

12. Datengeheimnis und Vertraulichkeit

12.1 Der Auftragnehmer ist unbefristet und über das Ende dieses Vertrages hinaus verpflichtet, die im Rahmen der vorliegenden Vertragsbeziehung erlangten personenbezogenen Daten vertraulich zu behandeln und einschlägige Geheimnisschutzregeln, denen der Auftraggeber unterliegt (z.B. § 203 StGB), zu beachten. Der Auftraggeber ist verpflichtet, den Auftragnehmer bei Auftragserteilung auf ggf. bestehende besondere Geheimnisschutzregeln hinzuweisen.

12.2 Der Auftragnehmer verpflichtet sich, seine Mitarbeiter mit den einschlägigen Datenschutzbestimmungen und Geheimnisschutzregeln vertraut zu machen und sie zur Verschwiegenheit zu verpflichten, bevor diese ihre Tätigkeit beim Auftragnehmer aufnehmen.

12.3 Der Auftragnehmer wird die Einhaltung der in dieser Ziffer genannten Maßnahmen in geeigneter Weise dokumentieren. Die Dokumentation ist dem Auftraggeber auf Verlangen vorzulegen

13. Schlussbestimmungen

14.1 Änderungen dieses Vertrags und Nebenabreden bedürfen der schriftlichen oder elektronischen Form, die eindeutig erkennen lässt, dass und welche Änderung oder Ergänzung der vorliegenden Bedingungen durch sie erfolgen soll.

14.2 Sollte sich die DSGVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.

14.3 Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

14.4 Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

Anlage 1 – Auftragsdetails

Der vorliegende Vertrag umfasst (im Zusammenhang mit dem Hauptvertrag) folgende Leistungen:

FALZEDER Consulting erbringt für den Kunden Dienstleistungen zur Erstellung und Verwaltung von Marketingkampagnen und zur Erstellung von Websites und Landing Pages im Rahmen von GoHighLevel. Die Datenverarbeitung umfasst die Erhebung, Speicherung, Organisation, Nutzung und ggf. Löschung von personenbezogenen Daten im Rahmen der Marketing- und Lead-Management-Aktivitäten. Der Zweck der Datenverarbeitung ist die Unterstützung des Kunden bei der Lead-Generierung, Kundenakquise und Kundenbindung sowie die Optimierung von Marketingmaßnahmen und die Durchführung von Analysen zur Steigerung der Kampagneneffizienz.

1. **Art der Leistungen:**
   - 1.1. Kampagnenerstellung und -verwaltung: Erstellen und Verwalten von Marketingkampagnen (z. B. E-Mail- oder SMS-Kampagnen) über GoHighLevel im Auftrag des Kunden.
   - 1.2. Webseitenerstellung und -pflege: Erstellung, Hosting und Pflege von Websites und Landing Pages im Rahmen von GoHighLevel, die personenbezogene Daten erfassen können (z. B. Kontaktformulare, Anmeldeformulare).
   - 1.3. Lead-Management: Verwaltung und Strukturierung von Kundendaten und Leads im CRM-System von GoHighLevel für eine zielgerichtete Kundenansprache.
   - 1.4. Analyse und Reporting: Bereitstellung von Analyseberichten und Berichten zur Kampagnenleistung basierend auf den Daten der Kunden.

2. **Art der Verarbeitung:**
   - 2.1. Erhebung und Speicherung: Erfassen von Kundendaten durch Formulare auf Websites oder im Rahmen von Kampagnen und deren Speicherung im CRM von GoHighLevel.
   - 2.2. Organisation und Strukturierung: Anlegen und Strukturieren von Kontakten und Leads, um die Daten übersichtlich zu verwalten.
   - 2.3. Verwendung und Übermittlung: Nutzung der Daten für gezielte Marketingaktivitäten und ggf. Übermittlung an andere Tools oder Plattformen, sofern in GoHighLevel konfiguriert.
   - 2.4. Löschung und Sperrung: Löschung oder Sperrung der Daten auf Anweisung des Kunden oder nach Ablauf der vertraglichen Laufzeit.

3. **Zweck der Verarbeitung:**
   - 3.1. Lead-Generierung und Kundenakquise: Verarbeitung von Daten zur Erfassung neuer Leads und zur Gewinnung von Kunden für den Kunden.
   - 3.2. Marketing und Kundenbindung: Personalisierung und Durchführung von Kampagnen, um die Kundenbindung zu fördern und die Zielgruppe des Kunden gezielt anzusprechen.
   - 3.3. Optimierung von Kampagnen und Geschäftsanalyse: Durchführung von Analysen und Optimierungen der Kampagnen, um die Effizienz und Wirksamkeit der Marketingmaßnahmen des Kunden zu verbessern.

Im Rahmen der vertraglichen Leistungserbringung werden einmalig oder regelmäßig folgende Datenarten verarbeitet:

1. Kontaktdaten

- Name (Vor- und Nachname): zur Identifizierung des Kontakts.
- E-Mail-Adresse: für E-Mail-Marketing und direkte Kommunikation.
- Telefonnummer: für SMS-Marketing und telefonische Kontaktaufnahme.
- Postadresse (wenn vorhanden): für gezielte Marketingmaßnahmen per Post oder zur Segmentierung nach Regionen.

