# Vertrag zur Auftragsverarbeitung

Dieser Auftragsverarbeitungsvertrag („AVV“) wird geschlossen zwischen:

dem jeweiligen Kunden, der die Dienstleistungen der Plattform Demandly nutzt
(im Folgenden „Auftraggeber“ oder „Verantwortlicher“)

und

Demandly (eine Marke von elevatemark)
Kirchstr. 22C
77736 Zell a.H.

(im Folgenden „Auftragnehmer“ oder „Auftragsverarbeiter“)

– gemeinsam auch „Vertragsparteien“ genannt –

## 1. Allgemeine Bestimmungen und Auftragsgegenstand

1.1. Mit diesem Vertrag wollen wir sicherstellen, 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 dafür verantwortlich, zu beurteilen, ob die Datenverarbeitungsvorgänge nach Art. 6 DSGVO zulässig sind, und die Betroffenenrechte zu wahren.

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

1.3. Dieser Vertrag enthält alle wichtigen Garantien und durchsetzbaren Rechte für die betroffenen Personen. Außerdem gibt es wirksame Rechtsbehelfe, wie in Artikel 46 Absatz 1 und Artikel 46 Absatz 2 Buchstabe c der DSGVO festgelegt.

1.4. Dieser Vertrag gilt natürlich trotzdem, auch wenn der Auftraggeber bestimmte Verpflichtungen gemäß der DSGVO hat.

1.5. Hier mal eine kurze Übersicht über die Datenübermittlung: Welche Daten werden genau übermittelt? Und zu welchem Zweck? Das steht alles in Anhang 1.

1.6. Der Auftraggeber versichert, sich im Rahmen des Möglichen 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 Daten werden ausschließlich in Deutschland, einem EU-Land oder einem Land des Europäischen Wirtschaftsraums verarbeitet. Die Daten werden nur in Ländern außerhalb der EU verarbeitet, wenn die DSGVO das erlaubt (Kapitel 5, Artikel 44 ff.). Außerdem muss der Auftraggeber vorher zustimmen.

1.8. Die Vergütung wird außerhalb dieses Vertrags vereinbart.

## 2. Vertragslaufzeit und Kündigung

Dieser Auftragsverarbeitungsvertrag gilt für die Dauer der Nutzung der Dienste von Demandly.
Er endet automatisch mit Beendigung des Hauptvertrages über die Nutzung der Plattform.

## 3. Weisungen des Auftraggebers

3.1. Als Auftraggeber kannst du dem Auftragnehmer sagen, was er mit deinen Daten machen soll. Du kannst zum Beispiel verlangen, dass er sie löscht, berichtigt, sperrt oder herausgibt. Der Auftragnehmer muss deinen Anweisungen folgen, solange sie nicht gegen Verträge oder Gesetze verstoßen.

3.2. Wenn der Auftragnehmer der Meinung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt, muss er den Auftraggeber sofort darüber informieren. Wenn eine Weisung erteilt wird, die der Auftragnehmer für nicht rechtmäßig hält, kann er deren Ausführung vorübergehend aussetzen, bis der Auftraggeber sie bestätigt oder ändert.

3.3. Grundsätzlich gilt: Weisungen müssen schriftlich oder in einem elektronischen Format (z. B. per E-Mail) erteilt werden. Wenn der Auftragnehmer eine schriftliche Bestätigung möchte, soll der Auftraggeber das auf Anfrage tun. Der Auftragnehmer sollte die mündliche Weisung

in einem Protokoll festhalten, das Datum, Uhrzeit und Namen der beteiligten Personen enthält.

3.4. Wenn der Auftraggeber will, kann er auf Anfrage des Auftragnehmers eine oder mehrere weisungsberechtigte Personen benennen. Bitte sag uns sofort Bescheid, wenn sich etwas ändert.

## 4. Kontrollbefugnisse des Auftraggebers

4.1. Der Auftraggeber kann regelmäßig im erforderlichen Umfang kontrollieren, ob die gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit eingehalten werden. Dazu kann er auch Dritte beauftragen. Der Auftragnehmer muss diese Kontrollen dulden und im erforderlichen Maße unterstützen. Er muss dem Auftraggeber alle Infos geben, die für die Kontrollen wichtig sind, und zwar vollständig und wahrheitsgemäß. Er muss ihm auch die gespeicherten Daten und Programme/Systeme zeigen und Vor-Ort-Kontrollen ermöglichen. Wenn der Auftraggeber der Verarbeitung der Daten außerhalb der Geschäftsräume (z. B. Privatwohnung) zugestimmt hat, muss der Auftragnehmer dafür sorgen, dass der Auftraggeber auch diese Räume zu Kontrollzwecken begehen darf.

