TelePsy

Datenverarbeitungsvereinbarung

Version 1.2 – 29.03.2019

ANWENDBARKEIT

Diese Datenverarbeitungsvereinbarung gilt für die gesamte Verarbeitung personenbezogener Daten, welche von der TelePsy Deutschland GmbH (nachfolgend: Auftragsverarbeiter) für Sie als Gegenpartei, für die Leistungen erbracht werden (nachfolgend: Verantwortlicher), durchgeführt werden. Der Verantwortliche nimmt durch die Aktivierung vom und das Einloggen im (Demo-)konto, die Leistungen des Auftragsverarbeiters in Anspruch und stimmt dieser Vereinbarung und deren Bedingungen zu. Die Allgemeinen Geschäftsbedingungen des Auftragsverarbeiters sind ein untrennbarer Bestandteil dieser Datenverarbeitungsvereinbarung und diese Datenverarbeitungsvereinbarung unterliegt den Allgemeinen Geschäftsbedingungen des Auftragsverarbeiters.

UNTER BERÜCKSICHTIGUNG FOLGENDER UMSTÄNDE:

(a) Der Verantwortliche möchte Leistungen des Auftragsverarbeiters, hinsichtlich der Entwicklung und der Zurverfügungstellung des Programms, in der unterschiedliche Instrumente zum Messen, Beobachten und Behandeln von Klienten/Patienten innerhalb der Gesundheidsfürsorge zur verfügung stehen, in Anspruch nehmen.

(b) Die Leistungen umfassen auch die Verarbeitung personenbezogener Daten, darunter Gesundheitsdaten.

(c) Der Auftragsverarbeiter verarbeitet die betreffenden Daten ausschließlich im Auftrag des Verantwortlichen und nicht für eigene Zwecke.

(d) Ab 25. Mai 2018 gilt die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 (Datenschutz-Grundverordnung).

(e) Die Vertragsparteien möchten in der vorliegenden Datenverarbeitungsvereinbarung die Absprachen hinsichtlich der Verarbeitung von personenbezogenen Daten im Rahmen der Leistungen festhalten.

(f) Die vorliegende Datenverarbeitungsvereinbarung ersetzt gegebenenfalls alle früheren Verträge der Vertragsparteien mit gleicher Absicht.

ERKLÄREN, FOLGENDES VEREINBART ZU HABEN:

Artikel 1. Begriffsbestimmungen

1.1. In der vorliegenden Datenverarbeitungsvereinbarung haben folgende Begriffe die folgende Bedeutung:

a)	Datenschutz-Grundverordnung bzw. DSGVO	Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.
b)	Betroffene Person	eine identifizierte oder identifizierbare natürliche Person (Artikel 4 Punkt 1 DSGVO).
c)	Dritter	ein Dritter im Sinne von Artikel 4 Punkt 10 DSGVO.
d)	Datenschutzbeauftragter	ein Beauftragter im Sinne von Artikel 37 ff. DSGVO.

e)	Vorkommnis	eine Beschwerde oder ein (Auskunfts-) Ersuchen einer betroffenen Person in Bezug auf die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter; eine Untersuchung bzw. Beschlagnahme der personenbezogenen Daten durch zuständige Beamte oder eine Vermutung, dass etwas Derartiges stattfinden wird; eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Punkt 12 DSGVO; jedweder nicht genehmigter Zugang, jedwede Löschung, Manipulation, jedweder Verlust oder irgendeine andere Form der unrechtmäßigen Verarbeitung der personenbezogenen Daten.
f)	Mitarbeiter	die von den Vertragsparteien zur Erfüllung der vorliegenden Datenverarbeitungsvereinbarung herangezogene natürliche Person, die bei einer oder für eine der Vertragsparteien beschäftigt ist.
g)	Vertrag bzw. Verträge	Jeder Vertrag und jede Vereinbarung in welcher der Auftragsverarbeiter leistungen für den Verantwortlichen verrichtet und wobei der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, wie z.B. Demokonten.
h)	Vertragspartei	Verantwortlicher oder Auftragsverarbeiter.
i)	Vertragsparteien	Verantwortlicher und Auftragsverarbeiter.
j)	Personenbezogene Daten	sämtliche Informationen zu einer identifizierten oder identifizierbaren natürlichen Person im Sinne von Artikel 4 Punkt 1 DSGVO.
k)	Unterauftragsverarbeiter	jede nicht untergeordnete Drittpartei, die vom Auftragsverarbeiter zur Verarbeitung personenbezogener Daten im Rahmen des Vertrags herangezogen wurde und bei der es sich nicht um Mitarbeiter handelt.
l)	Auftragsverarbeiter	der Auftragsverarbeiter im Sinne von Artikel 4 Punkt 8 DSGVO.
m)	Datenverarbeitungsvereinbarung	der vorliegende Vertrag.
n)	Verantwortlicher	der Verantwortliche im Sinne von Artikel 4 Punkt 7 DSGVO.

1.2. Die oben genannten sowie die sonstigen Begriffe werden gemäß der DSGVO ausgelegt. Bis zum 25. Mai 2018 werden Begriffe gemäß der entsprechenden Bestimmung im deutschen Datenschutzgesetz ausgelegt.

1.3. Wenn in der vorliegenden Datenverarbeitungsvereinbarung auf bestimmte Normen der gesetzliche Regelungen verwiesen wird (wie etwa auf die DIN ISO/IEC27001), ist damit regelmäßig die jeweils aktuelle Fassung zum Zeitpunkt der Auslegung des Vereinbarung gemeint. Wenn die betreffende Norm nicht mehr aktualisiert wird, ist statt dieser Norm die jeweils aktuelle Fassung der betreffenden nachfolgenden Norm zu lesen.

1.4. Eventuelle Textabweichungen haben nur dann Geltung, wenn sie in Anhang 4 konkret aufgeführt sind. Die Bestimmungen in Anhang 4 gelten gegenüber den sonstigen Bestimmungen in der vorliegenden Datenverarbeitungsvereinbarung vorrangig.