2. Unternehmensbezogene Informationen

- Firmenname und Position im Unternehmen: wenn Leads oder Kunden B2B-Kontakte sind.
- Branche und Unternehmensgröße: um die Zielgruppe spezifischer anzusprechen oder Kampagnen auf eine bestimmte Kundengruppe abzustimmen.

3. Interaktionsdaten

- Öffnungs- und Klickraten: bei E-Mail- und SMS-Kampagnen, um das Engagement und Interesse des Kontakts zu messen.
- Webseiten- und Landing Page-Besuche: Seitenaufrufe und Aufenthaltsdauer, die im Rahmen von Webanalyse-Tools innerhalb von GoHighLevel erfasst werden.
- Formulareinreichungen: Daten, die über Formulare auf Webseiten und Landing Pages übermittelt werden (z. B. Anfragen, Anmeldungen).

4. Kommunikationsdaten

- Nachrichtenverlauf: SMS- und E-Mail-Kommunikation, die zwischen deinem Kunden und seinen Leads/Kontakten stattgefunden hat. Dieser Verlauf wird gespeichert, um die Kundenhistorie nachvollziehen zu können und gezielte Nachverfolgungen zu ermöglichen.
- Chatverläufe: Falls der Chat- oder Helpdesk-Bereich von GoHighLevel verwendet wird, werden auch dortige Anfragen und Antworten dokumentiert.

5. Kampagnenbezogene Daten

- Kampagneninteraktionen und -ergebnisse: Informationen zu Aktionen, die ein Kontakt in einer Kampagne ausgeführt hat (z. B. Klick auf einen CTA, Anmeldungen zu Webinaren).
- Zuordnungen zu Segmenten und Tags: Einordnung der Kontakte in Segmente oder Kennzeichnung durch Tags, um gezielte Zielgruppenansprache zu ermöglichen.

6. Geräte- und Tracking-Daten

- IP-Adresse und Standortdaten (wenn zugänglich): Dies wird oft für regionale Segmentierungen oder für die Zielgruppenanalyse genutzt.
- Geräteinformationen und Browserdaten: um herauszufinden, welche Geräte und Browser genutzt werden. Diese Informationen werden für die technische Optimierung und die Segmentierung verwendet.
- Cookies und Pixel-Daten: falls Tracking für Retargeting-Kampagnen eingerichtet ist, können Daten wie Seitenbesuche und spezifische Klicks innerhalb von Websites oder Landing Pages erfasst werden.

7. Zahlungs- und Rechnungsdaten

Bei dem Kreis der von der Datenverarbeitung betroffenen Personen handelt es sich um:

- Leads und Interessenten
- Kunden
- Newsletter-Abonnenten
- Website-Besucher (wenn Tracking und Retargeting aktiviert sind)
- Event-Teilnehmer und Webinar-Besucher
- Kundensupport-Anfragende

Anlage 2 – Liste der bestehenden technischen und organisatorischen Maßnahmen des Auftragnehmers nach Art. 32 DSGVO

Der Auftragnehmer setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DSGVO festgelegt und mit dem Auftraggeber abgestimmt.

I. Zweckbindung und Trennbarkeit

Folgende Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

x physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern

x Logische Mandantentrennung (softwareseitig)

x Berechtigungskonzept

☐ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden

x Versehen der Datensätze mit Zweckattributen / Datenfeldern / Signaturen

☐ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten und abgesicherten IT-System

☐ Trennung von Produktiv- und Testsystem

☐ Sonstige:

II. Vertraulichkeit und Integrität

Folgende Maßnahmen gewährleisten die Vertraulichkeit und Integrität der Systeme des Auftragnehmers:

1. Verschlüsselung

Die im Auftrag verarbeiteten Daten bzw. Datenträger werden in folgender Weise verschlüsselt:

Datenübertragung: Die Verbindung zu GoHighLevel erfolgt verschlüsselt über HTTPS (SSL/TLS), wodurch die Daten gegen Abfangen und Manipulation während der Übertragung geschützt werden.

Daten in Ruhe: GoHighLevel speichert die Daten auch verschlüsselt, wenn sie auf den Servern ruhen, um zusätzliche Sicherheit gegen unbefugten Zugriff zu bieten.

2. Pseudonymisierung

„Pseudonymisierung“ bedeutet, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine Identifizierung der betroffenen Person ohne Hinzuziehung weiterer Informationen ausschließt (z.B. Verwendung von Fantasienamen, die ohne zusätzliche Informationen keiner bestimmten Person zugeordnet werden können).

x Nein

☐ Ja, und zwar in folgender Art und Weise:

3. Es wurden folgende Maßnahmen getroffen, um Unbefugte am Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu hindern (Zutrittskontrolle):

☐ Alarmanlage

☐ Absicherung von Gebäudeschächten

☐ Automatisches Zugangskontrollsystem

☐ Chipkarten-/Transponder-Schließsystem

☐ Schließsystem mit Codesperre

x Manuelles Schließsystem

☐ Biometrische Zugangssperren

☐ Videoüberwachung der Zugänge

☐ Lichtschranken / Bewegungsmelder

☐ Sicherheitsschlösser

☐ Schlüsselregelung (Schlüsselausgabe etc.)