4.2. Der Auftraggeber muss dafür sorgen, dass die Kontrollmaßnahmen angemessen sind und den Betrieb des Auftragnehmers nicht zu stark beeinträchtigen. Vor-Ort-Kontrollen sollten grundsätzlich zu den üblichen Geschäftszeiten und nach Terminvereinbarung mit angemessener Vorlaufzeit erfolgen, sofern der Kontrollzweck einer vorherigen Ankündigung nicht widerspricht.

4.3. Die Ergebnisse der Kontrollen und Weisungen sollten von beiden Vertragsparteien in einem Protokoll festgehalten werden.

## 5. Allgemeine Pflichten des Auftragnehmers

5.1. Die Daten, die wir vertragsgemäß verarbeiten, werden ausschließlich auf Grundlage der Vereinbarungen im Vertrag und der Weisungen des Auftraggebers verarbeitet. Eine andere Verarbeitung ist nur erlaubt, wenn es zwingende europäische oder nationale Rechtsvorschriften vorschreiben (z. B. wenn die Polizei oder der Staatsschutz ermitteln). Wenn eine Verarbeitung aufgrund zwingender Rechtsvorschriften erforderlich ist, sagt der Auftragnehmer dem Auftraggeber Bescheid, bevor er damit anfängt. Das gilt allerdings nur, wenn das betreffende Recht keine solche Mitteilung verbietet, weil es ein wichtiges öffentliches Interesse gibt.

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

5.3. Wenn 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. Er versichert dem Auftraggeber außerdem, dass er diesen unter Angabe seiner Kontaktdaten nennen wird (z. B. per E-Mail). Änderungen über Person und/oder Kontaktdaten des Datenschutzbeauftragten sind dem Auftraggeber unverzüglich mitzuteilen.

5.4. Die Datenverarbeitung außerhalb der Betriebsstätten des Auftragnehmers oder der Subunternehmer und/oder in Privatwohnungen (z. B. Fernzugriff oder Homeoffice des Auftragnehmers) ist nur mit ausdrücklicher Zustimmung des Auftraggebers gestattet.

5.5. Der Auftragnehmer muss sicherstellen, dass alle Personen, die mit den personenbezogenen Daten arbeiten, eine Verschwiegenheitspflicht haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Vor der Unterzeichnung der Verschwiegenheitspflicht dürfen die betreffenden Personen keinen Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.

5.6. Auf Anfrage stellt der Auftraggeber der betroffenen Person eine Kopie dieses Vertrages, einschließlich der von den Parteien ausgefüllten Anlage, unentgeltlich zur Verfügung. Wenn 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 dann aber eine aussagekräftige Zusammenfassung vor, damit die betroffene Person den Inhalt der Anlage verstehen kann und ihre Rechte ausüben kann. Wenn die betroffene Person nachfragt, erklären die Parteien ihr, warum sie bestimmte Informationen geschwärzt haben. Sie geben ihr aber keine Informationen preis, die geschwärzt wurden.. Diese Klausel gilt unbeschadet der Pflichten des Auftraggebers gemäß den Artikeln 13 und 14 der DSGVO.

5.7. 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 sorgt dafür, dass die Daten sicher sind. Er schützt sie vor unbeabsichtigten oder unrechtmäßigen Verletzungen der Datensicherheit. Dazu zählt auch, dass er dafür sorgt, dass die Daten nicht verloren gehen, verändert werden oder von Unbefugten eingesehen werden können. Die Parteien schauen sich an, was für einen angemessenen Schutz nötig ist. Dabei berücksichtigen sie den Stand der Technik, die Kosten für die Umsetzung, die Art, den Umfang, die Umstände und den Zweck der Verarbeitung sowie die Risiken für die betroffenen Personen. Damit der Auftragnehmer seinen Pflichten aus diesem Absatz nachkommen kann, setzt er mindestens die in Anhang II aufgeführten technischen und organisatorischen Maßnahmen um. Der Auftragnehmer überprüft regelmäßig, ob die Maßnahmen noch angemessen sind.