Artikel 2. Gegenstand der vorliegenden Datenverarbeitungsvereinbarung

2.1. Die vorliegende Datenverarbeitungsvereinbarung bezieht sich auf die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen im Rahmen der Erfüllung der Verträge.

2.2. Die Vertragsparteien schließen die Verträge, um den Sachverstand, den der Auftragsverarbeiter in Bezug auf die Verarbeitung und die Sicherheit personenbezogener Daten besitzt, zu den Zwecken zu nutzen, die sich aus den Verträgen ergeben und in der vorliegenden Datenverarbeitungsvereinbarung konkret aufgeführt sind. Der Auftragsverarbeiter garantiert, dass er dazu qualifiziert ist.

2.3. Die vorliegende Datenverarbeitungsvereinbarung ist untrennbarer Bestandteil der Verträge. Sofern die Bestimmungen in der Datenverarbeitungsvereinbarung den Bestimmungen in den Verträgen widersprechen, gelten die Bestimmungen in der Datenverarbeitungsvereinbarung vorrangig.

Artikel 3. Durchführung der Verarbeitung

3.1. Der Auftragsverarbeiter garantiert, dass er für den Verantwortlichen ausschließlich personenbezogene Daten verarbeitet, sofern:

a) dies für die Erfüllung des Vertrags erforderlich ist (im Rahmen der Vorgaben in Anhang 1); oder

b) der Verantwortlicher diesbezüglich konkrete schriftliche Anweisungen erteilt hat.

3.2. Im Rahmen der Bestimmungen in Absatz 1 von Artikel 3 Buchstabe a) verarbeitet der Auftragsverarbeiter die in Anlage 1 0 aufgeführten personenbezogenen Daten in der Art und Weise sowie zu den Zwecken, die in diesem Anhang genannt sind.

3.3. Der Auftragsverarbeiter befolgt alle berechtigten Anweisungen des Verantwortlichen im Zusammenhang mit der Verarbeitung der personenbezogenen Daten. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn Anweisungen seiner Auffassung nach dem geltenden Recht bezüglich der Verarbeitung personenbezogener Daten widersprechen.

3.4. Unbeschadet der Bestimmungen in Absatz 1 dieses Artikels 3 ist es dem Auftragsverarbeiter gestattet, personenbezogene Daten zu verarbeiten, wenn eine gesetzliche Vorschrift (einschließlich darauf beruhender richterlicher oder behördlicher Anordnungen) ihn zur Verarbeitung verpflichtet. In diesem Fall setzt der Auftragsverarbeiter den Verantwortlichen vor der Verarbeitung über die beabsichtigte Verarbeitung in Kenntnis, es sei denn, diese gesetzliche Vorgabe verbietet eine solche Mitteilung aus gewichtigen Gründen des öffentlichen Interesses. Der Auftragsverarbeiter versetzt den Verantwortlichen nach Möglichkeit in die Lage, sich gegen eine solche obligatorische Verarbeitung zu wehren und die obligatorische Verarbeitung auf den unbedingt notwendigen Umfang zu beschränken.

3.5. Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nachweislich in angemessener und gewissenhafter Weise sowie im Einklang mit den für ihn als Auftragsverarbeiter geltenden Verpflichtungen aufgrund der DSGVO bzw. – sofern noch zutreffend – nach dem Bundesdatenschutzgesetz sowie den übrigen Gesetzen und Bestimmungen. Der Auftragsverarbeiter legt in diesem Rahmen mindestens ein Verzeichnis der Verarbeitungstätigkeiten im Sinne von Artikel 30 DSGVO an und übermittelt dem Verantwortlichen auf erstes Verlangen eine Kopie dieses Verzeichnisses.

3.6. Wenn die Leistungserbringung durch den Auftragsverarbeiter auch die Verarbeitung von Gesundheitsdaten oder von anderen besonderen personenbezogenen Daten umfasst, garantiert der Auftragsverarbeiter, dass er nicht im Widerspruch zum entsprechenden Gesundheitsrecht handelt.

3.7. Außerhalb des Europäischen Wirtschaftsraums (EWR) verarbeitet der Auftragsverarbeiter keine personenbezogenen Daten und lässt dort keine solchen Daten von Dritten verarbeiten, es sei denn, der Verantwortliche hat dazu vorab ausdrücklich seine schriftliche Zustimmung erteilt.

3.8. Der Auftragsverarbeiter gewährleistet, dass die beteiligten Mitarbeiter eine Vertraulichkeitsvereinbarung unterzeichnet haben, und gewährt dem Verantwortlichen auf Verlangen Einblick in diese Vertraulichkeitsvereinbarung.

Artikel 4. Sicherheit der personenbezogenen Daten und Kontrolle

4.1. Der Auftragsverarbeiter trifft nachweislich geeignete und wirksame technische und organisatorische Sicherheitsvorkehrungen, die angesichts des aktuellen Stands der Technik und den damit verbundenen Kosten der (in 0 genannten) Art der zu verarbeitenden personenbezogenen Daten entsprechen und dem Schutz der personenbezogenen Daten vor Verlust, unbefugter Kenntnisnahme, Manipulation oder irgendeiner Form der unrechtmäßigen Verarbeitung dienen sowie die (pünktliche) Verfügbarkeit der Daten gewährleisten. In diesen Sicherheitsvorkehrungen sind die möglicherweise im Vertrag bereits festgelegten Maßnahmen bereits enthalten. Die Maßnahmen umfassen in jedem Fall Folgendes:

a) Maßnahmen, um zu gewährleisten, dass ausschließlich befugte Mitarbeiter Zugang zu den personenbezogenen Daten im Rahmen der angegebenen Zwecke haben;

