**Vereinbarung zur Auftragsverarbeitung von Daten**
**gemäß Art. 28 der EU-Datenschutz-Grundverordnung (DSGVO)**

Zwischen

(Praxis / Firma, Straße & Hausnummer, PLZ & Ort)

- vertreten durch -

(Name des gesetzlichen Vertreters & Unterzeichners, Position)

- nachstehend „Auftraggeber“ oder „Verantwortlicher“ genannt -

und

**FIBU-doc Praxismanagement GmbH**
Am Südhang 28
65510 Hünstetten
- vertreten durch Herrn Christian Brendel, Geschäftsführer -
- nachstehend „Auftragsverarbeiter“ oder „Auftragnehmer“ genannt -
- Verantwortlicher und Auftragsverarbeiter nachstehend gemeinsam auch „Parteien“ genannt -

Stand 23. Februar 2019

**Präambel**

(1) Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Auftrag i.S.d. Art. 4 Nr. 8 DSGVO. Der Auftraggeber hat den Auftragnehmer im Rahmen der Sorgfaltspflichten des Art. 28 DSGVO ausgewählt. Voraussetzung für die Zulässigkeit einer Auftragsverarbeitung ist, dass der Auftraggeber dem Auftragnehmer den Auftrag schriftlich erteilt. Dieser Vertrag enthält nach dem Willen der Parteien und insbesondere des Auftraggebers den schriftlichen Auftrag zur Auftragsverarbeitung i.S.d. Art. 28 DSGVO und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung.

(2) Sofern in diesem Vertrag der Begriff „personenbezogene Daten“ (nachfolgend auch „Daten“) benutzt wird, wird die Definition der „personenbezogene Daten“ i.S.d. Art. 4 Nr. 1 der DSGVO zugrunde gelegt.

(3) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 der DSGVO zugrunde gelegt.

## § 1 Gegenstand und Dauer des Auftrags

**Gegenstand**

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien, die sich aus der Bereitstellung der vertraglichen Leistungen durch den Auftragsverarbeiter ergeben. Die Regelungen dieser Vereinbarung gelten, soweit durch den Auftragsverarbeiter Leistungen gemäß bereits bestehender oder künftig abzuschließender Verträge mit dem Auftraggeber (nachfolgend die „Leistungsvereinbarung“) erbracht werden, und dabei ein Zugriff auf personenbezogene Daten des Auftraggebers nicht ausgeschlossen werden kann. Nicht-personenbezogene Daten sind nicht Gegenstand dieser Vereinbarung.

**Dauer & Beendigung**

(1) Die Laufzeit dieser Vereinbarung gilt für die Dauer der tatsächlichen Leistungserbringung durch den Auftragsverarbeiter, unabhängig von der Laufzeit etwaiger anderer Verträge, die die Parteien ebenfalls bzgl. der Erbringung der vereinbarten Leistungen abgeschlossen haben.

(2) Der Verantwortliche kann diese Vereinbarung jederzeit ohne Einhaltung einer Frist beenden, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters gegen diesen Vertrag vorliegt, der Auftragsverarbeiter Bestimmungen der DSGVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Verantwortlichen nicht erfüllen kann oder will. Etwaige andere Verträge, die ebenfalls die Erbringung der Leistungen des Auftragsverarbeiters für den Verantwortlichen regeln, kann der Verantwortliche in dem Fall ebenfalls ohne Einhaltung einer Frist kündigen.

(3) Bei einfachen (also weder vorsätzlichen noch grob fahrlässigen) Verstößen setzt der Verantwortliche dem Auftragsverarbeiter eine angemessene Frist zur Abstellung des Verstoßes.

(4) Der Auftragsverarbeiter verpflichtet sich, auch über das Ende der Leistungserbringung hinaus, die ihm in diesem Zusammenhang bekannt gewordenen Daten vertraulich zu behandeln.

(5) Nach Abschluss der vertraglich vereinbarten Leistungen oder nach Aufforderung durch den Verantwortlichen hat der Auftragsverarbeiter sämtlich in seinen Besitz gelangten Unterlagen, erstelle Verarbeitungs- und Nutzungsergebnisse sowie Datenbestande, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen und bestehende Kopien innerhalb einer angemessenen Frist datenschutzgerecht zu vernichten.

