

Vereinbarung

zwischen dem

RehaVitalisPlus e.V.

- Verantwortlicher - nachstehend Auftraggeber genannt -

und dem/der

.....

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

Präambel

Die Parteien haben einen Vertrag geschlossen, zu dessen Erfüllung der Auftragnehmer den Zugang zu personenbezogenen Daten des Auftraggebers benötigt und dem Auftragnehmer diesen Zugang ermöglicht. Zum Schutze der Persönlichkeitsrechte der Betroffenen im Sinne der Europäischen Grundverordnung (EU) 2016/679 (DS-GVO) und des Bundesdatenschutzgesetzes (BDSG) schließen die Parteien nun die nachfolgende Datenschutzvereinbarung („Datenschutzvereinbarung“).

Diese Datenschutzvereinbarung kann auch für zukünftige Verträge, welche die Verarbeitung von Daten im Auftrag des Auftraggebers durch den Auftragnehmer beinhalten, verwendet werden.

Hierzu muss in einem Vertrag auf diese Datenschutzvereinbarung ausdrücklich Bezug genommen werden und jeweils gesonderte Anlagen 1 (technische und organisatorische Sicherheitsmaßnahmen) zu dieser Datenschutzvereinbarung je Einzelvertrag, welcher die Verarbeitung von Daten im Auftrag des Auftraggebers durch den Auftragnehmer beinhaltet, ausgefüllt werden. Bestehende Verträge werden die Parteien entsprechend anpassen.

1. Gegenstand und Dauer des Auftrags

(1) Vertragsparteien

Parteien dieser Datenschutzvereinbarung sind RehaVitalisPlus e.V. und [Auftragnehmer].

(2) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus dem Kooperationsvertrag, auf den hier verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: (Definition der Aufgaben)

(3) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder (insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)

Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum

oder

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von zum gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

Zweck dieser Datenschutzvereinbarung ist es, den Betroffenen (im Sinne der o. g. Gesetze) davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Die Parteien sind sich darüber einig, dass die Bestimmungen dieser Datenschutzvereinbarung Vorrang haben vor allen anderen Bestimmungen in bestehenden und zukünftigen Hauptverträgen, welche die Verarbeitung von Daten im Auftrag des Auftraggebers durch den Auftragnehmer beinhalten und allen anderen zwischen den Parteien abgeschlossenen Hauptverträgen, soweit der Vertragsgegenstand betroffen ist.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung.

oder

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich 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 des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. Das angemessene Schutzniveau in

ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);

- wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i. V. m. 47 DS-GVO);
- wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO);
- wird hergestellt durch genehmigte Verhaltensregeln (Art 46 Abs. 2 lit. e i. V. m. 40 DS-GVO);
- wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i. V. m. 42 DS-GVO).
- wird hergestellt durch sonstige Maßnahmen: (Art. 46 Abs 2 lit. a, Abs. 3 litt. a und b DS-GVO)

(2) Art der Daten

- Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter:

oder

- Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)
 - Personenstammdaten
 - Kommunikationsdaten (z.B. Telefon, E-Mail)
 - Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
 - Kundenhistorie
 - Vertragsabrechnungs- und Zahlungsdaten
 - Planungs- und Steuerungsdaten
 - Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
 - Gesundheitsdaten (Angaben zur Rehabilitation)
 - ...

(3) Kategorien betroffener Personen

- Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter:

oder

- Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
 - Kunden
 - Interessenten
 - Abonnenten
 - Beschäftigte
 - Lieferanten
 - Handelsvertreter

- Ansprechpartner
 ...

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.
- Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
 - Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

- Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.
- b) Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] benannt.
- c) Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DS-GVO in der Union: [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail].
- d) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- e) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].
- f) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- g) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- h) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- i) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- j) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.
- k) In dringenden Fällen kann sich der Auftraggeber direkt an den DSB wenden.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleis-

tungen, die der Auftragnehmer z. B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

- a) Eine Unterbeauftragung ist unzulässig.
- b) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma Unterauftragnehmer	Anschrift/Land	Leistung

- c) Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:
 - der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
 - der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
 - eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

- (5) Eine weitere Auslagerung durch den Unterauftragnehmer
- ist nicht gestattet;
 - bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);
 - bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);

sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

- a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
- b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
- c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
- d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgeabschätzung
- e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhandigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Haftung und Rechte Dritter

(1) Soweit der Auftraggeber zum Ausgleich eines Schadens gegenüber dem Betroffenen verpflichtet ist, bleibt es ihr vorbehalten, den Auftragnehmer nach den allgemeinen Vorschriften und aufgrund dieser Datenschutzvereinbarung in Anspruch zu nehmen.