b) Maßnahmen, mit denen der Auftragsverarbeiter seinen Mitarbeitern und Unterauftragsverarbeitern Zugang zu personenbezogenen Daten ausschließlich über personengebundene Benutzerkonten gewährt, wobei die Nutzung dieser Konten in geeigneter Weise protokolliert wird und die betreffenden Konten ausschließlich zu den personenbezogenen Daten Zugang verschaffen, deren Zugang für die betreffenden (juristischen) Personen erforderlich ist;

c) Maßnahmen, um die personenbezogenen Daten vor unbeabsichtigter oder unrechtmäßiger Vernichtung, unbeabsichtigtem Verlust oder unbeabsichtigter Änderung, unbefugter oder unrechtmäßiger Speicherung, Verarbeitung, Zugang oder Offenlegung zu schützen;

d) Maßnahmen, um bezüglich der Verarbeitung personenbezogener Daten in den Systemen, die eingesetzt werden, um Leistungen für den Verantwortlichen zu erbringen, Schwachstellen zu identifizieren;

e) Maßnahmen, um die zeitnahe Verfügbarkeit der personenbezogenen Daten zu gewährleisten;

f) Maßnahmen, um zu gewährleisten, dass personenbezogene Daten logisch getrennt von solchen personenbezogenen Daten verarbeitet werden, die der Auftragsverarbeiter für sich selbst oder im Namen dritter Vertragsparteien verarbeitet;

g) die sonstigen Maßnahmen, die von den Vertragsparteien vereinbart wurden, und zwar gemäß den Festlegungen in Anlage 2.

4.2. Der Auftragsverarbeiter arbeitet nachweislich im Einklang mit DIN ISO/IEC 27001 und hat für die Verarbeitung personenbezogener Daten entsprechend formulierte Sicherheitsvorgaben implementiert, in denen in jedem Fall die in Absatz 1 dieses Artikels 4 genannten Maßnahmen dargelegt sind.

4.3. Der Auftragsverarbeiter erfüllt nachweislich die Sicherheitsanforderungen für Netzwerkverbindungen gemäß den Vorgaben in der DIN ISO/IEC27001.

4.4. Der Auftragsverarbeiter erfüllt nachweislich die Anforderungen bezüglich der Protokollierung gemäß den Vorgaben in der DIN ISO/IEC27001.

4.5. Der Auftragsverarbeiter erfüllt nachweislich die Anforderungen aus der DIN ISO/IEC27001, sofern deren Geltung für das Gesundheitswesen erklärt wurde.

4.6. Der Auftragsverarbeiter legt auf erstes Verlangen des Verantwortlichen eine von einem unabhängigen und diesbezüglich sachverständigen Dritten ausgefertigte gültige Bescheinigung vor (wenn er darüber verfügt), aus der hervorgeht, dass der Auftragsverarbeiter die Verpflichtungen aus diesem Artikel einhält.

4.7. Der Verantwortliche hat das Recht, die Einhaltung der oben in den Artikeln 4.1 bis 4.4 genannten Maßnahmen zu beaufsichtigen bzw. beaufsichtigen zu lassen. Der Auftragsverarbeiter gibt dem Verantwortlichen auf dessen Verlangen in jedem Fall einmal jährlich zu einem von den Vertragsparteien in gegenseitiger Absprache festzulegenden Zeitpunkt sowie darüber hinaus, wenn sich der Verantwortliche im Zusammenhang mit (mutmaßlichen) Informations- und Datenschutz-Vorkommnissen dazu veranlasst sieht, die Gelegenheit, dies zu kontrollieren bzw. kontrollieren zu lassen. Der Auftragsverarbeiter hat an einer solchen Überprüfung in angemessener Weise mitzuwirken. Der Auftragsverarbeiter befolgt eventuelle berechtigte Anweisungen des Verantwortlichen zur Anpassung der Sicherheitsvorgaben im Zusammenhang mit einer solchen Überprüfung innerhalb einer angemessenen Frist.

4.8. Die Vertragsparteien erkennen an, dass Sicherheitsanforderungen einem ständigen Wandel unterliegen und dass ein wirksamer Schutz häufige Evaluierungen und regelmäßige Verbesserungen veralteter Sicherheitsvorkehrungen erfordert. Der Auftragsverarbeiter evaluiert deshalb regelmäßig die aufgrund dieses Artikels 4 implementierten Maßnahmen und verbessert die Maßnahmen gegebenenfalls, damit die in diesem Artikel 4 genannten Verpflichtungen dauerhaft erfüllt werden. Die vorangegangenen Bestimmungen lassen die Weisungsbefugnis des Verantwortlichen unberührt, gegebenenfalls zusätzliche Maßnahmen zu treffen bzw. treffen zu lassen.

Artikel 5. Überwachung, Informationspflichten und Vorkommnis-Management

5.1. Der Auftragsverarbeiter überwacht die Sicherheitsvorkehrungen aktiv auf Verletzungen hin und erstattet dem Verantwortlichen gegenüber im Einklang mit diesem Artikel 5 Bericht bezüglich der Ergebnisse der Überwachung.

5.2. Sobald ein Vorkommnis eintritt, eingetreten ist oder eintreten könnte, ist der Auftragsverarbeiter verpflichtet, den Verantwortlichen darüber unverzüglich in Kenntnis zu setzen und dabei zu folgenden Punkten sämtliche relevante Informationen zu übermitteln:

1) Art des Vorkommnisses

2) die (möglicherweise) betroffenen personenbezogenen Daten

3) die festgestellten und die vermutlichen Folgen des Vorkommnisses sowie

4) die Maßnahmen, die getroffen wurden oder werden, um das Vorkommnis zu beseitigen bzw. dessen Folgen/Schäden möglichst weitgehend zu begrenzen.

5.3. Der Auftragsverarbeiter ist unbeschadet seiner sonstigen Verpflichtungen aus diesem Artikel verpflichtet, Maßnahmen zu treffen, die berechtigterweise von ihm erwartet werden können, um das Vorkommnis möglichst umgehend zu beseitigen bzw. die weiteren Folgen möglichst zu begrenzen. Der Auftragsverarbeiter hält unverzüglich Rücksprache mit dem Verantwortlichen, um diesbezüglich konkrete Absprachen zu treffen.