7.2. Der Auftragnehmer gibt seinem Personal nur Zugriff auf die Daten, die sie für die Durchführung, Verwaltung und Überwachung des Vertrags brauchen. Außerdem stellt er sicher, dass alle, die mit den Daten arbeiten, sich zur Verschwiegenheit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.3. Wenn beim Auftragnehmer Daten von Personen, mit denen er zu tun hat, nicht richtig geschützt werden, dann muss er dafür sorgen, dass das schnellstmöglich wieder in Ordnung kommt. Er muss auch dafür sorgen, dass die Folgen der Verletzung möglichst gering bleiben.

Außerdem muss er den Auftraggeber über den Vorfall informieren, sobald er davon erfährt. In der Meldung stehen die Kontaktdaten einer Anlaufstelle für weitere Infos, 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 wir nicht alle Informationen sofort bereitstellen können, enthalten die Meldung zunächst alle Informationen, die wir haben. Sobald wir weitere Infos haben, stellen wir sie ohne Verzögerung zur Verfügung.

7.4. Der Auftragnehmer arbeitet mit dem Auftraggeber zusammen, um sicherzustellen, dass alle Vorgaben der DSGVO eingehalten werden. Dazu gehört auch, die zuständige Aufsichtsbehörde und die betroffenen Personen zu benachrichtigen.

## 8. Unterstützungspflichten des Auftragnehmers

8.1. Der Auftragnehmer unterstützt den Auftraggeber bei dessen Pflichten zur Wahrung der Betroffenenrechte aus Kapitel III, Art. 12 – 22 DSGVO. Das 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 unterstützt den Auftraggeber außerdem bei dessen Pflichten nach Art. 32 – 36 DSGVO (insbesondere Meldepflichten). Wie weit diese Unterstützungspflicht geht, hängt davon ab, wie die Daten verarbeitet werden und welche Informationen dem Auftragnehmer zur Verfügung stehen.

## 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. Die Bestimmungen zu Unterauftragsverhältnissen gelten dabei sowohl für den Unterauftragnehmer als auch für sämtliche in der Folge in Anspruch genommenen weiteren (Sub)-Unterauftragnehmer.

9.2. Hiermit bestätigt der Auftraggeber die Beauftragung der in Anlage 3 aufgeführten Unterauftragnehmer. Die Beauftragung erfolgt unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2 und 4 DSGVO, die separat abgeschlossen wird.

9.3. Außerdem darf der Auftragnehmer weitere Leute hinzuziehen oder austauschen, wenn der Auftraggeber damit einverstanden ist. Der Auftragnehmer sagt dem Auftraggeber Bescheid, wenn er andere Leute mit ins Boot holen will. Wenn der Auftraggeber nicht will, dass ein weiterer Auftragnehmer mitmacht, kann er das dem Auftragnehmer schriftlich oder in Textform mitteilen.

9.4. Wenn der Auftraggeber Einspruch einlegen will, muss er das aus wichtigem Grund tun und dem Auftragnehmer nachweisen. Wenn der Auftraggeber nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, gilt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung als erloschen.

9.5. Wenn wir Subunternehmer in Drittstaaten beauftragen, müssen wir uns an die besonderen Voraussetzungen der Art. 44 ff. halten. Die DSGVO muss natürlich auch erfüllt sein.

9.6. Der Auftragnehmer sorgt dafür, dass der Auftraggeber gegenüber dem Unterauftragnehmer dieselben Anordnungsrechte und Kontrollrechte hat wie gegenüber dem Auftragnehmer. Falls ein Unterauftragnehmer seine Pflichten im Bereich Datenschutz nicht erfüllt, ist der Auftragnehmer gegenüber dem Auftraggeber dafür verantwortlich, dass der Unterauftragnehmer diese Pflichten einhält.

9.7. Wenn der Auftraggeber eine Kopie der Untervergabevereinbarung und etwaiger späterer Änderungen haben möchte, bekommt er die natürlich. Falls 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.

9.8. Der Auftragnehmer ist dafür verantwortlich, dass der Unterauftragnehmer seinen Pflichten gemäß dem Vertrag mit dem Auftragnehmer nachkommt. Wenn der Unterauftragnehmer seinen Pflichten nicht nachkommt, muss der Auftragnehmer den Auftraggeber darüber informieren.