## § 2 Konkretisierung des Auftragsinhaltes

**Art,Zweck und Ort der vorhergesehenen Verarbeitung von Daten**

Die Verarbeitung der Daten erfolgt zur Erfüllung der in den jeweils geltenden Leistungsvereinbarungen und den Allgemeinen Geschäftsbedingungen („AGB“) vereinbarten Regelungen. Die Verarbeitung erfolgt dabei primär

- In den lokalen Systemen des Auftraggebers: im Rahmen von Fernwartung in Zusammenhang mit technischem Support, Hilfestellungen und Schulungen zu den Produkten des Auftragsverarbeiters
- In den cloudbasierten Softwarelösungen des Auftragsverarbeiters auf Servern in innerhalb der Bundesrepublik Deutschland: bei Nutzung des Online-Controllings (control-doc, solvi control), der Online-Personaleinsatzplanung & -Zeiterfassung (pepito) und / oder des Online-Belegmanagements & der Online-Finanzbuchhaltung (solvi flow)
- Auf Servern von Unterauftragsverarbeitern des Auftragnehmers innerhalb der Bundesrepublik Deutschland, einem anderen Mitgliedstaat der Europäischen Union („EU“) oder einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum („EWR“): bei Nutzung von Diensten der Unterauftragsverarbeiter (siehe jeweils gültige Liste der Unterauftragsverarbeiter)
- In den lokalen Systemen des Auftragsverarbeiters in der Bundesrepublik Deutschland: im Rahmen ihrer Aufbereitung zur Analyse und Auswertung im Zusammenhang mit Beratungsprojekten oder für die weitere Verarbeitung in den oben genannten cloudbasierten Softwarelösungen
- Ggf. gemäß mit dem Auftraggeber geschlossener weiterer Leistungsvereinbarungen, auf die hier verwiesen wird

Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetzte und -verordnungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragsverarbeiter sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich. Der Auftraggeber trägt ferner Sorge dafür, dass der Auftragsverarbeiter bei der Erbringung der Leistungen möglichst wenig mit Daten des Auftraggebers und seiner Mitarbeiter, Kunden und Patienten in Berührung kommt bzw. nur mit solchen Daten, die zur Erfüllung der Leistungsvereinbarung zwingend notwendig sind. Er trägt ferner Sorge dafür, dass er von allen verarbeiteten Daten regelmäßig Datensicherungen anfertigt.

Die personenbezogenen Daten der Betroffenen beim Verantwortlichen werden durch den Verantwortlichen, seine Mitarbeiter oder Dienstleister (auf seine Weisung) oder die Betroffenen selbst in den zur Verfügung gestellten Anwendung erhoben, auf fachlicher Ebene verarbeitet und genutzt und / oder dem Auftragsverarbeiter zur weiteren Verarbeitung zur Verfügung gestellt. Eine Verarbeitung der Daten durch den Auftragnehmer erfolgt daher im Wesentlichen auf technischer Ebene, in jedem Fall ausschließlich im Rahmen der Leistungsverarbeitung und nie ohne, dass der Verantwortlichen, seine Mitarbeiter, Dienstleister oder die Betroffenen selbst die Daten zur Verfügung gestellt haben.

Bei der Erbringung der Leistung durch den Auftragsverarbeiter kann es jedoch dazu kommen, dass der Auftragsverarbeiter weitere Daten des Auftraggebers zur Kenntnis nehmen kann, insbesondere im Rahmen und zum Zweck der

- Fehleranalyse oder Reproduktion von Fehlern auf Basis von Logfiles
- Behebung von Fehlern und Störungen
- Tests bei Erstellung von neuen und Änderungen von bestehenden Programmen
- Bereitstellung von Speicherkapazitäten auf virtuellen und physischen Servern
- Unterstützung der Leistungsanpassung und Nutzungsoptimierung der Produkte und Services
- Sonstigen Unterstützung des Auftraggebers

**Art der Daten**

Folgende Arten / Kategorien von personenbezogenen Daten sind regelmäßig Gegenstand der Verarbeitung:

- Vertrags- & Stammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Abrechnungsrelevante Daten (Anschrift, Lastschriftauftrag, Kontodaten, Bestellhistorie, Zahlungshistorie, Kunderennummern, Mitgliedsnummern, Rechnungsdaten)

- Planungs- und Steuerungsdaten sowie Historie (absolvierte Schulungen & Seminare, Kontaktpunkte, Aufgaben & Projekte)
- Kundestrukturdaten (Größe, Rechtsform, Anzahl Mitarbeiter, verwendete Software & Dienstleister)
- Kontakt- & Kommunikationsdaten (Telefonnummern, E-Mail-Adressen, Postanschrift; inkl. zugehörige Korrespondenz)
- Auskunftsangaben (von Dritten, z.B. Auskunfteien oder aus öffentlichen Verzeichnissen)
- Nutzerdaten (Login- und Nutzungsdaten)

Für die folgenden Arten / Kategorien von personenbezogenen Daten des Auftraggebers legt der Verantwortliche in den zur Verfügung gestellten Anwendungen oder bei der geforderten Beratung eigenverantwortlich fest, ob und in welchem Umfang sie verarbeitet werden:

- Finanz- und Leistungsdaten (Kontenrahmen / -plan, Buchhaltung, Belege und Rechnungen, Planrechnung, Kontostände und -bewegungen, Darlehensstände, Honorarerlöse, Arbeitgeberbelastung, Raumaufteilung & -größe)
- Personaldaten (Personalnummern, Steuer-IDs, Titel, Namen, Qualifikationen / Typen, Arbeitszeiten, Ein- und Austrittsdaten, Einsatzzeiten & -orte, vertragliche Regelungen, Urlaubsansprüche, Abwesenheiten)

Es kann ferner nicht ausgeschlossen werden, dass in den zur Verfügung gestellten Anwendungen (z.B. in Freitextfeldern) weitere Datenkategorien erfasst werden oder dem Auftragsverarbeiter im Rahmen von Beratungsmandaten weitere Datenkategorien anderweitig zur Verfügung gestellt werden. Der Verantwortliche hat Sorge zu tragen, dass dies nicht oder nur im Einklang mit den Regelungen dieser Vereinbarung und der anwendbaren Datenschutzgesetzte erfolgt.

**Kategorien betroffener Personen**

Folgende Kategorien von betroffenen Personen sind durch die Verarbeitung erfasst:

- Auftraggeber / Inhaber des Auftraggebers

Für die folgenden Kategorien von betroffenen Personen (soweit es sich jeweils um natürliche Personen handelt) legt der Verantwortliche in den zur Verfügung gestellten Anwendungen oder bei der geforderten Beratung eigenverantwortlich fest, ob und in welchem Umfang sie von der Verarbeitung betroffen sind:

- Mitarbeiter & Ansprechpartner des Auftraggebers
- Kunden & Patienten des Auftraggebers
- Lieferanten & Dienstleister des Auftraggebers
- Geschäftspartner & Interessenten des Auftraggebers

## § 3 Rechte und Pflichten sowie Weisungsbefugnisse des Verantwortlichen

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer.

(2) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Verantwortliche verantwortlich. Gleichwohl ist der Auftragsverarbeiter verpflichtet, alle Anfragen zur Geltendmachung von Betroffenenrechten, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

(3) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Verantwortlichem und Auftragsverarbeiter abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Verantwortliche erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Weisungsberechtigte Personen beim Verantwortlichen sind die auf dem Deckblatt aufgeführten gesetzlichen Vertreter, sofern hier nichts anderes angegeben ist:

-

Weisungsempfänger beim Auftragsverarbeiter ist:

- Herr Christian Brendel, Geschäftsführer, 06126 - 501 91 14, datenschutz@fibu-doc.de

Für Weisungen zu nutzende Kommunikationskanäle:

- E-Mail an datenschutz@fibu-doc.de
- Post an FIBU-doc Praxismanagement GmbH, Datenschutz, Am Südhang 28, 65510 Hünstetten

Bei einem Wechsel oder längerfristigen Verhinderung sind der anderen Vertragspartei unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. Vertreter zu benennen.

