KI TELEFON AGENT

Vertrag zur Auftragsverarbeitung

Vertrag zur Auftragsverarbeitung für die Nutzung der Software
„KI-Telefon-Agent.com“

zwischen

AI Voice Impact UG (haftungsbeschränkt)
HRB: 195056
Hohe Bleichen 8,
20354 Hamburg

support@ai-voice-impact.com

- im Folgenden: Auftragnehmer –

und

Firma:

Adresse:

- im Folgenden: Auftraggeber -
schließen folgenden Vertrag:

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 der Bundesrepublik Deutschland, 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

Der vorliegende Vertrag wird auf unbestimmte Zeit geschlossen und kann von jeder Vertragspartei mit einer Frist von drei 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.

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. Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der Vertragslaufzeit regelmäßig im erforderlichen Umfang zu kontrollieren oder durch Dritte kontrollieren zu lassen. Der Auftragnehmer wird diese Kontrollen dulden und sie im erforderlichen Maße unterstützen. Er wird dem Auftraggeber insbesondere die für die Kontrollen relevanten Auskünfte vollständig und wahrheitsgemäß erteilen, ihm die Einsichtnahme in die gespeicherten Daten und Datenverarbeitungsprogramme/ -systeme gewähren sowie Vorort-Kontrollen ermöglichen. Sofern der Auftraggeber der Verarbeitung der Daten außerhalb der Geschäftsräume (z.B. Privatwohnung) zugestimmt hat, hat der Auftragnehmer dafür zu sorgen, dass der Auftraggeber auch diese Räume zu Kontrollzwecken begehen darf.

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 Vor Ort Kontrollen 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 mitgliedstaatlicher 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. 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 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.

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

6. Technische und organisatorische Maßnahmen

6.1. 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.

6.2. 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.

6.3. 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 innerhalb von 36 Stunden, 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.

6.4. 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.

7. Unterstützungspflichten des Auftragnehmers

7.1. 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.

7.2. 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.

8. Einsatz von Unter-Auftragnehmern (Subunternehmer)

8.1. 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.

8.2. 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 (allgemein) zu.

8.3. Überdies genehmigt der Auftraggeber hiermit in allgemeiner Weise die Inanspruchnahme weiterer Unter-Auftragnehmer 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. Nach dem Einspruch des Auftraggebers können beide Vertragsparteien den Vertrag mit einer Frist von 14 Tagen kündigen. Wenn der Auftraggeber sich innerhalb von 14 Tagen nicht widerspricht, gilt seine Zustimmung.

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

8.5. Der Auftragnehmer stellt sicher, dass der Auftraggeber gegenüber dem Unterauftragnehmer 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.

8.6. 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.

8.7. 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.

9. 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 Unter-Auftragnehmer 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.

10. 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.

11. 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

12. Haftung

13.1 Jede Partei haftet gegenüber der/den anderen Partei(en) für Schäden, die sie der/den anderen Partei(en) durch einen Verstoß gegen diese Klauseln verursacht.

13.2 Der Auftragnehmer haftet gegenüber der betroffenen Person, und die betroffene Person hat Anspruch auf Schadenersatz für jeden materiellen oder immateriellen Schaden, den der Auftragnehmer oder sein UnterAuftragnehmer der betroffenen Person verursacht, indem er deren Rechte als Drittbegünstigte gemäß diesen Klauseln verletzt.

13.3 Ungeachtet von Nummer 13.2 haftet der Auftragnehmer gegenüber der betroffenen Person, und 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 verursacht, indem er deren Rechte als Drittbegünstigte gemäß diesen Klauseln verletzt. Dies gilt unbeschadet der Haftung des Auftraggebers und, sofern der Auftraggeber ein im Auftrag eines Verantwortlichen handelnder Auftragnehmer ist, unbeschadet der Haftung des Verantwortlichen gemäß der Verordnung (EU) 2016/679 oder gegebenenfalls der Verordnung (EU) 2018/1725.

13.4 Die Parteien erklären sich damit einverstanden, dass der Auftraggeber, der nach Nummer 13.3 für durch den Auftragnehmer (oder dessen UnterAuftragnehmer) verursachte Schäden haftet, berechtigt ist, vom Auftragnehmer den Teil des Schadenersatzes zurückzufordern, der der Verantwortung des Auftragnehmers für den Schaden entspricht.

13.5 Ist mehr als eine Partei für Schäden verantwortlich, die der betroffenen Person infolge eines Verstoßes gegen diese Klauseln entstanden sind, so haften alle verantwortlichen Parteien gesamtschuldnerisch, und die betroffene Person ist berechtigt, gegen jede der Parteien gerichtlich vorzugehen.

13.6 Die Parteien erklären sich damit einverstanden, dass eine Partei, die nach Nummer 13.5 haftbar gemacht wird, berechtigt ist, 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 auf das Verhalten eines UnterAuftragnehmers berufen, um sich seiner eigenen Haftung entziehen.

13. Schlussbestimmungen

14.1 *Die Einrede des Zurückbehaltungsrechts, gleich aus welchem Rechtsgrund, an den vertragsgegenständlichen Daten sowie an evtl. vorhandenen Datenträgern wird ausgeschlossen.*

14.2 *Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.*

14.3 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.

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

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

14.6 Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift (Auftraggeber)	Unterschrift (Auftragnehmer)

KI TELEFON AGENT

Anlage 1 – Auftragsdetails

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

- Beschäftigte
- Kunden
- Interessenten
- Geschäftspartner

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

- Personenstammdaten (Name, Vorname, Adresse)
- Kommunikationsdaten (E-Mail, Telefonnummer, Handynummer)
- Rechnungsdaten
- Zahlungsdaten
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)

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

- Bereitstellung eines KI-Telefon-Agenten auf Grundlage des Vertrags in der jeweiligen aktuellen Fassung auf der Website ki-telefon-agent.com/preise

Folgende Leistungen werden vom Auftraggeber beauftragt:

- Setup, Wartung und Support eines KI-Telefon-Agenten in folgenden Umfang (Umfang richtet sich nach Tarif):
    - Batch-Kampagnen (Massenanrufe) Automatische Gesprächsführung KI-gestützte Terminvereinbarung Lead-Qualifizierung & Routing Echtzeit Gesprächsaufzeichnung Gesprächskontrolle & CRM-Integration API-Zugriff & Webhooks
    - LLM Agent (Large Language Model) Voice Agent API
    - Transcriber (Gesprächstranskription) KI-optimierte Gesprächsführung Automatisierte Follow-ups per E-Mail/SMS Integration mit CRM-Systemen
    - Erweiterte Analysen & Performance-Tracking Echtzeit-Transkription der Gespräche Anrufweiterleitung Buchung in Echtzeit
    - SMS senden

KI TELEFON AGENT

ANHANG II – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

Beschreibung der von dem Datenimporteur ergriffenen technischen und organisatorischen Maßnahmen (einschließlich aller relevanten Zertifizierungen) zur Gewährleistung eines angemessenen Schutzniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen.

Es werden nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO getroffen.

1. Vertraulichkeit

Zutrittskontrolle
Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen.

- Empfang / Rezeption / Pförtner
- Sicherheitsschlösser
- Videoüberwachung der Eingänge
- Mitarbeiter- / Besucherausweise
- Besucher in Begleitung durch Mitarbeiter

Zugangskontrolle
Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können. Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

- Login mit Benutzername + Passwort
- Login mit biometrischen Daten
- Anti-Viren-Software Server
- Anti-Virus-Software Clients
- Anti-Virus-Software mobile Geräte

- Firewall
- Einsatz VPN bei Remote-Zugriffen
- Verschlüsselung von Datenträgern
- Verschlüsselung Smartphones
- Automatische Desktopsperre
- Verschlüsselung von Notebooks / Tablet
- Verwalten von Benutzerberechtigungen
- Erstellen von Benutzerprofilen
- Richtlinie „Sicheres Passwort“
- Richtlinie „Löschen / Vernichten“
- Allg. Richtlinie Datenschutz und / oder Sicherheit

Zugriffskontrolle
Maßnahmen, 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. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

- Akten Schredder (mind. Stufe 3, cross cut)
- Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten
- Minimale Anzahl an Administratoren
- Verwaltung Benutzerrechte durch Administratoren

Trennungskontrolle
Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

- Trennung von Produktiv- und Test-Umgebung
- Mandantenfähigkeit relevanter Anwendungen
- Festlegung von Datenbankrechten

Pseudonymisierung & Verschlüsselung
Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

2. Integrität

Eingabekontrolle
Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

- Technische Protokollierung der Eingabe, Änderung und Löschung von Date
- Manuelle oder automatisierte Kontrolle der Protokolle
- Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
- Klare Zuständigkeiten für Löschungen

Weitergabekontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

- Protokollierung der Zugriffe und Abrufe
- Bereitstellung über verschlüsselte Verbindungen wie sftp, https
- Nutzung von Signaturverfahren

Auftragskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

- Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
- Auswahl des Auftragnehmers unter Sorgfalts Gesichtspunkte (gerade in Bezug auf Datenschutz und Datensicherheit)
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standardvertragsklauseln
- Schriftliche Weisungen an den Auftragnehmer
- Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
- Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
- Regelung zum Einsatz weiterer Subunternehmer
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und sei Schutzniveaus

3. Verfügbarkeit und Belastbarkeit

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raid Systeme, Plattenspiegelungen etc.

- Feuer- und Rauchmeldeanlagen
- Feuerlöscher im Serverraum
- Serverraumüberwachung Temperatur und Feuchtigkeit
- Serverraum klimatisiert
- Schutzsteckdosenleisten Serverraum
- RAID-System / Festplattenspiegelung
- Alarmmeldung bei unberechtigtem Zutritt zum Serverraum
- Kontrolle des Sicherungsvorgangs (Backup & Recovery-Konzept)
- keine sanitären Anschlüsse im oder oberhalb des Serverraums
- Getrennte Partitionen für Betriebssysteme und Daten

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutzmanagement

- Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt
- Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet
- Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich
- Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach

Incident-Response-Management
Unterstützung bei der Reaktion auf Sicherheitsverletzungen

- Einsatz von Firewall und regelmäßige Aktualisierung

- Einsatz von Virenscanner und
- regelmäßige Aktualisierung
- Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
- Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem

Privacy by Design/Privacy by Default Privacy by design / Privacy by default

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
- Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maß- nahmen

KI TELEFON AGENT

ANHANG III – LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

1. Name: BEK Service GmbH
Anschrift: Westendstr. 2A, 87439 Kempten (Allgäu), Deutschland

Gegenstand/Art der Verarbeitung:

● Bereitstellung der Technischen Infrastruktur KI-Telefon-Agent Dauer der Verarbeitung: fortlaufend

2. Name: SiliconForest UG (haftungsbeschränkt)
Anschrift: Grävenhorster Straße 6, 28755 Bremen, Deutschland

Gegenstand/Art der Verarbeitung:

Freelancer: Technische Umsetzung, Entwicklung und Betreuung einzelner Projektbestandteile (Freelancer-Entwicklung, Integration, Fehlerbehebung, Testing) im Rahmen der Bereitstellung der KI-Telefonie-Dienstleistungen.

3. Name: Contabo GmbH, Welfenstraße 22, 81541 München

Gegenstand/Art der Verarbeitung:

Serverbetrieb für Custom-Endpoints zur Datenaufbereitung innerhalb von Aktionen, für KI-Telefoninstanzen, Dispatcher-Service zum Auslösen von Outbound-Gesprächen abhängig von der jeweiligen Kundenkonfiguration.