**10. Mitteilungspflichten des Auftragnehmers**

10.1 Wenn es zu Verstößen gegen diesen Vertrag, gegen die Weisungen des Auftraggebers oder gegen sonstige datenschutzrechtliche Bestimmungen kommt, muss der Auftraggeber sofort informiert werden. Das gilt auch, wenn ein begründeter Verdacht besteht. Diese Pflicht gilt für den Auftragnehmer selbst, für eine bei ihm angestellte Person, für einen Unterauftragnehmer oder für eine sonstige Person, die er zur Erfüllung seiner vertraglichen Pflichten eingesetzt hat.

10.2 Als Auftragnehmer sind wir verpflichtet, unseren Auftraggeber bei der Erfüllung seiner gesetzlichen Informationspflichten nach Art. 33 und 34 DSGVO zu unterstützen. Meldungen an Behörden oder Betroffene nach Art. 33 und 34 DSGVO dürfen wir erst nach vorheriger Weisung des Auftraggebers durchführen.

10.3 Wenn ein Betroffener, eine Behörde oder ein sonstiger Dritter den Auftragnehmer um Auskunft, Berichtigung, Sperrung oder Löschung bittet, wird der Auftragnehmer die Anfrage sofort an den Auftraggeber weiterleiten. Wir werden dem Ersuchen des Betroffenen aber nur nachkommen, wenn der Auftraggeber damit einverstanden ist.

10.4 Wenn eine Behörde plant, Aufsichtshandlungen oder sonstige Maßnahmen durchzuführen, die auch die Verarbeitung, Nutzung oder Erhebung von Daten durch den Auftraggeber betreffen könnten, muss der Auftragnehmer den Auftraggeber darüber informieren. Außerdem muss der Auftragnehmer den Auftraggeber sofort über alle Ereignisse oder Maßnahmen Dritter informieren, durch die die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.

**11. Vertragsbeendigung, Löschung und Rückgabe der Daten**

Wenn die Datenverarbeitung abgeschlossen ist oder der Vertrag endet, muss der Auftragnehmer alle personenbezogenen Daten löschen oder zurückgeben. Das gilt, solange keine gesetzliche Pflicht zur Speicherung der Daten mehr besteht (z. B. gesetzliche Aufbewahrungsfristen). Der Auftraggeber kann die Maßnahmen des Auftragnehmers überprüfen, wenn er das möchte. Er kann sich auch die Löschprotokolle und die Datenverarbeitungsanlagen vor Ort ansehen.

**12. Datengeheimnis und Vertraulichkeit**

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

12.2 Der Auftragnehmer sorgt dafür, dass seine Mitarbeiter die Datenschutzbestimmungen und Geheimnisschutzregeln kennen und sich daranhalten. Das gilt vor allem, wenn sie ihre Arbeit beim Auftragnehmer aufnehmen.

12.3 Der Auftragnehmer hält sich an alles, was in dieser Ziffer steht, und dokumentiert das auch. Wenn du willst, kannst du dir die Dokumentation natürlich jederzeit ansehen.

**13. Haftung**

13.1 Wenn eine Partei gegen diese Regeln verstößt, muss sie der/den anderen Partei/en den Schaden ersetzen, den sie dadurch verursacht hat/haben.

13.2 Wenn der Auftragnehmer oder sein Unterauftragnehmer gegen diese Regeln verstößt, kann die betroffene Person Schadenersatz verlangen. Das gilt für materielle und immaterielle Schäden, die durch den Verstoß entstanden sind.

13.3 Unabhängig von Nummer 13.2 haftet der Auftragnehmer gegenüber der betroffenen Person. Die betroffene Person hat Anspruch auf Schadenersatz für jeden materiellen oder immateriellen Schaden, den der Auftraggeber oder der Auftragnehmer (oder dessen Unterauftragnehmer) der betroffenen Person zufügt, indem er deren Rechte als Drittbegünstigte gemäß diesen Klauseln verletzt. Das gilt aber trotzdem, auch wenn der Auftraggeber dafür verantwortlich ist. Und wenn der Auftraggeber ein Auftragnehmer ist, der im Auftrag eines Verantwortlichen arbeitet, gilt das auch für den Verantwortlichen. Das steht in der Verordnung (EU) 2016/679 oder gegebenenfalls in der Verordnung (EU) 2018/1725.