5.4. Der Auftragsverarbeiter arbeitet jederzeit mit dem Verantwortlichen zusammen, befolgt die Anweisungen des Verantwortlichen und ermöglicht es dem Verantwortlichen, eine eingehende Untersuchung des Vorkommnisses durchzuführen, bezüglich des Vorkommnisses eine angemessene Reaktion zu formulieren und geeignete Folgeschritte zu unternehmen, darunter auch die Benachrichtigung der deutschen Datenschutzbehörde und/oder der betroffenen Person im Sinne von Artikel 5.8.

5.5. Der Auftragsverarbeiter hält jederzeit schriftliche Verfahren vor, die es ihm ermöglichen, dem Verantwortlichen sofort eine Reaktion zu einem Vorkommnis zu übermitteln und zur Abwicklung des Vorkommnisses effektiv mit dem Verantwortlichen zusammenzuarbeiten. Der Auftragsverarbeiter übermittelt dem Verantwortlichen auf dessen Verlangen eine Zweitschrift dieser Verfahren.

5.6. Meldungen, die aufgrund von Artikel 5.2 erfolgen, werden unverzüglich an den Verantwortlichen gerichtet oder bei Notwendigkeit an einen vom Verantwortlichen während der Dauer der vorliegenden Datenverarbeitungsvereinbarung schriftlich mitgeteilten Mitarbeiter des Verantwortlichen. Wenn der Verantwortliche einen Datenschutzbeauftragten eingesetzt hat, werden die Meldungen an diesen Datenschutzbeauftragten geschickt.

5.7. Dem Auftragsverarbeiter ist es nicht gestattet, betroffenen Personen oder anderen Drittparteien Informationen zu Vorkommnissen zu erteilen, außer, der Auftragsverarbeiter ist gesetzlich dazu verpflichtet, oder die Vertragsparteien haben diesbezüglich etwas anderes vereinbart. Die Regelungen des Art. 33 DSGVO bleiben unberührt.

5.8. Wenn und sofern die Vertragsparteien vereinbart haben, dass der Auftragsverarbeiter im Zusammenhang mit einem Vorkommnis unmittelbaren Kontakt zu den Behörden oder anderen Drittparteien unterhält, setzt der Auftragsverarbeiter den Verantwortlichen darüber fortlaufend in Kenntnis.

Artikel 6. Mitwirkungspflichten

6.1. Die DSGVO und andere (Datenschutz-) Gesetze sprechen der betroffenen Person bestimmte Rechte zu. Der Auftragsverarbeiter unterstützt den Verantwortlichen umfassend und zeitnah bei der Erfüllung der Verpflichtungen, die sich für den Verantwortlichen aufgrund dieser Rechte ergeben.

6.2. Eine beim Auftragsverarbeiter eingehende Beschwerde oder eine Anfrage einer betroffenen Person bezüglich der Verarbeitung personenbezogener Daten leitet der Auftragsverarbeiter unverzüglich an den Verantwortlichen weiter.

6.3. Auf erstes Verlangen des Verantwortlichen diesbezüglich übermittelt der Auftragsverarbeiter dem Verantwortlichen sämtliche relevanten Informationen bezüglich der Aspekte der von ihm vollzogenen Verarbeitung personenbezogener Daten, damit der Verantwortliche auch anhand dieser Informationen nachweisen kann, dass die geltenden (Datenschutz-) Gesetze eingehalten werden.

6.4. Der Auftragsverarbeiter bietet auf erstes Verlangen des Verantwortlichen ferner alle erforderliche Unterstützung bei der Einhaltung der sich aufgrund des geltenden Datenschutzrechts für den Verantwortlichen ergebenden gesetzlichen Verpflichtungen (wie etwa die Durchführung einer Datenschutz-Folgenabschätzung).

Artikel 7. Beauftragung von Unterauftragsverarbeitern

7.1. Der Verantwortliche gewährt dem Auftragsverarbeiter das Recht, Aktivitäten (darunter Aktivitäten der Verarbeitung personenbezogener Daten und solche, für deren Ausführung die Verarbeitung personenbezogener Daten notwendig ist), (teils) durch andere als die in Anlage 1 aufgeführten Unterauftragsverarbeiter durchführen zu lassen, worüber der Auftragsverarbeiter den Verantwortlichen stets vor Beginn der Aktivitäten informiert. Der Verantwortliche hat das Recht, Widerspruch gegen den Einsatz eines Unterauftragsverarbeiters einzulegen, in welchem Falle der Verantwortliche und Auftragsverarbeiter zusammen nach einer passenden Lösung suchen werden. Sollte keine passende Lösung gefunden werden, hat der Verantwortliche das Recht, die Verträge mit dem Auftragsverarbeiter unverzüglich zu beenden.

7.2. Der Auftragsverarbeiter erlegt dem Unterauftragsverarbeiter die gleichen oder strengere Verpflichtungen auf, wie sie für ihn selbst aus der vorliegenden Datenverarbeitungsvereinbarung sowie dem geltenden Gesetz erwachsen. Der Auftragsverarbeiter hält diese Vereinbarungen schriftlich fest und überwacht deren Einhaltung durch den Unterauftragsverarbeiter. Der Auftragsverarbeiter übermittelt dem Verantwortlichen auf Verlangen eine Zweitschrift der mit dem Unterauftragsverarbeiter geschlossenen Verträge.

7.3. Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen weiterhin uneingeschränkt für die Folgen der Beauftragung eines Unterauftragsverarbeiters. Die Zustimmung des Verantwortlichen zur Beauftragung eines Unterauftragsverarbeiters mit entsprechenden Arbeiten lässt unberührt, dass für den Einsatz von Unterauftragsverarbeitern in einem Land außerhalb des Europäischen Wirtschaftsraums eine Zustimmung im Einklang mit Artikel 3.7 der vorliegenden Datenverarbeitungsvereinbarung erforderlich ist.