(2) Der Auftraggeber behält sich das Recht vor, darüber hinausgehende Schäden gegenüber dem Auftragnehmer geltend zu machen, soweit diese Schäden vom Auftragnehmer (oder seinen Mitarbeitern, Erfüllungsgehilfen oder Unterauftragnehmern) verursacht wurden oder diese auf einem Verstoß von XX (oder ihren Mitarbeitern, Erfüllungsgehilfen oder Unterauftragnehmern) gegen dieser Datenschutzvereinbarung beruhen.

(3) Bei gerichtlichen Auseinandersetzungen mit Betroffenen hat der Auftraggeber das alleinige Entscheidungsrecht; der Auftragnehmer unterstützt den Auftraggeber durch Information und Beratung.

(4) Der Auftragnehmer ist verpflichtet, eine ausführliche Dokumentation der Datenverarbeitung und Nutzung zu führen, anhand derer der Auftraggeber den Nachweis über die ordnungsmäßige Durchführung der Datenverarbeitung und Nutzung führen kann.

12. Höhere Gewalt

Können durch Einwirkung höherer Gewalt, z. B. Krieg oder Unruhe, Streik oder Aussperrung, Naturkatastrophen, Epidemien oder Quarantäne, Maßnahmen der Regierung oder ähnliche Umstände ver-

tragliche Verpflichtungen nicht oder nicht rechtzeitig erfüllt werden, so ist die betreffende Vertragspartei während der Dauer der Einwirkung von der Einhaltung dieser Verpflichtung befreit. Die Parteien werden sich über Fälle höherer Gewalt gegenseitig unterrichten.

13. Sonstige Bestimmungen

(1) Die Abtretung dieser Datenschutzvereinbarung oder irgendwelcher Rechte und Pflichten daraus, ist ohne vorherige schriftliche Zustimmung durch die andere Partei nicht erlaubt.

(2) Änderungen und Ergänzungen zu dieser Datenschutzvereinbarung müssen als solche bezeichnet sein und bedürfen der Schriftform und der Unterschrift durch beide Vertragsparteien.

(3) Die Unwirksamkeit einer oder mehrerer Bestimmungen dieser Datenschutzvereinbarung berührt nicht die Wirksamkeit dieser Datenschutzvereinbarung im Übrigen. Die Parteien sind verpflichtet, eine unwirksame Bestimmung durch eine wirksame zu ersetzen, die dem mit der unwirksamen Bestimmung verfolgten wirtschaftlichen Zweck möglichst nahe kommt.

(4) Der Abschluss dieser Datenschutzvereinbarung verpflichtet keine der Parteien zum Abschluss weiterer Verträge, noch stellt diese Datenschutzvereinbarung eine Absichtserklärung im Hinblick auf den Abschluss weiterer Verträge dar.

(5) Auf diese Datenschutzvereinbarung findet ausschließlich das Recht der Bundesrepublik Deutschland Anwendung unter Ausschluss des Internationalen Privatrechts (Kollisionsrecht) und des UN Kaufrechts und das Recht, welches durch die DS-GVO begründet ist.

Gerichtsstand ist **Düsseldorf**.

In Streitfällen soll zunächst eine gütliche Einigung durch die Parteien angestrebt werden.

Düsseldorf, den **[Datum]**

[Ort], den **[Datum]**

RehaVitalisPlus e. V.

[Auftragnehmer]

.....

.....

.....

.....

BITTE AUSFÜLLEN!

Anlage 1 – Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle

Beispiele: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;

Ihre Maßnahmen:

- Zugangskontrolle

Beispiele: Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;

Ihre Maßnahmen:

- Zugriffskontrolle

Beispiele: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;

Ihre Maßnahmen:

- Trennungskontrolle

Beispiele: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;

Ihre Maßnahmen:

- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Beispiele: 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;

Ihre Maßnahmen:

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle

Beispiele: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

Ihre Maßnahmen:

-
- Eingabekontrolle

Beispiele: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

Ihre Maßnahmen:

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle

Beispiele: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;

Ihre Maßnahmen:

- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

Ihre Maßnahmen:

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Datenschutz-Management;

Ihre Maßnahmen:

- Incident-Response-Management;

Ihre Maßnahmen:

- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);

Ihre Maßnahmen:

- Auftragskontrolle

Beispiele: Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Ihre Maßnahmen:
