Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO

Praxis/Klinik (Name/Anschrift)

_____

_____

_____

-im Folgenden: **Auftraggeber**-

Und

ReHa-Hilfe e.V.

Vollmannstr. 16
81927 München

-im Folgenden: **Auftragnehmer**-

Der Auftraggeber (für die Verarbeitung verantwortlich) und der Auftragnehmer schließen den folgenden Vertrag zur Auftragsverarbeitung gemäß Art. 28 der europäischen Datenschutz-Grundverordnung (DSGVO). Auf Grundlage des zwischen den Parteien bestehenden Vertragsverhältnisses (Hauptvertrag) verarbeitet der Auftragnehmer personenbezogene Daten für den Auftraggeber. Die sich daraus ergebenden datenschutzrechtlichen Rechte und Verpflichtungen der Parteien werden durch diesen Auftrags-verarbeitungsvertrag konkretisiert.

§ 1 Gegenstand und Dauer der Verarbeitung

a) Gegenstand des Vertrages ist die Verarbeitung personenbezogener Daten (nachstehend „Daten“ genannt) durch den Auftragnehmer für den Auftraggeber in dessen Auftrag und nach dessen Weisung. Der Gegenstand und die Dauer des Vertrages richten sich nach dem Hauptvertrag.

b) Der Auftraggeber kann diesen Vertrag sowie den Hauptvertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen dieser Vereinbarung vorlieget, ein solcher schwerwiegender Verstoß liegt insbesondere dann vor, wenn der Auftragnehmer die Daten des Auftraggebers für andere als die nach dieser Vereinbarung bestimmten Zwecke verwendet oder gegen eine wesentliche Pflicht aus dieser Vereinbarung verstößt.

c) Auch bei Nichtvorliegen der zuvor genannten Voraussetzungen ist der Auftraggeber berechtigt, diese Vereinbarung und den Hauptvertrag fristlos zu kündigen, wenn der Auftragnehmer wiederholt

gegen diese Vereinbarung verstößt. Ein vorheriger schriftlicher Hinweis oder ein Hinweis in Textform des Auftraggebers ist hierfür Voraussetzung.

§ 2 Umfang, Art und Zweck der Verarbeitung

Umfang, Art und Zweck der Verarbeitung personenbezogener Daten ergeben sich aus dem zwischen den Parteien geschlossenen Dienstleistungsvertrag. Der Auftragnehmer führt dabei insbesondere folgende Verarbeitungen für den Auftraggeber durch:

☐ Verarbeitung und Analyse von Sprachaufzeichnungen

§ 3 Art der personenbezogenen Daten

Der Auftragnehmer erhält Zugriff auf folgende personenbezogene Daten (dadurch, dass der Auftraggeber ihm die Daten bereitstellt oder ihm einen Zugriff auf die Daten ermöglicht), bzw. der Auftraggeber erlaubt dem Auftragnehmer folgende personenbezogene Daten zu erheben:

☐ Personenstammdaten
☐ Sprachaufzeichnungen/ Ton-Aufnahmen

§ 4 Kreis der betroffenen Personen

Bei den betroffenen Personen der oben aufgelisteten Daten handelt es sich um:

☐ PatientInnen
☐ TherapeutInnen

§ 5 Rechte und Pflichten des Auftraggebers; Kontrollrechte

a) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie zur Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich und somit Verantwortlicher im Sinne des Art. 4 Abs. 7 DSGVO.

b) Der Auftraggeber erteilt dem Auftragnehmer Weisungen über die Art und den Umfang der Verarbeitung der personenbezogenen Daten.

c) Vor Beginn des Auftrages und der damit verbundenen Datenverarbeitung und im Anschluss regelmäßig ist der Auftraggeber berechtigt, nach rechtzeitiger vorheriger Anmeldung zu den üblichen Geschäftszeiten, sich von der Einhaltung der bei dem Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit zu überzeugen. Der Auftraggeber kann diese Kontrolle auch durch einen Dritten durchführen lassen.

