Vereinbarung zur Auftragsverarbeitung nach Artikel 28 Datenschutz-Grundverordnung DSGVO

Die Vereinbarung tritt mit Beginn der Nutzung der Dienstleistungen des Auftragnehmers durch den Auftraggeber in Kraft und läuft für die Dauer des zwischen den Parteien bestehenden Hauptvertrages über die Nutzung der Dienstleistungen des Auftragnehmers durch den Auftraggeber. Die Vereinbarung ersetzt etwaige bestehende Vereinbarungen zur Auftragsvereinbarung zwischen dem Auftraggeber und dem Auftragnehmer.

Präambel
Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der Erbringung der Dienstleistungen des Auftragnehmers für den Auftraggeber ergeben.

§ 1 Definitionen

(1) **„Personenbezogene Daten“** sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden kann.

(2) **„Verarbeitung“** ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung, die Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich, die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(3) **„Einschränkung der Verarbeitung“** ist eine Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;

(4) **„Pseudonymisierung“** ist eine Verarbeitung personenbezogener Daten in einer Weise, in der die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die Daten keiner betroffenen Person zugewiesen werden können.

(5) **„Verantwortlicher“** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO).

(6) **„Auftragsverarbeiter“** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(7) **„Unter-Auftragsverarbeiter“** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten des Verantwortlichen im Auftrag des Auftragsverarbeiters verarbeitet.

(8) **„Empfänger“** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht; Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder anderen Rechtsvorschriften personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung.

(9) **„Verletzung des Schutzes personenbezogener Daten“** ist eine Verletzung der Sicherheit, die zur unbeabsichtigten oder unrechtmäßigen Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten geführt hat, die verarbeitet wurden.

(10) **„besondere Kategorien personenbezogener Daten“** sind

a) Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen,
b) genetische Daten,
c) biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,
d) Gesundheitsdaten und
e) Daten zum Sexualleben oder zur sexuellen Orientierung.

(11) **„Weisung“** ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Pseudonymisierung, Einschränkung der Verarbeitung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch den konkreten Umfang der Leistungen bzw. den Anlagen zu dieser Vereinbarung festgelegt und können vom Auftraggeber danach durch einzelne dokumentierte Weisungen geändert, ergänzt oder ersetzt werden (Allgemeine Weisung und/oder Einzelweisung).

§ 2 Gegenstand des Auftrags, Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers zur Erbringung der in **Anlage 1** genannten Dienstleistungen/Arbeiten. Der Auftraggeber ist in diesen Fällen Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Werden personenbezogene Daten im Auftrag eines Verantwortlichen durch andere Personen oder Stellen verarbeitet, hat der Verantwortliche für die Einhaltung der Vorschriften der DSGVO und anderer Vorschriften über den Datenschutz zu sorgen. Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** zu diesem Vertrag festgelegt.

(2) Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Verarbeitung verantwortlich und ergreift alle notwendigen Maßnahmen zur Einhaltung des Datenschutzes.

(3) Aufgrund der vorstehenden Verantwortlichkeit kann der Auftraggeber auch während der Laufzeit der Vereinbarung und nach Beendigung der Vereinbarung die Berichtigung, Löschung, Einschränkung der Verarbeitung und Herausgabe von Daten verlangen bzw. jederzeit Weisungen erteilen.

(4) Die Inhalte dieser Vereinbarung gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verarbeitungen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

(5) Die Verarbeitung von Patientendaten im Rahmen der Bereitstellung von durch die Patienten des Auftraggebers freiwillig angelegte Konten zur Verwaltung der Termine erfolgt durch den Auftragnehmer als Verantwortlichen i.S.d. Art. 4 Nr. 7 DSGVO. Die Regelungen aus dieser Vereinbarung zur Auftragsverarbeitung sind auf diese Leistungen, die der Auftragnehmer direkt gegenüber den Patienten des Auftraggebers erbringt, nicht anwendbar.

(6) Änderungen des Vertragsgegenstands und Verfahrensänderungen sind abzustimmen und entsprechend dokumentiert festzulegen.

§ 3 Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf personenbezogene Daten nur im Rahmen des Auftrages und der dokumentierten Weisungen des Auftraggebers verarbeiten. Jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten des Auftraggebers hat, darf diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass

sie nach dem geltenden Recht zur Verarbeitung verpflichtet ist. Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust treffen, die den Forderungen der DSGVO (Art. 32 DSGVO) entsprechen. Einzelheiten hierzu sind in § 4 bzw. der **Anlage 2** geregelt.

(3) Der Auftragnehmer führt - soweit anwendbar - gemäß Art. 30 Abs. 2 DSGVO ein Verzeichnis aller Kategorien von Verarbeitungen, die er im Auftrag des Auftraggebers durchführt. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO (u. a. Meldepflichten, Datenschutzfolgenabschätzung und vorherige Konsultationen).

(4) Der Auftragnehmer gewährleistet, dass er die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter zur Wahrung der Vertraulichkeit verpflichtet hat und in geeigneter Art und Weise in die für sie maßgeblichen Bestimmungen des Datenschutzes, das Geschäftsgeheimnisschutzgesetz (GeschGehG) sowie (soweit originär bzw. derivativ) anwendbar zur Wahrung der Verschwiegenheit im Sinne von § 203 StGB bzw. die Pflichten im Umgang mit personenbezogenen Daten und der Aufgabensituation (Leistungen) entsprechend angemessen eingewiesen und verpflichtet hat. Die Schweigepflicht und die Verpflichtung zur Vertraulichkeit bestehen auch nach Beendigung der Tätigkeit fort.

(5) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Der Auftragnehmer wird dem Auftraggeber den Namen und die Kontaktdaten seines Datenschutzbeauftragten gesondert in Textform mitteilen.

(6) Nach Beendigung der Vereinbarung hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Wese zu dokumentieren. Der Auftragnehmer darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den Auftragnehmer eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

(7) Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu protokollieren, zu kontrollieren und in geeigneter Weise nachzuweisen bzw. zu dokumentieren. 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.

(8) Der Auftragnehmer wird die Datenverarbeitung im Auftrag grundsätzlich in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen. Dem Auftragnehmer ist eine Datenverarbeitung auch außerhalb von EU oder EWR erlaubt, wenn entsprechende Unterauftragnehmer im Drittland unter Einhaltung der Voraussetzungen von § 9 eingesetzt werden und die Voraussetzungen der Art. 44-48 DSGVO erfüllt sind bzw. eine Ausnahme i.S.d. Art. 49 DSGVO vorliegt.

§ 4 Besondere Pflichten des Auftragnehmers/Anforderungen an die Sicherheit der Datenverarbeitung

(1) Der Auftraggeber und der Auftragnehmer haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten. Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vor-gaben aus Art. 32 DSGVO.

(2) Die Maßnahmen nach Absatz 1 sollen dazu führen, dass

- die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden und die Verfügbarkeit der personenbezogenen Daten
- und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden kann.

(3) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage 2** zu dieser Vereinbarung beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann einmal jährlich oder bei begründeten Anlässen eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

§ 5 Pflichten des Auftraggebers

(1) Der Auftraggeber und der Auftragnehmer sind betreffend ihrer zu verarbeitenden personenbezogenen Daten für die Einhaltung der jeweils einschlägigen Datenschutzgesetze verantwortlich.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest. Entstehen nach Vertragsbeendigung zusätzliche Kosten durch die Herausgabe oder Löschung der Daten (z. B. Migration auf einen Dritten), so trägt diese der Auftraggeber. Art. 20 der DSGVO verbleibt unberührt.

(4) Erteilt der Auftraggeber Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten vom Auftraggeber zu tragen.

§ 6 Anfragen/Rechte der betroffenen Personen

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützten. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

(3) Der Auftraggeber erstattet dem Auftragnehmer die durch diese Unterstützung entstandenen Kosten.

§ 7 Meldepflichten des Auftragnehmers

Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.
Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbe-sondere folgende Informationen beinhalten:

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

eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

§ 8 Kontrollpflichten

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO.
Hierfür kann er alternativ

- o Selbstauskünfte des Auftragnehmers einholen;
- o sich nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten mit einer angemessenen Frist von mindestens zwei Wochen ohne Störung des Betriebsablaufs persönlich überzeugen.

Der Nachweis kann durch den Auftragnehmer zudem erfolgen durch

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

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte (soweit möglich auch durch und die Einsichtnahme in die gespeicherten personenbezogenen Daten des Auftraggebers und die Datenverarbeitungsprogramme) zu geben, die zur Durchführung einer Kontrolle erforderlich sind.

(3) Soweit der Auftraggeber oder der Kunde des Auftraggebers ein datenschutzrelevantes Audit durch einen unabhängigen Dritten durchführen lässt, muss dieser Dritte eine

Geheimhaltungsvereinbarung unterzeichnen, deren Geheimhaltungsbestimmungen im Wesentlichen den Bestimmungen des Vertrags entsprechen, um vertrauliche Informationen bzw. personenbezogene Daten des Auftragnehmers zu schützen.

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

§ 9 Unterauftragsverhältnisse bzw. Subunternehmer

(1) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen Subunternehmen des Auftragnehmers zur Leistungserfüllung heranzieht bzw. Unternehmen mit Leistungen unterbeauftragt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer wird den Auftraggeber im Falle eines geplanten Wechsels eines Unterauftragnehmers oder bei geplanter Beauftragung eines neuen Unterauftragnehmers rechtzeitig, spätestens aber 4 Wochen vor dem Wechsel bzw. der Neubeauftragung in Textform informieren („Information"). Der Auftraggeber hat das Recht, dem Wechsel oder der Neubeauftragung des Unterauftragnehmers unter Angabe einer Begründung in Textform binnen drei Wochen nach Zugang der „Information" zu widersprechen. Der Widerspruch kann vom Auftraggeber jederzeit in Textform zurückgenommen werden. Im Falle eines Widerspruchs kann der Auftragnehmer das Vertragsverhältnis mit dem Auftraggeber mit einer Frist von mindestens 14 Tagen zum Ende eines Kalendermonats kündigen. Der Auftragnehmer wird bei der Kündigungsfrist die Interessen des Auftraggebers angemessen berücksichtigen. Wenn kein Widerspruch des Auftraggebers binnen drei Wochen nach Zugang der „Information" erfolgt gilt dies als Zustimmung des Auftraggebers zum Wechsel bzw. zur Neubeauftragung des betreffenden Unterauftragnehmers.

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

(4) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten. Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

(5) Die in **Anlage 3** zu diesem Vertrag aufgeführten Subunternehmer sind vom Auftragnehmer für die Erfüllung der wesentlichen Vertragspflichten eingesetzte und bereits geprüfte Subunternehmer.

§ 10 Haftung

(1) Der Auftragnehmer und Auftraggeber haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung. Der Auftragnehmer stimmt eine etwaige Erfüllung von Haftungsansprüchen mit dem Auftragsgeber an.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn/soweit eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einer betroffenen Person eingetreten ist, verantwortlich ist. Im Übrigen gilt Art. 82 Abs. 5 DSGVO.

(3) Sofern vorstehend nicht anders geregelt, entspricht die Haftung im Rahmen dieses Vertrages der des Hauptvertrages.

§ 11 Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

§ 12 Informationspflichten, Schriftformklausel, Rechtswahl

Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Liquidationsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlicher" im Sinne der DSGVO liegen.

(2) Änderungen und Ergänzungen dieser Vereinbarung und aller seiner Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Ergänzend gelten die Allgemeinen Geschäftsbedingungen des Auftragnehmers. Es gilt ausschließlich deutsches Recht unter Ausschluss des materiellen internationalen Privat- sowie Kollisionsrechts.

§ 13 Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

§ 14 Schlussbestimmung und Anlagenverzeichnis

(1) Die Nichtigkeit, Undurchsetzbarkeit oder Unwirksamkeit einzelner Bestimmungen, auch sofern diese später in den Vertrag aufgenommen oder in einem Nachtrag geregelt werden, berührt die Gültigkeit der übrigen Bestimmungen nicht. Anstelle der unwirksamen, nichtigen oder undurchsetzbaren Bestimmung werden die Vertragsparteien eine Bestimmung vereinbaren, die, soweit rechtlich möglich, dem am nächsten kommt, was nach dem Sinn und Zweck der unwirksamen, nichtigen oder undurchsetzbaren Bestimmung gewollt ist. Gleiches gilt:

- für unbeabsichtigte Regelungslücken; in diesem Fall vereinbaren die Vertragsparteien eine Bestimmung, die dem am nächsten kommt, was nach dem Sinn und Zweck des vorliegenden Vertrages geregelt worden wäre, wenn die Parteien von der Regelungslücke gewusst hätten; oder
- sollte eine Bestimmung des vorliegenden Vertrages hinsichtlich einer Zeitspanne oder eines im Vertrag festgelegten Verhaltens unwirksam sein, so vereinbaren die Vertragsparteien eine Zeitspanne bzw. ein Verhalten, was rechtlich zulässig ist und dem ursprünglich Vereinbarten am nächsten kommt.