(4) Der Verantwortliche ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

(5) Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(6) Der Verantwortliche ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragsverarbeiter vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

(7) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

## § 4 Rechte und Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten ausschließlich entsprechend der gesetzlichen Bestimmungen, der Bestimmungen dieses Vertrags für die in § 2 beschriebenen Zwecke, nach Weisung des Verantwortlichen und für die unten beschriebenen statistischen Zwecke.

(2) Ist der Auftragsverarbeiter aufgrund einer gesetzlichen Bestimmung gehindert, die Daten entsprechend dieses Vertrags und der Weisungen des Verantwortlichen zu verarbeiten, informiert er den Verantwortlichen hierüber, es sei denn, eine solche Inkenntnissetzung ist aus wichtigen Gründen des öffentlichen Interesses gesetzlich untersagt (Art. 28 Abs. 3 Satz 2 lit. a DSGVO). Der Auftragsverarbeiter ist in diesem Fall berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen nach Überprüfung bestätigt oder geändert wurde.

(3) Der Auftragsverarbeiter darf die Daten für keine anderen als die hier genannten Zwecke verwenden und ist insbesondere nicht berechtigt, die ihm überlassenen Daten an Dritte weiterzugeben. Kopien und Duplikate werden ohne vorherige Einwilligung des Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung. Im Fall der Wartung, Fernwartung und/oder IT-Fehleranalyse ist der Zugriff auf Daten des Verantwortlichen nach Möglichkeit zu vermeiden oder auf das Minimum zu beschränken.

(4) Der Auftragsverarbeiter kann die vom Auftraggeber zur Verfügung gestellten und im Rahmen seiner Leistungserbringung zusätzlich gewonnenen Daten für rein statistische Zwecke aggregieren und / oder anonymisieren und daraus Statistiken ohne Nennung des Auftraggebers und in eigenem Namen

veröffentlichen. Dies beschränkt sich auf ausschließlich anonymisierte, aggregierte Daten ohne jeglichen Personenbezug.

(5) Der Auftragsverarbeiter sichert zu, einen fachkundigen und zuverlässigen Datenschutzbeauftragten bestellt zu haben, der seine Tätigkeit gemäß Art. 38 und Art. 29 der DSGVO ausübt. Die Kontaktdaten des Datenschutzbeauftragten sind weiter unten in dieser Vereinbarung sowie auf der Homepage des Auftragsverarbeiters leicht zugänglich hinterlegt. Ein Wechsel des Datenschutzbeauftragten wird dem Verantwortlichem unverzüglich mitgeteilt.

(6) Der Auftragsverarbeiter verpflichtet sich der Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 Satz 2 lit. b, Art. 29 und Art. 32 Abs. 4 DSGVO. Der Auftragsverarbeiter 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.

(7) Die Erbringung der vereinbarten Datenverarbeitung findet, soweit unten nicht anders aufgeführt, im Gebiet der Bundesrepublik Deutschland, einem anderen Mitgliedstaat der EU oder einem Vertragsstaat des Abkommens über den EWR statt.

(8) Datenverarbeitungen in sogenannten Drittländern dürfen nur erfolgen, sofern der Auftraggeber zuvor schriftlich zugestimmt hat und zusätzlich die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z.B. Angemessenheitsbestätigung der Kommission, EU-Standardvertragsklauseln oder eine weitere geeignete Rechtsgrundlage wie das EU-US Privacy Shield).

(9) Der Auftragsverarbeiter selbst überwacht auch die Einhaltung der gesetzlichen Bestimmungen sowie die Bestimmungen dieses Vertrags im eigenen Bereich. Der Auftragsverarbeiter führt in regelmäßigen Abständen Kontrollen durch, um die Wirksamkeit und den Erfolg der umgesetzten technischen und organisatorischen Datenschutzmaßnahmen zu prüfen.

(10) Der Auftragsverarbeiter ist zur Unterstützung des Verantwortlichen entsprechend dessen Weisungen verpflichtet, wenn der Verantwortliche seine Pflichten gegenüber betroffenen Person erfüllt, die ihre Rechte nach den Bestimmungen der Art. 12 ff. DSGVO ausüben (z. B. Recht auf Auskunft, Berichtigung).