13.4 Die Parteien sind sich einig, dass der Auftraggeber, der nach Nummer 13.3 für Schäden haftet, die durch den Auftragnehmer oder dessen Unterauftragnehmer verursacht wurden, berechtigt ist, einen Teil des Schadenersatzes vom Auftragnehmer zurückzufordern. Dieser Teil entspricht der Verantwortung des Auftragnehmers für den Schaden.

13.5 Wenn mehrere Parteien für Schäden verantwortlich sind, die einer Person durch einen Verstoß gegen diese Klauseln entstanden sind, dann haften alle Parteien gesamtschuldnerisch. Die betroffene Person kann dann gegen jede der Parteien gerichtlich vorgehen.

13.6 Die Parteien sind sich einig, dass eine Partei, die nach Nummer 13.5 haftbar gemacht wird, das Recht hat, von der/den anderen Partei(en) den Teil des Schadenersatzes zurückzufordern, der deren Verantwortung für den Schaden entspricht.

13.7 Der Auftragnehmer kann sich nicht rausreden, indem er sagt, dass der Unterauftragnehmer einen Fehler gemacht hat. Er muss selbst für seine Fehler gerade stehen.

**14. Schlussbestimmungen**

14.1 Wenn sich was an diesem Vertrag ändert oder wenn es Nebenabreden gibt, dann muss das schriftlich oder elektronisch festgehalten werden. Dabei muss klar sein, was geändert oder ergänzt werden soll.

14.2 Wenn sich die DSGVO oder andere gesetzliche Regelungen während der Vertragslaufzeit ändern, gelten die Verweise hier auch für die jeweiligen Nachfolgeregelungen.

14.3 Wenn einzelne Teile dieser Vereinbarung nicht gelten oder nicht mehr gelten, bleibt die Wirksamkeit der übrigen Bestimmungen davon unberührt.

14.4 Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

## Anlage 1 – Auftragsdetails

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

Bereitstellung einer cloudbasierten White-Label-SaaS-Plattform für Agenturen und Dienstleister zur Erstellung, Verwaltung und Nutzung von KI-gestützten Chat- und Telefonagenten unter eigener Marke.

Hierzu gehören insbesondere:

- Bereitstellung und Hosting der Plattform
- Verwaltung von Benutzerkonten und Kundenkonten
- Einrichtung, Konfiguration und Betrieb von KI-Chatagenten
- Einrichtung, Konfiguration und Betrieb von KI-Telefonagenten
- Verarbeitung von Chatnachrichten, Spracheingaben und Gesprächsinhalten
- Automatisierte Kundenkommunikation
- Lead-Qualifizierung und Weiterleitung von Anfragen
- Terminbuchung und Terminverwaltung
- CRM- und Kommunikationsintegrationen
- Protokollierung, Administration, Fehleranalyse und Systemsicherheit

Art der Verarbeitung:
Erheben, Erfassen, Organisieren, Speichern, Anpassen, Auslesen, Verwenden, Übermitteln, Bereitstellen, Abgleichen, Einschränken, Löschen und gegebenenfalls Archivieren personenbezogener Daten im Rahmen der Nutzung der Plattform.

Zweck der Verarbeitung:
Die Verarbeitung personenbezogener Daten erfolgt ausschließlich zum Zweck der Bereitstellung, Durchführung und technischen Unterstützung der vertraglich geschuldeten Leistungen des Auftragsverarbeiters, insbesondere zum Betrieb von KI-gestützten Chat- und Telefonagenten, zur Automatisierung von Kommunikationsprozessen, zur Bearbeitung von Kundenanfragen, zur Lead-Qualifizierung, zur Terminvereinbarung sowie zur Bereitstellung damit verbundener CRM- und Kommunikationsfunktionen.

