Auftragsdatenvereinbarung

zwischen dem/der

Praxis (siehe Stempel Seite 4)

- Verantwortlicher - nachstehend Auftraggeber genannt -

und

SoliPrax e.K., Inhaber Hans-Joachim Engels, Heilpraktiker, Max-Planck-Str. 27a , 50858 Köln

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

1. Gegenstand

Gegenstand dieser Vereinbarung ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers nach dessen Weisung.

2. Zwecke und Dauer der Datenverarbeitung

(1) Abrechnungsservice für die Praxis des Auftraggebers.

(2) Die Dauer der Datenverarbeitung entspricht der Laufzeit der Leistungsvereinbarung.

3. Arten personenbezogener Daten, Personenkategorien

Folgende personenbezogenen Daten werden vom Auftragnehmer zu den Zwecken der Rechnungsabwicklung verarbeitet:

- ☐ Personenstammdaten (Personal, Patienten)
- ☐ Patientendaten und Patientenhistorie
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung)
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Diagnosen nebst Zusatzkommentaren
- ☐ Behandlungsleistungen nebst Anmerkungen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☐ Rechnungsempfänger und Patienten
- ☐ Praxisinhaber und seine Mitarbeiter
- ☐ Mitarbeiter der SoliPrax e.K.
- ☐ externe Dienstleister (nur nach Auftragsdatenverarbeitung)

Der Zugriff auf die vorgenannten Daten durch den Auftragnehmer erfolgt gemäß dem Dienstleistungsvertrag

4. Verantwortlichkeit

Der Auftraggeber ist „Herr der Daten“ und für die Einhaltung der gesetzlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenverarbeitung und die Einhaltung etwaiger gesetzlicher Schweigepflichten (insbesondere § 203 StGB) verantwortlich. Die Verantwortung des Auftragnehmers in den in der DSGVO genannten Fällen bleibt unberührt.

5. Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Auftraggebers, sofern er nicht durch gesetzliche Bestimmungen, denen der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

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

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen die DSGVO oder gegen andere anwendbare Datenschutzbestimmungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

6. Transfer in Drittstaaten

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 Voraussetzungen der DSGVO erfüllt sind.

7. Pflichten des Auftragnehmers

Den Auftragnehmer treffen im Rahmen dieses Auftrages folgende Pflichten:

a) Der Auftragnehmer hat die Rene-Rautenberg GmbH als externen Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr Hans-Joachim Engels, Heilpraktiker, Max-Planck-Str. 27a, 50858 Köln benannt;

b) Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;

c) Der Auftragnehmer gewährleistet die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in Anlage];

d) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Maßnahmen der Aufsichtsbehörden, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch für etwaige Ordnungswidrigkeiten- oder Strafverfahren, soweit sie die Auftragsverarbeitung im Rahmen dieser Vereinbarung betreffen;

e) Der Auftragnehmer informiert den Auftraggeber unverzüglich, soweit es in seinem Einflussbereich zu Datenschutzverstößen oder Datenpannen kommt. Zudem informiert er den Auftraggeber über sonstige Umstände, die zur einer Gefährdung des Auftrags führen können (z.B. drohende Pfändung, Insolvenz);

f) Soweit der Auftraggeber seinerseits behördlichen Maßnahmen oder Ansprüchen Dritter im Zusammenhang mit der Auftragsverarbeitung ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen;

g) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Informationspflichten gegenüber den Aufsichtsbehörden, Datenschutz-Folgeabschätzungen und vorherige Konsultationen mit den Aufsichtsbehörden;

h) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Person nachzukommen;

i) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten.

8. Unterbeauftragungen

(1) Der Auftragnehmer nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Auftraggebers in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragnehmer den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

(2) Nimmt der Auftragnehmer die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in diesem Vertrag oder anderen Rechtsinstrument zwischen dem Auftraggeber und dem Auftragnehmer festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden muss, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

9. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, die Einhaltung der Pflichten des Auftragnehmers durch Kontrollen beim Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Kontrollen dürfen zu den üblichen Geschäftszeiten erfolgen und sind in der Regel rechtzeitig anzumelden sind.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen. Der Nachweis solcher Maßnahmen kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Prüfberichte unabhängiger Instanzen (z.B. Datenschutzauditoren));
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Kosten etwaiger Kontrollen trägt der Auftraggeber.