(11) Der Auftragsverarbeiter hat nur nach Weisung des Verantwortlichen, und sofern die berechtigten Interessen des Auftragsverarbeiters dem nicht entgegenstehen, die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten und nicht direkt beantworten. Die Prüfung der Anfrage obliegt ausschließlich dem Verantwortlichen.

(12) Der Verantwortliche fordert den Auftragsverarbeiter in Textform zur Mitwirkung auf, insofern eine Mitwirkung des Auftragsverarbeiter erforderlich ist. Für alle sich daraus ergebenden Tätigkeiten beim Auftragsverarbeiter - soweit sie keiner gesetzlichen Verpflichtung entsprechen - wird ein angemessenes Entgelt vereinbart, soweit erkennbar wird, dass das übliche Maß überschritten wird.

(13) Der Auftragsverarbeiter wird, soweit ein Zusammenhang mit der Datenverarbeitung durch den Verantwortlichen besteht, den Verantwortlichen auch bei der Wahrnehmung seiner sonstigen gesetzlichen Pflichten unterstützen. Er wird insbesondere den Verantwortlichen unverzüglich über Fälle von schwerwiegenden Betriebsstörungen, bei Verdacht auf Datenschutzverletzungen und / oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten durch den Auftragsverarbeiter, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte informieren.

(14) Der Auftragsverarbeiter trifft in diesen Fällen außerdem unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Verantwortlichen und ersucht um weitere Weisungen.

(15) Die Meldung über die Verletzung des Schutzes personenbezogener Daten enthält möglichst zumindest folgende Informationen:

a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;

b. eine Beschreibung der von dem Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(16) Der Auftragsverarbeiter ist sich bewusst, dass der Verantwortliche u.a. nach Art. 33 und 34 DSGVO verpflichtet ist, den Aufsichtsbehörden Datenschutzverletzungen unverzüglich zu melden. Die entsprechenden Informationen sind zu dokumentieren; sie müssen die für die Meldung an die Aufsichtsbehörden erforderlichen Details enthalten. Im Fall von Datenschutzverletzungen unterstützt der Auftragsverarbeiter den Verantwortlichen auf Weisung bei der Benachrichtigung der betroffenen Personen und der Aufsichtsbehörde.

(17) Der Auftragsverarbeiter hat den Verantwortlichen umgehend über sämtliche an den Auftragsverarbeiter gerichtete Mitteilungen der Aufsichtsbehörden (z. B. Anfragen, Benachrichtigung über Maßnahmen oder Auflagen) in Verbindung mit der Verarbeitung von Daten nach diesem Vertrag zu informieren. Vorbehaltlich zwingender gesetzlicher Auflagen darf der Auftragsverarbeiter Auskünfte an Dritte, auch an Aufsichtsbehörden, nur nach vorheriger Zustimmung (schriftlich oder per E-Mail) durch und in Abstimmung mit dem Verantwortlichen erteilen.

(18) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei Datenschutzüberprüfungen durch die Aufsichtsbehörden, sofern diese Überprüfungen die Datenverarbeitung gemäß dieser Vereinbarung betreffen, und ist zur Umsetzung der Auflagen der Aufsichtsbehörde in Absprache mit dem Verantwortlichen verpflichtet.

(19) Bei Fertigstellung der Auftragsarbeit oder früher auf Verlangen des Verantwortlichen löscht der Auftragsverarbeiter alle personenbezogenen Daten bzw. vernichtet Datenträger mit personenbezogenen Daten datenschutzgerecht entsprechend aktueller und anerkannter technischer Standards in der Weise, dass eine Wiederherstellung der Daten nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. Ausgenommen hiervon sind anonymisierte Daten, die zu statistischen Zwecken oder Testzwecken benötigt werden.

## § 5 Technische und organisatorische Sicherheitsmaßnahmen

(1) Der Auftragsverarbeiter wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Der Auftragsverarbeiter hat die Sicherheit gemäß Art. 28 Abs. 3 Satz 2 lit. c der DSGVO, insbesondere in Verbindung mit Art. 5 Abs. 1 und Abs. 2 der DSGVO, herzustellen.