d) Der Auftragnehmer erklärt sich damit einverstanden, dass sich der Auftraggeber jederzeit nach vorheriger Ankündigung von der Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang selbst oder durch Dritte überzeugen kann, dies insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Systeme sowie sonstige Kontrollen vor Ort.

e) Der Auftragnehmer hat eventuelle Kontrollmaßnahmen der Datenschutzaufsichtsbehörde gem. Art. 58 DSGVO und § 40 BDSG-neu zu dulden. Er wird den Auftraggeber unverzüglich nach Ankündigung oder Kenntniserlangung über die Durchführung der Kontrollmaßnahme sowie bei anderweitigen

Anfragen, Ermittlungen oder Erkundigungen der Datenschutzaufsichtsbehörde, insbesondere auch, wenn diese im Rahmen einer vorherigen Konsultation gem. Art. 36 DSGVO erfolgen, informieren, soweit die Maßnahmen oder Anfragen Datenverarbeitungen betreffen können, die der Auftragnehmer für den Auftraggeber erbringt.

f) Auf Verlangen des Auftraggebers weist der Auftragnehmer die Einhaltung der getroffenen technischen und organisatorischen Maßnahmen nach. Dabei kann der Nachweis durch die Vorlage eines aktuellen Testats oder Berichts (wie z.B. Wirtschaftsprüfer, externer Datenschutzbeauftragter, Revisor oder einem externen Datenschutzauditor) und gegebenenfalls einer geeigneten Zertifizierung (z.B. nach BSI-Grundschutz, ISO27001 oder nach einem genehmigten Zertifizierungsverfahren gem. Art. 42 DSGVO) oder die Einhaltung genehmigter Verhaltensregeln gem. Art. 40 DSGVO erbracht werden. Die Kontrollrechte des Auftraggebers bleiben hiervon unberührt.

§ 6 Pflichten von des Auftragnehmers

a) Der Auftragnehmer ist verpflichtet, personenbezogene Daten ausschließlich weisungsgemäß und nach den Vorgaben dieses Vertrages zu verarbeiten.

b) Bei der Gewährung der Rechte der Betroffenen gemäß Art. 15 ff. DSGVO (Berichtigung, Einschränkung der Verarbeitung, Löschung, Benachrichtigung und Auskunftserteilung) wird der Auftragnehmer den Auftraggeber auf erstes Anfordern im Rahmen seiner Möglichkeiten unterstützen. Der Auftragnehmer wird hierfür geeignete technische und organisatorische Maßnahmen treffen. Der Auftragnehmer hat auf Weisung die personenbezogenen Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder die Verarbeitung einzuschränken.

c) Sollte die im Auftrag des Auftraggebers erhobenen Daten Gegenstand eines Verlangens auf Datenportabilität gemäß Art. 20 DSGVO sein, wird der Auftragnehmer dem Auftraggeber den betreffenden Datensatz unverzüglich auf Anforderung in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung stellen.

d) Sofern sich eine betroffene Person unmittelbar an den Auftragnehmer mit der Wahrnehmung ihrer Betroffenenrechte wendet, hat dieser dieses Ersuchen unverzüglich an den Auftraggeber weiterzuleiten.

e) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf hinweisen, wenn diese der Meinung ist, dass eine erteilte Weisung gegen gesetzliche Vorschriften verstößt. Die Durchführung der entsprechenden Weisung kann dieser solange aussetzen, bis sie durch den Auftraggeber bestätigt oder abgeändert wird.

f) Nach Beendigung des Hauptvertrages ist der Auftragnehmer verpflichtet, sämtliche in seinen Besitz gelangten personenbezogenen Daten die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen sowie datenschutz- und datensicherheitskonform und gemäß den Weisungen zu löschen. Dies betrifft auch etwaige Datensicherungen bei dem Auftragnehmer. Die datenschutz- und datensicherheitskonforme Löschung ist zu dokumentieren mit Datumsangabe dem Auftraggeber schriftlich zu bestätigen.

g) Der Auftragnehmer stellt sicher, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpfichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitsficht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspficht besteht auch nach Beendigung des Auftrages fort. Sofern

der Auftragnehmer im Zusammenhang mit den Leistungen für den Auftraggeber an der Erbringung geschäftsmäßiger Telekommunikationsdienste mitwirkt, ist er verpflichtet, die hieran beteiligten Beschäftigten schriftlich auf das Fernmeldegeheimnis gemäß dem Telekommunikationsgesetz zu verpflichten.