Artikel 8. Haftung

8.1. Die Vertragsparteien tragen jeweils die Verantwortung für ihr eigenes Handeln.

8.2. Etwaige Beschränkungen der Haftung im Vertrag gelten mutatis mutandis auch für die vorliegende Datenverarbeitungsvereinbarung, und zwar in folgender Weise:

a) Eventuelle (implizite oder explizite) Haftungsausschlüsse für Verlust und/oder Manipulation von personenbezogenen Daten sind ausgeschlossen.

b) Eventuelle (implizite oder explizite) Haftungsausschlüsse für Bußgelder, die von der Datenschutzbehörde AP oder einem anderen Aufsichtsorgan auferlegt werden und in unmittelbarem Zusammenhang mit einem zurechenbaren Mangel, einem zurechenbaren Verhalten oder Versäumnis des Auftragsverarbeiters stehen, sind ausgeschlossen.

8.3. Der Auftragsverarbeiter schützt und entschädigt den Verantwortlichen gegenüber sämtlichen Forderungen, Maßnahmen, Ansprüchen Dritter sowie Bußgeldern der Datenschutzbehörde, die sich unmittelbar ergeben aus einem zurechenbaren Mangel des Auftragsverarbeiters und/oder dessen Subunternehmern/Unterauftragsverarbeitern bezüglich der Einhaltung seiner Verpflichtungen aus der vorliegenden Datenverarbeitungsvereinbarung und/oder einer Verletzung der geltenden Gesetze im Bereich der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter und/oder dessen Subunternehmer/Unterauftragsverarbeiter.

8.4. Sofern die Vertragsparteien gegenüber Dritten, darunter die betroffene Person, gesamtschuldnerisch haften oder die Datenschutzbehörde ihnen gemeinsam ein Bußgeld auferlegt, sind sie jeweils für den Anteil der

Schuld, der ihnen im Verhältnis untereinander zukommt, verpflichtet, sich gemäß den Bestimmungen der Gesamtschuld (§ 431 BGB) an Schulden und Kosten zu beteiligen, es sei denn, in der DSGVO ist etwas anderes festgelegt. In diesem Fall gilt die DSGVO vorrangig.

8.5. Sofern im Vertrag keine Haftungsbeschränkung für den Verantwortlichen enthalten ist, gilt die in Absatz 2 enthaltene Beschränkung für den Auftragsverarbeiter auch für den Verantwortlichen.

8.6. Jedwede Haftungsbeschränkung entfällt für die betreffende Vertragspartei im Falle von Vorsatz oder grober Fahrlässigkeit seitens der betreffenden Vertragspartei.

8.7. Die Vertragsparteien kümmern sich um eine ausreichende Deckung der Haftung.

Artikel 9. Kosten

9.1. Bezüglich der Kosten für die Verarbeitung von Daten, die mit der normalen Erfüllung des Vertrags verbunden sind, gilt, dass diese in den bereits im Rahmen des Vertrags zu zahlenden Entgelten enthalten sind.

9.2. Etwaige Unterstützungen oder andere ergänzende Leistungen, die der Auftragsverarbeiter aufgrund der vorliegenden Datenverarbeitungsvereinbarung zu erbringen hat oder um die der Verantwortliche ersucht, darunter sämtliche Ersuchen um zusätzliche Informationen, werden gegenüber dem Verantwortlichen gemäß den in 0 aufgeschlüsselten Tarifen in Rechnung gestellt.

Artikel 10. Dauer und Beendigung

10.1. Die vorliegende Datenverarbeitungsvereinbarung beginnt im Moment des erstmaligen Inanspruchnehmens von Leistungen des Auftragsverarbeiters durch den Verantwortlichen und dauert solange an wie der Auftragsverarbeiter Leistungen für den Verantwortlichen erbringt, in dessen Rahmen der Auftragsverarbeiter personenbezogene Daten für den Verantwortlichen verarbeitet.

10.2. Die Datenverarbeitungsvereinbarung ist integraler und untrennbarer Bestandteil des Vertrags. Eine Beendigung des Vertrags hat, ungeachtet des Grundes der Beendigung (Kündigung, Auflösung), zur Folge, dass auch die Datenverarbeitungsvereinbarung aus demselben Grund beendet wird (und umgekehrt), es sei denn, die Vertragsparteien haben in diesem Fall etwas anderes vereinbart.

10.3. Verpflichtungen, die ihrer Art nach für eine Fortdauer auch nach Beendigung der vorliegenden Datenverarbeitungsvereinbarung vorgesehen sind, behalten nach Beendigung der vorliegenden Datenverarbeitungsvereinbarung ihre Geltung. Dazu gehören beispielsweise die Bestimmungen, die sich aus den Bestimmungen bezüglich Vertraulichkeit, Haftung, Streitbeilegung und anwendbares Recht ergeben.

10.4. Die Vertragsparteien haben unbeschadet der Bestimmungen diesbezüglich im Vertrag jeweils das Recht, die Erfüllung der vorliegenden Datenverarbeitungsvereinbarung und des damit zusammenhängenden Vertrags auszusetzen bzw. ohne gerichtliches Eingreifen mit sofortiger Wirkung zu kündigen, wenn:

a) die andere Vertragspartei aufgelöst wird oder anderweitig aufhört zu existieren;

b) die andere Vertragspartei der Erfüllung ihrer Verpflichtungen aus der vorliegenden Datenverarbeitungsvereinbarung nachweislich [ernsthaft] nicht nachkommt und dieser zurechenbare Mangenach einer entsprechenden schriftlichen Mahnung nicht innerhalb von 30 Tagen behoben wurde;

c) eine Vertragspartei für insolvent erklärt wird oder gesetzlichen Zahlungsaufschub beantragt und dadurch die Erfüllung der Datenverarbeitungsvereinbarung gefähreded ist.