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

- Stammdaten (z. B. Vorname, Nachname)
- Kontaktdaten (z. B. E-Mail-Adresse, Telefonnummer, Anschrift)
- Unternehmensdaten (z. B. Firmenname, Position, Branche)
- Kommunikationsdaten (z. B. Chatnachrichten, E-Mails, Gesprächsinhalte, Sprachaufzeichnungen, Gesprächstranskripte)
- Termin- und Buchungsdaten (z. B. gebuchte Termine, Terminzeiten, Kalenderinformationen)
- Nutzungs- und Interaktionsdaten (z. B. Nutzung der Plattform, Interaktionen mit Chat- oder Telefonagenten)
- CRM-Daten und Kundendaten (z. B. Leads, Kundenanfragen, Gesprächsnotizen, Statusinformationen)
- technische Daten (z. B. IP-Adresse, Geräteinformationen, Browserinformationen, Logfiles)
- Metadaten der Kommunikation (z. B. Zeitpunkt von Nachrichten oder Anrufen, Dauer von Gesprächen, Routinginformationen)

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

- Kunden und Endkunden des Auftraggebers
- Interessenten und Leads des Auftraggebers
- Nutzer von Chat- und Telefonagenten des Auftraggebers
- Mitarbeiter und sonstige Beschäftigte des Auftraggebers
- Geschäftspartner, Lieferanten und Dienstleister des Auftraggebers
- Ansprechpartner bei Kunden oder Geschäftspartnern des Auftraggebers
- sonstige Personen, die über Kommunikationskanäle (z. B. Chat, Telefon, E-Mail, Formulare oder Terminbuchung) mit dem Auftraggeber in Kontakt treten

## 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:

☐ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern

☑ Logische Mandantentrennung (softwareseitig)

☑ Berechtigungskonzept

☑ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden

☑ 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: Verschlüsselte Datenübertragung (TLS/HTTPS), rollenbasierte Zugriffskontrolle sowie Zugriffsbeschränkungen innerhalb der Plattform

### 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:

Die Übertragung personenbezogener Daten erfolgt ausschließlich über verschlüsselte Verbindungen mittels TLS/SSL (HTTPS). Dadurch wird sichergestellt, dass Daten während der Übertragung zwischen Endgerät, Servern und eingesetzten Diensten vor unbefugtem Zugriff geschützt sind.

Gespeicherte Daten werden auf den eingesetzten Server- und Cloud-Systemen durch Verschlüsselungsmechanismen der jeweiligen Infrastrukturanbieter geschützt (z. B. Verschlüsselung ruhender Daten / „Encryption at Rest“). Darüber hinaus werden sensible Zugangsdaten und Authentifizierungsinformationen durch geeignete kryptografische Verfahren (z. B. Hashing und sichere Authentifizierungsverfahren) geschützt.

Der Zugriff auf verschlüsselte Daten ist ausschließlich autorisierten Systemkomponenten und berechtigten Personen im Rahmen eines rollenbasierten Zugriffskonzepts möglich.

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).

☑ Nein.

Die im Rahmen der Plattform verarbeiteten personenbezogenen Daten werden grundsätzlich nicht pseudonymisiert, da die Verarbeitung der Daten im Auftrag des Auftraggebers zur direkten Kommunikation mit Kunden, Interessenten oder sonstigen Kontaktpersonen erforderlich ist (z. B. im Rahmen von Chat-, Telefon- oder CRM-Funktionen).

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
☑ 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: Physische Zutrittskontrollen der Rechenzentren durch den jeweiligen Cloud-/Hosting-Anbieter (z. B. Zugangskontrollen, Sicherheitszonen, Videoüberwachung, autorisierte Zugangssysteme).

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

☑ Zuordnung von Benutzerrechten
☑ Erstellen von Benutzerprofilen
☑ Passwortvergabe
☑ Passwort-Richtlinien (z. B. Mindestlänge, Komplexität)
☐ Authentifikation mit biometrischen Verfahren
☑ 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
☑ Einsatz von Anti-Viren-Software
☑ Verschlüsselung von Datenträgern in Laptops / Notebooks
☑ Einsatz einer Hardware-Firewall
☑ Einsatz einer Software-Firewall

☑ Sonstige: Zugriffsbeschränkung durch rollenbasiertes Berechtigungskonzept, verschlüsselte Datenübertragung (TLS/HTTPS) sowie Zugriffsschutz auf Cloud-Infrastruktur durch Sicherheitsmechanismen des Hosting-Anbieters.