§ 7 Leistungsort

a) Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung durch den Auftraggeber und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

b) Sofern die Verarbeitung personenbezogener Daten außerhalb der EU erfolgt, garantiert der Auftragnehmer, dass die nach den jeweils geltenden Datenschutzvorschriften anwendbaren Voraussetzungen für das Eingreifen eines Erlaubnistatbestandes für die Verarbeitung personenbezogener Daten außerhalb der EU erfüllt sind ("datenschutzrechtliche Rechtfertigung"). Dies ist zum einen gegeben, sofern und soweit die EU-Kommission diesem bzw. dieser ein angemessenes Schutzniveau bescheinigt hat. Weiterhin wenn die Verarbeitung der personenbezogenen Daten außerhalb der EU ausschließlich im Rahmen eines Programms erfolgt, dem von der EU-Kommission ein angemessenes Schutzniveau bescheinigt wurde (gegenwärtig z.B. das EU-U.S. Privacy Shield), und er die für die Teilnahme an dem Programm erforderlichen formellen und inhaltlichen Voraussetzung erfüllt, er sich hierfür qualifiziert hat und während der Laufzeit des Auftrages ununterbrochen für das Programm qualifiziert bleibt.

§ 8 Unterauftragsverhältnisse

a) Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Auftragnehmer den Auftraggeber im Einzelfall.

b) Der Auftraggeber kann der Änderung – innerhalb einer angemessenen Frist – aus wichtigem Grund – gegenüber der vom Auftraggeber bezeichneten Stelle widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.

c) Bei Einschaltung eines weiteren Auftragsverarbeiter muss stets ein Schutzniveau, welches mit demjenigen dieser Vereinbarung vergleichbar ist, gewährleistet werden. Der Auftragnehmer bleibt jedoch zu jeder Zeit verantwortlich für jegliche Handlung oder Unterlassung der von ihm beauftragten weiteren Auftragsverarbeiter, in selber Weise wie er für die eigenen Handlungen und Unterlassungen verantwortlich ist.

d) Der Auftragnehmer hat die Einhaltung der Pflichten des weiteren Auftragsverarbeiters regelmäßig zu überprüfen. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der weitere Auftragsverarbeiter die zugesicherten und erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat.

e) Der Auftragnehmer arbeitet derzeit bei der Erfüllung des Auftrags mit den folgenden weiteren Auftragsverarbeitern zusammen, mit deren Beauftragung sich der Auftraggeber einverstanden erklärt:

Name und Anschrift des Subunternehmers	Beschreibung der Leistungen
clickworker GmbH Büropark Bredeney Hatzper Str. 30 45149 Essen	Vermittlung der Laienhörer zur Bewertung der Sprachaufnahmen
1blu AG Riedemannweg 60 13627 Berlin	V-Server, Hosting der KommPaS WebApp, E-Mail-Versand

§ 9 Technische und organisatorische Maßnahmen

a) Der Auftragnehmer ist verpflichtet, die Grundsätze ordnungsgemäßer Datenverarbeitung gem. Art 32 i.V.m Art. 5 Abs. 1 DSGVO einzuhalten. Er wird alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Standes der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene ergreifen. Die zu treffenden Maßnahmen umfassen insbesondere Maßnahmen, mit denen eine angemessene Pseudonymisierung und Verschlüsselung gewährleistet werden kann sowie Maßnahmen zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Maßnahmen, die die Kontinuität der Verarbeitung nach Zwischenfällen gewährleisten.

b) Die von dem Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sind ausführlich in der Anlage zu diesem Vertrag dargestellt und sind Vertragsbestandteil.