10.5. Angesichts der großen Abhängigkeit des Verantwortlichen vom Auftragsverarbeiter sowie des Kontinuitätsrisikos bei Vorkommnissen und Schwierigkeiten (wie etwa Insolvenz) erklärt der Auftragsverarbeiter sich bereits jetzt bereit, zur Verringerung der genannten Risiken auf erstes Verlangen des Verantwortlichen zusätzliche Vereinbarungen mit dem Verantwortlichen zu treffen. Diese zusätzlichen Vereinbarungen können unter anderem bestehen aus:

a) Vereinbarungen über regelmäßige Rückübermittlungen oder die Übermittlung an eine dritte Partei der vom Auftragsverarbeiter verarbeiteten Daten; und/oder

b) der Abschluss einer Vereinbarung mit einer dritten Partei, die dahingehend lautet, dass die betreffende dritte Partei sich gesamtschuldnerisch verpflichtet oder einsteht für die Erfüllung des Vertrags; und/oder

c) der Abschluss einer (dreiseitigen) Vereinbarung mit einer dritten Partei, die dahingehend lautet, dass die betreffende dritte Partei (dauerhaft) sämtliche erforderlichen Daten erhält, um gegebenenfalls die aufgrund des Vertrags zu erbringenden Leistungen (oder einen Teil davon) – gegebenenfalls auf der Grundlage eines neuen Vertrag – anstelle des Auftragsverarbeiters oder parallel zu diesem erbringen zu können.

10.6. Der Auftragsverarbeiter besitzt einen Ausstiegsplan bezüglich der Erfüllung sämtlicher Verpflichtungen aus der vorliegenden Datenverarbeitungsvereinbarung für den Fall, dass der Vertrag oder die Datenverarbeitungsvereinbarung (zwischenzeitlich) beendet wird. Der Auftragsverarbeiter übermittelt auf erstes Verlangen des Verantwortlichen eine Zweitschrift dieses Plans.

10.7. Der Verantwortliche hat das Recht, die vorliegende Datenverarbeitungsvereinbarung sowie den Vertrag mit sofortiger Wirkung zu kündigen, wenn der Auftragsverarbeiter zu erkennen gibt, dass er die Zuverlässigkeitsanforderungen, die aufgrund von Entwicklungen des Gesetzes und/oder der Rechtsprechung an die Verarbeitung personenbezogener Daten gestellt werden, nicht (länger) erfüllen kann.

10.8. Der Auftragsverarbeiter hat den Verantwortlichen über eine beabsichtigte Übernahme oder eine Eigentumsübertragung im Vorfeld rechtzeitig zu informieren.

10.9. Dem Auftragsverarbeiter ist es ohne ausdrückliche schriftliche Zustimmung des Verantwortlichen nicht gestattet, die vorliegende Datenverarbeitungsvereinbarung sowie die Rechte und Pflichten, die mit der vorliegenden Datenverarbeitungsvereinbarung zusammenhängen, an eine dritte Partei zu übertragen.

Artikel 11. Aufbewahrungsfristen, Rückgabe und Vernichtung personenbezogener Daten

11.1. Der Auftragsverarbeiter bewahrt die personenbezogenen Daten nicht länger auf als unbedingt erforderlich. Berücksichtigt werden dabei die gesetzlichen Aufbewahrungsfristen oder eine eventuell zwischen den Vertragsparteien getroffene Vereinbarung über Aufbewahrungsfristen gemäß den Festlegungen in Anhang 1. Unter keinen Umständen bewahrt der Auftragsverarbeiter die personenbezogenen Daten länger auf als bis zum Ende der vorliegenden Datenverarbeitungsvereinbarung. Der Verantwortliche legt fest, ob und – wenn ja – wie lange Daten aufbewahrt werden müssen.

11.2. Bei Beendigung der Datenverarbeitungsvereinbarung bzw. – wenn zutreffend – am Ende der vereinbarten Aufbewahrungsfristen bzw. auf schriftliches Verlangen des Verantwortlichen vernichtet der Auftragsverarbeiter zu angemessenen Kosten die personenbezogenen Daten unwiderruflich bzw. lässt sie unwiderruflich vernichten oder gibt sie an den Verantwortlichen zurück. Über Vernichtung oder Rückgabe entscheidet der Verantwortliche. Auf Verlangen des Verantwortlichen übermittelt der Auftragsverarbeiter einen Beweis dafür, dass die Daten unwiderruflich vernichtet oder gelöscht wurden. Eine eventuelle Rückgabe der Daten erfolgt in

einem allgemein üblichen, strukturierten und dokumentierten Datenformat auf elektronischem Weg. Wenn Rückgabe, unwiderrufliche Vernichtung oder Löschung nicht möglich sind, setzt der Auftragsverarbeiter den Verantwortlichen davon unverzüglich in Kenntnis. In diesem Fall garantiert der Auftragsverarbeiter, dass er die personenbezogenen Daten vertraulich behandelt und nicht länger verarbeitet.

Artikel 12. Rechte an geistigem Eigentum

12.1. Sofern die (Sammlung der) personenbezogenen Daten durch etwaige Rechte an geistigem Eigentum geschützt sind (ist), erteilt der Verantwortliche dem Auftragsverarbeiter seine Zustimmung, die personenbezogenen Daten im Rahmen der Erfüllung der vorliegenden Datenverarbeitungsvereinbarung zu verwenden.

Artikel 13. Schlussbestimmungen

13.1. Die in der Präambel enthaltenen Umstände sind Bestandteil der vorliegenden Datenverarbeitungsvereinbarung.

13.2. Im Falle der Nichtigkeit bzw. Anfechtbarkeit einer oder mehrerer Bestimmungen aus der vorliegenden Datenverarbeitungsvereinbarung bleiben die übrigen Bestimmungen uneingeschränkt in Kraft.