10. Sicherheitskopien, Löschung und Rückgabe von personenbezogenen Daten

(1) Der Auftragnehmer darf Sicherheitskopien erstellen, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind.

(2) Nach Abschluss der Erbringung der Verarbeitungsleistungen hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben, sofern nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

11. Kündigung

Das Recht zur Kündigung dieser Vereinbarung aus wichtigem Grund bleibt unberührt. Kündigungen bedürfen zu ihrer Wirksamkeit der Schriftform.

12. Schlussbestimmungen

(1) Änderungen und Ergänzungen des Vertrags bedürfen der Schriftform. Dies gilt auch für die Änderung oder Aufhebung dieser Klausel.

(2) Allgemeine Geschäftsbedingungen der Parteien finden auf diese Vereinbarung keine Anwendung.

(3) Auf diesen Vertrag ist ausschließlich das deutsche Recht anzuwenden.

(4) Ausschließlicher Gerichtsstand ist Köln, sofern jede Partei Kaufmann oder juristische Person des öffentlichen Rechts ist.

(5) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein, berührt dies die Gültigkeit der übrigen Bestimmungen grundsätzlich nicht. Die Vertragsparteien werden sich bemühen, anstelle der unwirksamen Bestimmung eine solche zu finden, die dem Vertragziel rechtlich und wirtschaftlich am ehesten gerecht wird.

(6) Die in diesem Vertrag genannte Anlagen sind Vertragsbestandteil.

……, den _____

Köln, den 22. Mai 2018

PraxisStempel und Nachname in Druckbuchstaben
und Unterschrift

_____
Auftraggeber

_____
Auftragnehmer

Bitte unterschrieben zurücksenden per Fax an: 02234-60 161-21
oder per Post an SoliPrax e.K., Max-Planck-Str. 27a, 50858 Köln
oder eingescannt an abst@soliprax.de

Anlage – Technisch-organisatorische Maßnahmen

Organisatorische Maßnahmen

- ☐ Verpflichtungserklärung der Mitarbeiter wurde unterzeichnet
- ☐ Formulare für Kundenanfragen und Beschwerden, Kundenauskünfte
- ☐ Formular für Datenpannen
- ☐ Verfahrensregister beim Auftragnehmer sind vorhanden, vollständig, aktuell
- ☐ Nachweise über durchgeführte Schulungen der Mitarbeiter zum Datenschutz liegen vor
- ☐ Datenschutzbeauftragter ist schriftlich bestellt

Zutrittskontrolle

- ☐ Geschäftsführer ist für die Zutrittskontrolle verantwortlich
- ☐ Schließanlage
- ☐ Abschließbare Fenster
- ☐ Alarmanlage
- ☐ Sicherung der Räume (Büros werden abgeschlossen)
- ☐ Besucher werden erfasst

Zugangskontrolle

- ☐ Berechtigungskontrolle durch Geschäftsführung
- ☐ Zugang zu Rechnern/Systemen nur mit autorisierten Zugangsdaten möglich
- ☐ Benutzerkennung mit Passwort
- ☐ Firewall
- ☐ Virenscanner
- ☐ Externe Dienstleister werden auf Geheimhaltung verpflichtet

Weitergabekontrolle

- ☐ Firewall
- ☐ Virenscanner
- ☐ Geschäftsführung genehmigt Fernwartung

Eingabekontrolle

- ☐ Protokollierung eingegebener Daten
- ☐ Systemwartungsarbeiten werden dokumentiert

Verfügbarkeitskontrolle

Maßnahmen, um sicherzustellen, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt werden

- ☐ Brandschutzmaßnahmen / Rauchmelder
- ☐ Überspannungsschutz
- ☐ Unterbrechungsfreie Stromversorgung
- ☐ RAID (Festplattenspiegelung)
- ☐ Backupkonzept / E-Mail Archivierung
- ☐ Virenscanner

Trennungsgebot

- ☐ softwareseitige Kundentrennung

Systemprüfung

Die Systeme sowie Datensicherungen (Hardware und Software) werden regelmäßig auf einwandfreie Funktion geprüft