§ 10 Haftung

a) Der Auftragnehmer haftet gegenüber dem Auftraggebern gemäß der gesetzlichen Regelungen für sämtliche Schäden durch schuldhafte Verstöße gegen diesen Vertrag, sowie gegen die ihn treffenden gesetzlichen Datenschutzbestimmungen, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung verursachen.

b) Für den Ersatz von Schäden, die ein Betroffener aufgrund einer nach der DSGVO oder dem BDSG-neu oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses geltend macht, der Auftraggeber bzw. der Auftragnehmer gem. Art. 82 DSGVO gegenüber dem Betroffenen verantwortlich. Der Auftragnehmer stellt den Auftraggeber im Innenverhältnis von allen Schadensersatzansprüchen frei, die aufgrund einer schuldhaften Verletzung der Verpflichtungen aus diesem Vertrag durch den Auftragnehmer gegen den Auftraggeber geltend gemacht werden.

§ 11 Vertraulichkeit und Geheimhaltung

Der Auftraggeber ist dem Gesetz nach zur Verschwiegenheit verpflichtet (Berufsgeheimnisträger) und somit neben den datenschutzrechtlichen Schutzmaßnahmen verpflichtet, fremde Geheimnisse zu schützen. Die Offenbarung fremder Geheimnisse, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis – oder Betriebs, oder Geschäftsgeheimnis, ist unter Strafe gestellt (§ 203 StGB). Um diese Geheimnisse zu schützen und die Offenbarung auszuschließen, verpflichtet sich der Auftragnehmer zu dieser besonderen Vertraulichkeit und Geheimhaltung und wird im gleichen Maße die berufsrechtliche Verschwiegenheit waren.

§ 12 Schlussbestimmungen

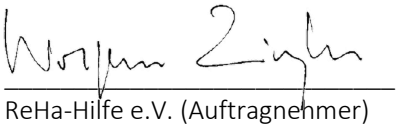
a) Im Falle von Widersprüchen zwischen den Bestimmungen in dieser Vereinbarung und den Regelungen des Hauptvertrages gehen die Bestimmungen dieser Vereinbarung vor.

b) Änderungen und Ergänzungen dieser Vereinbarung müssen schriftlich erfolgen und bedürfen der ausdrücklichen Angabe, dass damit die vorliegenden Bestimmungen geändert und/oder ergänzt werden. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

c) Sollte eine Bestimmung dieser Vereinbarung unwirksam oder nicht durchsetzbar sein oder werden, so bleiben die übrigen Bestimmungen dieser Vereinbarung hiervon unberührt. Die unwirksame oder nicht durchsetzbare Bestimmung ist durch eine wirksame und durchsetzbare Bestimmung zu ersetzen, welche dem Zweck der ersetzenden Bestimmung am nächsten kommt.

d) Diese Vereinbarung unterliegt deutschem Recht.

e) Sofern der Zugriff auf die Daten durch Maßnahmen Dritter (z.B. Maßnahmen eines Insolvenzverwalters, Beschlagnahme durch Finanzbehörden, etc.) gefährdet wird, hat der Auftragnehmer den Auftraggeber unverzüglich hierüber zu benachrichtigen.

_____	München, 2. 6. 2020
Ort, Datum	Ort, Datum
_____	
Auftraggeber	ReHa-Hilfe e.V. (Auftragnehmer)

ANLAGE - Technische und organisatorische Maßnahmen

Der Auftragnehmer versichert die folgenden technische und organisatorische Maßnahmen getroffen zu haben:

1. Maßnahmen zur Sicherung der Vertraulichkeit

a) Zutrittskontrolle

Maßnahmen, die unbefugten Personen den Zutritt zu IT-Systemen und Datenverarbeitungsanlagen mit denen personenbezogene Daten verarbeitet werden, sowie vertraulichen Akten und Datenträgern physisch verwehren.