13.3. In allen Fällen, die in der vorliegenden Datenverarbeitungsvereinbarung nicht berücksichtigt sind, entscheiden die Vertragsparteien nach gegenseitiger Rücksprache.

13.4. Diese Datenverarbeitungsvereinbarung unterliegt dem deutschen Recht.

13.5. Die Vertragsparteien bemühen sich, Konflikte in gegenseitiger Absprache zu lösen. Dazu gehört auch die Möglichkeit, die Streitsache durch eine in gegenseitiger Absprache festzulegende Mediation oder ein entsprechendes Schiedsverfahren beizulegen.

13.6. Streitsachen bezüglich der vorliegenden Datenverarbeitungsvereinbarung oder im Zusammenhang damit werden ausschließlich dem im Vertrag genannten Gericht oder Schiedsrichter vorgelegt.

Anlage 1: Beschreibung der personenbezogenen Daten, Art der Verarbeitung usw.

Diese Datenverarbeitungsvereinbarung bildet einen Anhang zu folgenden Verträgen und bezieht sich auf die folgenden Verarbeitungsformen personenbezogener Daten.

Vertrag	Der Vertrag ist durch Unterzeichnung des Angebots oder durch die Inanspruchnahme eines Demokontos zustande gekommen.
Kurzbeschreibung der Leistungen	Die Bereitstellung einer E-Health-Plattform für Diagnostik, Wirkungsmessung und Behandlung von psychischen und physischen Problemen.
Art der Verarbeitung	Verarbeitung von Patienten- und Kundendaten
Art der personenbezogenen Daten	Kontaktdaten Vertragsdaten (Vertragsverhältnis, Produkte und Leistungen usw.) Finanzdaten, medizinische Daten, Kommunikationsdaten (E-Mail und Chat) sowie sonstige Daten, die Patienten und medizinisches Personal bei der Verwendung des Programms eingeben
Kategorien betroffener Personen	Medizinisches Personal, Mitarbeiter, Patienten, Familienangehörige, Freunde und sonstige Bekannte sowie Personen, zu denen Patient oder medizinisches Personal bei der Nutzung des Programms Informationen eingeben.
Zweck der Verarbeitung	Diagnostik, Wirkungsmessung und Behandlung von psychischen und/oder körperlichen Problemen.
Genehmigte Unterauftragsverarbeiter	• Centron GmbH (Hostingprovider): www.centron.de, Heganger 29, D-96103 Hallstadt, Deutschland • AFAS (Verarbeitung von Kundendaten für Rechnungsstellung): www.afas.nl, Philipsstraat 9, 3833 LC Leusden, Niederlande • Stepco (Datensicherungen der Büroumgebung, einschließlich E-Mails): www.stepco.nl, Aziëstraat 15, 6014 DA Ittervoort, Niederlande • Alterdesk (Videoanrufe und Chat): www.alterdesk.com, Comeniusstraat 5, 1817 MS, Alkmaar, Niederlande • Zivver: Verschlüsselte und gesicherte E-Mail-Kommunikation (www.zivver.nl) • Spryng: SMS-Authentifizierung (www.spryng.nl) • FreshMail: Newsletter für Kunden (www.freshmail.com)
Vereinbarungen zu Aufbewahrungsfristen	Daten des Verantwortlichen (und seiner Kunden/Patienten) werden während der gesamten Vertragslaufzeit aufbewahrt, es sei denn, der Verantwortliche veranlasst die Löschung dieser daten. Nach Beendigung des Vertrags werden diese Daten von der Datenbank des Auftragsverarbeiters, und innerhalb von drei Monaten automatisch aus den Back-Ups des Auftragsverarbeiters gelöscht. Daten des Auftragsverarbeiters werden gemäß der jeweiligen gesetzlichen Fristen und Rahmenbedigungen aufbewahrt.

Anlage 2: Beschreibung der konkreten Sicherheitsvorkehrungen

Gebäude
Technische und organisatorische Maßnahmen, mit denen der physische Zugang zu den Gebäuden, in denen die Datenverarbeitung erfolgt, durch Unbefugte verhindert werden soll:

- Türsicherung (elektrischer Türöffner mit Zugangskennung und protokollierter Schlüsselzuweisung)
- Videoüberwachung mit Bewegungssensor und Aufnahmefunktion
- Einbruchsalarmsystem mit anschließender Überprüfung durch Sicherheitsdienst

Netzwerk und Computer
Technische und organisatorische Maßnahmen, mit denen der Zugang zu Netzwerk und Computern des Auftragsverarbeiters durch Unbefugte verhindert werden soll:

- Auf allen Arbeitsplatzcomputern wird Festplattenverschlüsselung eingesetzt.
- Jeder Arbeitsplatzcomputer ist mit Anti-Virus-Software ausgestattet, die automatisch aktualisiert wird.
- Computer werden automatisch aktualisiert, sobald Sicherheits-Updates zur Verfügung stehen.
- Anmeldung mit Benutzername und Passwort.
- Passwortzuweisung und -vorgaben (einschließlich Vorgaben bezüglich Länge und Komplexität).
- Passwörter dürfen ausschließlich in einem digitalen (Offline-) Passworttresor aufbewahrt werden.
- Computer werden nach einer gewissen Zeit der Inaktivität automatisch gesperrt.
- Einsatz differenzierter Autorisierungen.
- Nur Administratoren können Software installieren/deinstallieren.
- Zahl der Administratoren ist auf das „unbedingt Notwendige“ beschränkt.
- Protokoll von Zugang und Aktionen aller Nutzer.
- Die Nutzung von Datenträgern oder E-Mail für sensible Daten ist nur gestattet, sofern dies notwendig ist, auf Verlangen des Verantwortlichen und angemessen verschlüsselt (AES-256 oder stärker).
- Die Netzwerke werden mit einer Firewall geschützt.
- Das Unternehmensnetzwerk ist vom Gastnetzwerk getrennt.