☐ Personenkontrolle beim Pförtner / Empfang

☐ Protokollierung der Besucher

☐ Sorgfältige Auswahl von Reinigungspersonal

☐ Sorgfältige Auswahl von Wachpersonal

☐ Tragepflicht von Berechtigungsausweisen

☐ Zutrittskonzept / Besucherregelung

☐ Sonstige:

4. Es wurden folgende Maßnahmen getroffen, die die Nutzung der Datensysteme durch unbefugte Dritte verhindern (Zugangskontrolle):

x Zuordnung von Benutzerrechten

x Erstellen von Benutzerprofilen

x Passwortvergabe

x Passwort-Richtlinien (regelmäßige Änderung, Mindestlänge, Komplexität etc.)

☐ Authentifikation mit biometrischen Verfahren

x Authentifikation mit Benutzername / Passwort

☐ Zuordnung von Benutzerprofilen zu IT-Systemen

☐ Gehäuseverriegelungen

☐ Einsatz von VPN-Technologie bei der Übertragung von Daten

☐ Verschlüsselung mobiler IT-Systeme

☐ Verschlüsselung mobiler Datenträger

☐ Verschlüsselung der Datensicherungssysteme

☐ Sperren externer Schnittstellen (USB etc.)

☐ Einsatz von Intrusion-Detection-Systemen

☐ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)

☐ Einsatz von Anti-Viren-Software

☐ Verschlüsselung von Datenträgern in Laptops / Notebooks

☐ Einsatz einer Hardware-Firewall

x Einsatz einer Software-Firewall

☐ Sonstige:

5. Es wurden folgende Maßnahmen getroffen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle):

x Berechtigungskonzept

x Verwaltung der Rechte durch Systemadministrator

x regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte (insb. bei Ausscheiden von Mitarbeitern o.Ä.)

x Anzahl der Administratoren ist auf das „Notwendigste“ reduziert

x Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel

☐ Sichere Aufbewahrung von Datenträgern

☐ physische Löschung von Datenträgern vor Wiederverwendung

☐ ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)

☐ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)

☐ Protokollierung der Vernichtung

☐ Verschlüsselung von Datenträgern

☐ Sonstige:

6. Mit Hilfe folgender Maßnahmen kann nachträglich überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle).

x Protokollierung der Eingabe, Änderung und Löschung von Daten

☐ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.

x Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

x Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

☐ Sonstige:

7. Folgende Maßnahmen gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle).

x Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)

x vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen

x schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag)

x Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis

x Auftragnehmer hat Datenschutzbeauftragten bestellt

x Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

x Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart

x laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

x Vertragsstrafen bei Verstößen

☐ Sonstige:

8. Folgende Maßnahmen gewährleisten, dass personenbezogene Daten bei der Weitergabe (physisch und / oder digital) nicht von Unbefugten erlangt oder zur Kenntnis genommen werden können (Transport- bzw. Weitergabekontrolle):

☐ Einsatz von VPN-Tunneln

☐ Verschlüsselung der Kommunikationswege (z.B. Verschlüsselung des E- Mail-Verkehrs)

☐ Verschlüsselung physischer Datenträger bei Transport

☐ Sonstige:

III. Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit der Systeme

Folgende Maßnahmen gewährleisten, dass die eingesetzten Datenverarbeitungssysteme jederzeit einwandfrei funktionieren und personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind

☐ Unterbrechungsfreie Stromversorgung (USV)

☐ Klimatisierung der Serverräume

☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen

☐ Schutzsteckdosenleisten in Serverräumen

☐ Feuer- und Rauchmeldeanlagen in Serverräumen

☐ Feuerlöschgeräte in Serverräumen

☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen

☐ Erstellen eines Backup- & Recoverykonzepts

☐ Testen von Datenwiederherstellung

☐ Erstellen eines Notfallplans

☐ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

☐ Serverräume nicht unter sanitären Anlagen

☐ In Hochwassergebieten: Serverräume über der Wassergrenze

☐ belastbares Datensicherungs- und Widerherstellungskonzept vorhanden

☐ Sonstige:

IV. Besondere Datenschutzmaßnahmen Es liegen schriftlich vor:

☐ interne Verhaltensregeln

☐ Risikoanalyse

☐ Datenschutz-Folgenabschätzung

☐ Datensicherheitskonzept

☐ Wiederanlaufkonzept

☐ Zertifikat:

☐ Sonstiges

V. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen

Der Auftragnehmer wird die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen im Abstand von 12 Monaten und anlassbezogen, prüfen, evaluieren und bei Bedarf anpassen.

Anlage 3 – Liste der bestehenden Subunternehmer zum Zeitpunkt des Vertragsschlusses

(Unternehmens-) Name und Anschrift	**Beschreibung der Leistung**	**Ort der Leistungserbringung und Name, Funktion und Kontaktdaten einer Kontaktperson**