Beschreibung des Zutrittskontrollsystems:

- ☐ Das Rechenzentrum verfügt über einbruchshemmende Türen und Lüftungsklappen.
- ☐ Es besteht eine Schlüsselregelung samt dokumentierter Schlüsselvergabe.
- ☐ Das Rechenzentrum ist durch ein personalisiertes biometrisches Zutrittskontrollsystem abgesichert.
- ☐ Eine Richtlinie regelt den Zutritt und die Überwachung von Besuchern.
- ☐ Der Zutritt zu den Serverräumen ist gesondert geregelt.
- ☐ Besucher im Rechenzentrum werden protokolliert.
- ☐ Videoüberwachung ist im Rechenzentrum installiert.
- ☐ Es besteht eine Alarmanlage, deren Auslösung eine automatische Benachrichtigung des Bereitschaftsdienstes nach sich zieht.
- ☐ Das Rechenzentrum weist keine Fenster auf.

b) Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte datenschutzrechtlich geschützte Daten verarbeiten oder nutzen können.

Beschreibung des Zugangskontrollsystems:

- ☐ Kennwortverfahren, d.h. persönlicher und individueller User Log-In bei Anmeldung am System (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennwortes)
- ☐ Einrichtung eines Benutzerstammsatzes pro User
- ☐ Begrenzung der Zahl der berechtigten Mitarbeiter
- ☐ Authentifizierungsverfahren

c) Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, so dass Daten bei der Verarbeitung, Nutzung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Beschreibung des Zugriffskontrollsystems:

- ☐ Berechtigungskonzepte (Profile, Rollen, etc.) und deren Dokumentation

☐ Archivierungskonzept

d) Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und so von anderen Daten und Systemen getrennt sind, dass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist.

Beschreibung des Trennungskontrollvorgangs:

☐ Berechtigungskonzepte
☐ Softwareseitige Kundentrennung
☐ Trennung von Test- und Produktivsystemen

e) Pseudonymisierung

Maßnahmen, die den unmittelbaren Personenbezug während der Verarbeitung in einer Weise reduzieren, dass nur mit Hinzuziehung zusätzlicher Informationen eine Zuordnung zu einer spezifischen betroffenen Person möglich ist. Die Zusatzinformationen sind dabei durch geeignete technische und organisatorische Maßnahmen von dem Pseudonym getrennt aufzubewahren.

Beschreibung des Pseudonymisierungsverfahrens:

☐ zufällig generierte IDs

2. Maßnahmen zur Sicherung der Integrität

a) 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 sowie Maßnahmen mit denen überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten vorgesehen ist.

Beschreibung der Weitergabekontrolle:

☐ Übermittlung von Daten über verschlüsselte Datennetze oder Tunnelverbindungen

b) Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind.

Beschreibung des Eingabekontrollvorgangs:

☐ Veränderungen von personenbezogenen Daten können nur mit dem zugehörigen Nutzeraccount vorgenommen werden

3. Maßnahmen zur Sicherung der Verfügbarkeit und Belastbarkeit

a) Verfügbarkeitskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Beschreibung des Verfügbarkeitskontrollsystems:

- ☐ Um die Daten nach einem Ausfall wiederherstellen zu können, existiert ein vollständiges Backup- & Recovery-Konzept.
- ☐ Es wird eine tägliche Datensicherung automatisch durchgeführt.
- ☐ Um größtmögliche Verfügbarkeit der Daten zu erzielen, werden in den Servern RAID-Systeme eingesetzt.

b) rasche Widerherstellbarkeit

Maßnahmen, die die Fähigkeit sicherstellen, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Beschreibung der Maßnahmen:

- ☐ Datensicherungsverfahren

4. Maßnahmen zur regelmäßigen Evaluation der Sicherheit der Datenverarbeitung

Maßnahmen, die die datenschutzkonforme und sichere Verarbeitung sicherstellen.

Beschreibung der Überprüfungsverfahren:

- ☐ Datenschutzmanagement