Programm
Technische und organisatorische Maßnahmen, mit denen der Zugang zum Programm, mit dem die personenbezogenen Daten verarbeitet werden, durch Unbefugte verhindert werden soll:

- Die gesamte Datenübertragung mit dem Programm erfolgt verschlüsselt.
- Anmeldung mit Benutzername und Passwort.
- Passwortzuweisung und -vorgaben (einschließlich Vorgaben bezüglich Länge und Komplexität).
- Optionen für Zwei-Faktor-Authentifizierung.
- Optionen für IP-Beschränkungen.
- Einsatz differenzierter Autorisierungen (mit Kunde, Rollen und Genehmigungen).
- Zahl der Administratoren ist auf das „unbedingt Notwendige“ beschränkt.
- Protokoll von Zugang und Aktionen aller Nutzer.
- Automatische Abmeldung nach einer gewissen Zeit der Inaktivität.
- Automatische Sperrung nach zu vielen falschen Anmeldeversuchen.
- Serverzugriff anhand IP-Adresse geschützt.
- Auftragsverarbeiter hat Protokolle für (Weiter-) Entwicklung und Administration des Programms.
- Die Sicherheit des Programms wird in der Praxis regelmäßig durch unabhängige Parteien getestet.

Programmentwicklung
Technische und organisatorische Maßnahmen, die der Auftragsverarbeiter bei der (Weiter-) Entwicklung des Programms trifft:

- Sicherheitsanforderungen werden bei der Erstellung der Spezifikationen festgelegt.
- Sicherheitsanforderungen werden in Testscripts integriert und getestet.
- Regressionstests werden in Testscripts integriert und ausgeführt.
- Die gesamte Datenübertragung vom/zum Programm erfolgt verschlüsselt.
- Authentifizierung und Autorisierung werden regelmäßig geprüft.
- Die Eingabe von Daten wird immer validiert.
- Die Ausgabe von Daten wird immer validiert und bereinigt, um ungültige oder unzutreffende Ausgaben zu vermeiden.
- Genehmigungen werden möglichst defensiv eingestellt.
- Programmcode wird möglichst defensiv entwickelt.
- Die Protokollierung wird bei Bedarf erweitert.
- Review-Verfahren für die Implementierung des Programmcodes von Drittanbietern.
- Der entwickelte Programmcode wird von anderen Personen überprüft und nicht von den Entwicklern des Programmcodes selbst.
- Entwickelter Programmcode wird von zwei verschiedenen Personen getestet, die den Programmcode nicht selbst entwickelt haben.
- Beanstandeter Programmcode, der angepasst wurde, wird erneut einer Überprüfung und Tests unterzogen.
- Es gibt getrennte Umgebungen für Entwicklung, Test, Genehmigung und produktiven Einsatz.
- Personenbezogene Daten aus dem produktiven Einsatz werden nicht für Entwicklung, Test und Genehmigung verwendet.

Beschäftigte
Maßnahmen, denen die Beschäftigten des Auftragsverarbeiters nachkommen müssen:

- Die Beschäftigten erhalten Schulungen im Bereich Datenschutz und Informationssicherheit.
- Die Beschäftigten haben eine Vertraulichkeitserklärung unterschrieben.
- Die Beschäftigten haben bei Beschäftigungsantritt ein Führungszeugnis vorzulegen.
- Die Beschäftigten sind gebunden an Verhaltensregeln für verantwortliche Nutzung von Programm, Gebäuden, Computern, Druckern, E-Mail und Internet des Auftragsverarbeiters.
- Die Beschäftigten haben (potenzielle) Sicherheitsvorkommnisse dem Sicherheitsverantwortlichen („Security Officer“) zu melden.

Verfügbarkeit
Technische und organisatorische Maßnahmen, mit denen die Verfügbarkeit der Systeme und Programme des Auftragsverarbeiters gewährleistet werden:

- Systeme, auf denen das Programm des Auftragsverarbeiters läuft, sind bei einem nach DIN ISO/IEC27001zertifizierten Provider untergebracht.
- Systeme, auf denen das Programm des Auftragsverarbeiters läuft, sind skalierbar.
- Systeme, auf denen das Programm des Auftragsverarbeiters läuft, sind redundant ausgelegt.
- Systeme, auf denen das Programm des Auftragsverarbeiters läuft, verfügen über eine Notstromversorgung.
- Systeme, auf denen das Programm des Auftragsverarbeiters läuft, sind ausschließlich für die Administratoren des Providers zugänglich.
- Der Provider setzt in den Server-Räumen Klimatisierung ein.
- Der Provider setzt in den Server-Räumen Brand- und Rauchmeldeanlagen ein.
- Der Provider setzt für die Systeme des Auftragsverarbeiters (pro-) aktives Monitoring ein.
- Der Provider macht tägliche Snapshots der gesamten Programmumgebung des Auftragsverarbeiters.
- Der Provider macht tägliche Datensicherungen der gesamten Programmumgebung des Auftragsverarbeiters.
- Der Auftragsverarbeiter macht täglich eine externe Datensicherung der Programmumgebung.
- Datensicherungen werden drei Monate lang aufbewahrt.

- Der Auftragsverarbeiter bewahrt Daten des Verantwortlichen unbefristet auf und vernichtet sie erst bei Beendigung des Vertrags des Verantwortlichen mit dem Auftragsverarbeiter.
- Der Auftragsverarbeiter testet regelmäßig die Wiederherstellung der Datensicherung.
- Der Auftragsverarbeiter setzt für seine Programme (pro-) aktives Monitoring ein.
- Der Auftragsverarbeiter hat einen Plan zur Aufrechterhaltung des Geschäftsbetriebs (Business Continuity Plan) erstellt.

Anlage 3: Aufschlüsselung der Tarife

Der Stundensatz beträgt 100,– € zzgl. Mehrwertsteuer.