5. Zugriffskontrolle

Es wurden folgende Maßnahmen getroffen:

☑ Berechtigungskonzept
☑ Verwaltung der Rechte durch Systemadministrator
☑ regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte
☑ Anzahl der Administratoren ist auf das notwendige Minimum reduziert
☑ Passwortrichtlinie inkl. Mindestlänge und Komplexität
☐ Sichere Aufbewahrung von Datenträgern
☐ physische Löschung von Datenträgern vor Wiederverwendung
☐ ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
☐ Einsatz von Aktenvernichtern bzw. Dienstleistern
☐ Protokollierung der Vernichtung
☑ Verschlüsselung von Datenträgern
☑ Sonstige: Rollenbasierte Zugriffskontrolle innerhalb der Plattform sowie Zugriffsbeschränkung auf Cloud-Infrastruktur und Systeme nur für autorisierte Administratoren.

6. Eingabekontrolle

☑ 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
☑ Nachvollziehbarkeit durch individuelle Benutzernamen
☐ Aufbewahrung von Formularen
☑ Vergabe von Rechten zur Eingabe, Änderung und Löschung auf Basis eines Berechtigungskonzepts
☑ Sonstige: Systemprotokolle und Logfiles zur Nachverfolgung von Systemzugriffen und Änderungen.

7. Auftragskontrolle

☑ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
☑ vorherige Prüfung und Dokumentation der Sicherheitsmaßnahmen
☑ schriftliche Weisungen an den Auftragnehmer (AVV)
☑ Verpflichtung der Mitarbeiter auf das Datengeheimnis
☐ Auftragnehmer hat Datenschutzbeauftragten bestellt
☑ Sicherstellung der Löschung von Daten nach Beendigung des Auftrags
☑ Kontrollrechte gegenüber dem Auftragnehmer vereinbart
☑ laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
☐ Vertragsstrafen bei Verstößen
☑ Sonstige: Einsatz ausschließlich vertraglich gebundener Unterauftragsverarbeiter gemäß Art. 28 DSGVO.

8. Weitergabekontrolle

☐ Einsatz von VPN-Tunneln
☑ Verschlüsselung der Kommunikationswege (TLS / HTTPS)
☐ Verschlüsselung physischer Datenträger bei Transport
☑ Sonstige: Verschlüsselte Datenübertragung zwischen Plattform, APIs und eingesetzten Cloud- und Kommunikationsdiensten.

III. Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit

☐ Unterbrechungsfreie Stromversorgung
☐ Klimatisierung der Serverräume
☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit
☐ Schutzsteckdosenleisten
☐ Feuer- und Rauchmeldeanlagen
☐ Feuerlöschgeräte
☐ Alarmmeldung bei unberechtigten Zutritten
☑ Erstellen eines Backup- & Recoverykonzepts
☑ Testen von Datenwiederherstellung
☑ Erstellen eines Notfallplans
☑ Aufbewahrung von Datensicherungen an ausgelagertem Ort
☐ Serverräume nicht unter sanitären Anlagen
☐ Serverräume über Hochwassergrenze
☑ belastbares Datensicherungs- und Wiederherstellungskonzept vorhanden
☑ Sonstige: Nutzung hochverfügbarer Cloud-Infrastruktur mit redundanten Systemen und Monitoring.

IV. Besondere Datenschutzmaßnahmen

☑ interne Verhaltensregeln
☑ Risikoanalyse
☐ Datenschutz-Folgenabschätzung
☑ Datensicherheitskonzept
☑ Wiederanlaufkonzept
☐ Zertifikat
☑ Sonstiges: Regelmäßige Überprüfung der technischen und organisatorischen Maßnahmen.

V. Überprüfung der Maßnahmen

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

Anlage 3 – Subunternehmer

| Unternehmen | Beschreibung der Leistung | Ort der Leistung | Kontakt |
|---|---|---|---|
| OpenAI, LLC | KI-Verarbeitung (LLM / Chat / Voice) | USA | https://openai.com |
| Twilio Inc. | Telefonie, SMS, Kommunikationsinfrastruktur | USA | https://twilio.com |
| Stripe Payments Europe Ltd | Zahlungsabwicklung | Irland | https://stripe.com |
| HighLevel LLC (GoHighLevel) | CRM- und Automationsplattform | USA | https://gohighlevel.com |
| Cloudflare Inc. | CDN, Sicherheit, Infrastruktur | USA / EU | https://cloudflare.com |