(2) 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. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstande und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen gemäß Art. 32 Abs. 1 der DSGOV trifft der Auftragsverarbeiter folglich geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(3) Die vom Auftragsverarbeiter getroffenen technischen und organisatorischen Sicherheitsmaßnahmen sind in der Anlage 2 dieser Vereinbarung detailliert beschrieben.

(4) Der Verantwortliche hat die technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung zu prüfen und dem Auftragnehmer Änderungswünsche mitzuteilen. Der Auftragnehmer ist berechtigt, Änderungswünsche abzulehnen und/oder unter Vorbehalt der Kostenübernahme durch den

Auftraggeber zu stellen. Soweit die technischen und organisatorischen Maßnahmen gemäß der Anlage 2 vom Verantwortlichen akzeptiert werden, werden diese ausschließliche Grundlage des Auftrages.

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

(6) Der Auftragsverarbeiter stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DSGVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(7) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann durch aktuelle Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsbeauftragter) erfolgen.

(8) Der Verantwortliche dokumentiert das Kontrollergebnis und teilt es dem Auftragsverarbeiter mit. Bei Fehlern oder Unregelmäßigkeiten, die der Verantwortliche insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragsverarbeiter unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren künftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Verantwortliche dem Auftragsverarbeiter die notwendigen Verfahrensänderungen unverzüglich mit.

(9) Für die Ermöglichung von Kontrollen durch den Verantwortlichen kann der Auftragsverarbeiter einen Vergütungsanspruch geltend machen.

(10) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

(11) Die Parteien sind sich ferner darüber einig, dass zur Anpassung an technische, wirtschaftliche und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen sind zu dokumentieren. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

## § 6 Unterauftragsverarbeiter

(1) Der Verantwortliche erklärt sich damit einverstanden, dass der Auftragsverarbeiter zur Verarbeitung von personenbezogenen Daten gemäß der DSGVO Unterauftragsverarbeiter hinzuzieht. Ein Unterauftragsverarbeitungsverhältnis liegt vor, wenn der Auftragsverarbeiter Dritte mit der Verarbeitung von personenbezogenen Daten des Verantwortlichen beauftragt oder Dritte die Zugriffsmöglichkeit auf diese Daten erhalten.

(2) Nicht hierzu gehören Nebenleistungen, welche der Auftragsverarbeiter z.B. als Telekommunikations- und Informationsleistungen, Post- und Transportdienstleistungen, im Zahlungsverkehr (Banken, Kreditkarteninstitute), 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.

(3) Der Verantwortliche ist ferner damit einverstanden, dass der Auftragsverarbeiter zur Erfüllung seiner vertraglich vereinbarten Leistungen verbundene Unternehmen des Auftragsverarbeiters gemäß §§ 15 ff. AktG zur Leistungserfüllung heranzieht bzw. diese mit Leistungen unterbeauftragt

(4) Der Auftragsverarbeiter ist verpflichtet Unterauftragsverarbeiter sorgfältig auszuwählen und stellt sicher, dass Unterauftragsverarbeiter durch schriftliche Verträge gebunden und dazu verpflichtet werden, das vom Auftragsverarbeiter in dieser Vereinbarung gewährleistete Datenschutzniveau zur Verfügung zu stellen. Der Auftragsverarbeiter hat die Einhaltung der Pflichten der Unterauftragsverarbeiter, insbesondere die Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen, vor Beginn der Datenverarbeitung und sodann regelmäßig zu überprüfen. Das Ergebnis ist jeweils zu dokumentieren und dem Verantwortlichen auf Aufforderung zur Verfügung zu stellen. Entsprechendes gilt im Verhältnis der Unterauftragsverarbeiter zu durch diese hinzugezogene Unter-Unterauftragsverarbeiter.

(5) Die zurzeit mit der Verarbeitung von Daten beschäftigten Unterauftragsverarbeiter sind in Anlage 1 dieser Vereinbarung aufgeführt und ebenso auf der Homepage des Auftragsverarbeiters leicht zugänglich hinterlegt. Mit der Beauftragung erklärt sich der Verantwortliche einverstanden.

(6) Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Unterauftragsverarbeiter, wodurch der Auftraggeber die Möglichkeit erhält, derartigen Änderungen zu widersprechen (Art. 28 Abs. 2 Satz 2 DSGVO). Der Verantwortlichen wird nur widersprechen, wenn schwerwiegende datenschutzrechtliche Gründe dies erfordern. Die Zustimmung gilt als erteilt, wenn der oder die Betroffene nicht innerhalb einer Frist von zwei Wochen widerspricht. Können sich der Verantwortliche und der Auftragsverarbeiter nicht auf eine einvernehmliche Lösung einigen, kann jede Seite den Hauptvertrag innerhalb von vier Wochen nach Scheitern der Verhandlungen kündigen (Sonderkündigungsrecht).

(7) Erbringt der Unterauftragnehmer die vereinbarten Leistungen außerhalb der EU / des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

**§ 7 Ansprechpartner Datenschutz**

Ansprechpartner beim Verantwortlichen sind die auf dem Deckblatt aufgeführten gesetzlichen Vertreter, sofern hier nichts anderes angegeben ist:

Ansprechpartner beim Auftragsverarbeiter ist:
Christian Brendel (Geschäftsführer)
Am Südhang 28, 65510 Hünstetten
datenschutz@fibu-doc.de

Datenschutzbeauftragter des Auftragsverarbeiters ist:
IITR Datenschutz GmbH
RA Dr. Sebastian Kraska
Marienplatz 2, 80331 München
email@iitr.de

**§ 8 Haftung**

(1) Auf Art. 82 DSGVO wird verwiesen. Im Übrigen wird folgendes vereinbart.

(2) Soweit der Auftragsverarbeiter gemäß den Weisungen des Verantwortlichen handelt und die technischen und organisatorischen Maßnahmen sowie die sonstigen ihm durch diese Vereinbarung

auferlegten Verpflichtungen beachtet, stellt der Verantwortliche den Auftragsverarbeiter auf erstes Anfordern von allen rechtlichen Ansprüchen, Schäden und Kosten frei, insbesondere soweit diese dadurch entstehen, dass Dritte oder betroffene Personen aus der Datenverarbeitung resultierende Ansprüche gegen den Auftragsverarbeiter geltend machen.

(3) Hiervon umfasst sind insbesondere auch die Kosten der notwendigen Rechtsverteidigung einschließlich sämtlicher Gerichts- und Anwaltskosten in der jeweiligen gesetzlichen Höhe, sowie Bußgelder in tatsächlich festgesetzter Höhe. Gegenstand der Freistellung sind demnach insbesondere Ansprüche aufgrund von rechtswidrigen Weisungen des Verantwortlichen gemäß Art. 28 Abs. 3 S. 3 DSGVO sowie nicht ausreichender technischer und organisatorischer Maßnahmen, welche vom Verantwortlichen freigegeben wurden.

(4) Dem Verantwortliche bleibt im Nachgang vorbehalten, nachzuweisen, dass die gegen den Auftragsverarbeiter gerichteten, vorgenannten Ansprüche und Bußgelder nicht auf Weisungen oder Pflichtverletzungen des Verantwortlichen beruhen.

## § 9 Schlussbestimmungen

(1) Der Auftragsverarbeiter darf keine der Daten aus dem Grund zurückbehalten, dass er selbst ein Recht gegenüber dem Verantwortlichen hat.

(2) Von der Ungültigkeit einer Bestimmung dieses Vertrags bleibt die Gültigkeit der übrigen Bestimmungen unberührt. Sollte sich eine Bestimmung als unwirksam erweisen, werden die Parteien diese durch eine neue ersetzen, die dem von den Parteien Gewollten am nächsten kommt.

(3) Sämtliche Änderungen dieses Vertrags sowie Nebenabreden bedürfen der Schriftform (einschließlich per E-Mail). Dies gilt auch für das Abbedingen dieser Schriftformklausel selbst.

(4) Gerichtsstand für alle Streitigkeiten aus oder in Zusammenhang mit diesem Vertrag ist Frankfurt am Main. Dieser gilt vorbehaltlich eines etwaigen ausschließlich gesetzlichen Gerichtsstandes.

| | |
|---|---|
| , den | Hünstetten, den 23.02.2019 |
| _____ | _____ |
| Verantwortlicher | Auftragsverarbeiter |
| | fibu◆doc Praxismanagement |