(2) Die folgenden Anlagen gelten als vertragswesentliche Bestandteile:

- Anlage 1 - Gegenstand, Art und Umfang der Daten
- Anlage 2 - Technische und organisatorische Maßnahmen
- Anlage 3 - Genehmigte Subauftragnehmer

Anlage 1 - Gegenstand, Art und Umfang der Daten

Die Beauftragung des Auftragnehmers umfasst das Nachfolgende:

1. Gegenstand der Beauftragung

1.1 Der Auftrag des Auftraggebers an den Auftragnehmer umfasst je nach Beauftragungsumfang folgende Arbeiten und/oder Leistungen

O-TIS Online-Terminvereinbarung und -verwaltung
Terminverwaltung und Workflows
Zuweisermodul
Videosprechstunde
Digitale Visitenkarte
Auslastungsoptimierung
SMS Versand
Patientenchat und Dokumentenaustausch
DokFee Digitale Rezeption
DokFee Voice KI-gestützter Anrufbeantworter zur Sprachaufzeichnung und Transkription von Patientenanrufen
DokFee Anamnese und Online Formulare

2. Umfang, Art, Zweck der Daten sowie Datenverarbeitung

2.1 Art und Zweck der Verarbeitung personenbezogener Daten richtet sich nach den vom Auftraggeber in Anspruch genommenen Modulen und liegt in der Erbringung der durch den Auftraggeber in Anspruch genommenen Dienstleistungen des Auftragnehmers:

O-TIS Online-Terminvereinbarung und -verwaltung
Terminverwaltung und Workflows
Zuweisermodul
Videosprechstunde
Digitale Visitenkarte
Auslastungsoptimierung
SMS Versand
Patientenchat und Dokumentenaustausch
DokFee Digitale Rezeption
DokFee Voice KI-gestützter Anrufbeantworter zur Sprachaufzeichnung und Transkription von Patientenanrufen
DokFee Anamnese und Online Formulare

2.2 Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

Patientendaten, z. B. Vorname, Nachname, Geburtstag, Adresse, E-Mail-Adresse, Telefonnummer, Patientennummer, Nachrichten, Sperrvermerk, Behandlungstermine, Erinnerungsmerkmale, Praxis, geplante Behandlungsdauer, Behandler, Raum und Notizen.
Sprachaufzeichnungen, Transkriptionen (bei gebuchtem Modul DokFee Voice)
Metadaten der Anrufe und Videosprechstunde (z. B. Zeitstempel, Telefonnummer, Praxiszuordnung) (bei gebuchtem Modul)
Anamnese und Online-Formulare (bei gebuchtem Modul)
Inhalte der Videosprechstunde (bei gebuchtem Modul)

Daten können sowohl aus dem EVIDENT Praxisverwaltungssystem des Auftraggebers an die O-TIS Webseite übertragen werden oder durch Patienten eingegeben werden.

2.3 Behandlerdaten von Überweisern

Name der Praxis, Titel, Vorname, Nachname, Namenszusatz, Geschlecht, Anrede, Straße, Hausnummer, PLZ, Ort, Telefon, Mobilnummer, E-Mail, Geburtsdatum, Beruf, Duzfreund, Notizen, Logo, Bilder, Nachrichtentexte zwischen Zuweiser und Praxis, Dateien, die zwischen Zuweiser und Praxis ausgetauscht werden können

2.4 Praxisdaten

Behandlername, Arbeitszeiten und Verfügbarkeiten

2.5 Protokolle für Terminerinnerungen, -absagen oder -verschiebungen

Erinnerungsdatum, Nachname, Vorname, Behandlung, Nachricht, Status, E-Mail, Telefonnummer, Behandlung, Grund

2.6 Soweit Daten durch Patienten bei der Registrierung oder nach Anmeldung in ihrem Konto angegeben werden, erfolgt die Verarbeitung gemäß § 2 Abs. 5 durch den Auftragnehmer als Verantwortlichen iSd. Art. 4 Nr. 7 DSGVO. Dabei handelt es sich um die folgenden Daten:

Daten von Patienten: Passworthash, E-Mail-Adresse, Geburtsdatum, Adresse, ob AGB akzeptiert wurden, ob eine Verifizierung der Mailadresse stattgefunden hat, Nachrichtentexte zwischen Patienten und Praxis, Dateien, die zwischen Patienten und Praxis ausgetauscht werden

Daten von Familienmitgliedern: Vorname, Nachname, Geburtsdatum, Straße, PLZ, Ort, Telefonnummer und E-Mail-Adresse

3. Kreis der Betroffenen

Beschäftigte des Auftraggebers (Ärzte)
Zuweisende Ärzte
Patienten des Auftraggebers

Anlage 2 – Technische und organisatorische Maßnahmen

Stand

Vorbemerkung:
Unsere Daten werden auf Systemen unseres Unterauftragsverarbeiters, der Hetzner Online GmbH gehostet. Daten der Patienten von Kunden, die wir als Auftragsverarbeiter verarbeiten, werden nur temporär auf diesen Systemen gespeichert, da die Daten ansonsten komplett im Evident des Auftraggebers vorgehalten werden und durch dieses an unsere Software übermittelt, sowie später von unserer Software an Evident übermittelt werden. Daten von Patienten, die sich bei uns registrieren, werden auf den Systemen der Hetzner Online GmbH verarbeitet.
Die nachfolgenden Beschreibungen der technischen und organisatorischen Maßnahmen erstrecken sich insofern auf die Sicherung des Zugriffs aus unseren Geschäftsräumen bzw. von unseren Endgeräten aus und die von uns vorgenommene Konfiguration der von Hetzner betriebenen Server. Für die Sicherheitsmaßnahmen von Hetzner verweisen wir auf deren TOMs, die wir auf Anfrage gerne jederzeit in der aktuellen Version vorlegen können.
Für die Module DokFee Voice (KI-Anrufbeantworter), DokFee Dashboard und Videosprechstunde verweisen wir analog auf die TOMs der dafür zum Einsatz kommenden Unterauftragsverarbeiter RED Medical Systems GmbH und Microsoft Ireland Operations Limited. Auch hier erfolgt nur eine temporäre Speicherung von Daten für die Dauer der Sprechstunde bzw. der Spracherkennung und Transkription. Gespeicherte Sprachaufnahmen und Transkriptionen werden ebenfalls bei Hetzner gespeichert.

Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Individueller Login mit Benutzername + Passwort	Dokumentiertes Berechtigungskonzept
Login mit biometrischen Daten	Passwortmindestvorgaben
Anti-Virus-Software Clients und regelmäßige Aktualisierung	Passwortmanager
Anti-Virus-Software mobile Geräte und regelmäßige Aktualisierung	
Software Firewall Clients	

Keine Verwendung von externen Datenträgern oder USB-Sticks	
Verschlüsselung Smartphones	
Automatische Desktopsperre mit Passwortschutz	
Festplattenverschlüsselung Laptops	
E-Mail Spamfilter	

Zugriffskontrolle

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

Technische Maßnahmen	**Organisatorische Maßnahmen**
Keine Verwendung von Papierunterlagen oder Ausdrucken	Dokumentiertes Berechtigungskonzept
Sicheres Überschreiben / Physische Löschung von Datenträgern	Minimale Anzahl an Administratoren
Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	Verwaltung Benutzerrechte durch Administrator
	Änderung von Zugriffsrechten bei Wechsel der Tätigkeit oder Verlassen des Unternehmens
	Regelmäßige Prüfung von Benutzerrechten

Trennung

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Trennung von Produktiv- und Testumgebung	Getrennte Nutzeraccounts je nach Praxis
Mandantenfähigkeit	Festlegung von Datenbankrechten
Virtuelle Trennung von Daten je nach Praxis	

Pseudonymisierung & Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Technische Maßnahmen	Organisatorische Maßnahmen
Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System	
Verschlüsselung der Sprachaufzeichnungen/Transkriptionen während der Speicherung und Übertragung	
Verschlüsselung aller Daten bei Hetzner durch Public/Private Key	

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Technische Maßnahmen	Organisatorische Maßnahmen
E-Mail-Transportverschlüsselung	Sprachaufzeichnungen, Transkriptionen: Konfiguration der Löschfristen durch den Auftraggeber
Komplette Kommunikation ist SSL verschlüsselt und erfolgt über das HTTP(s) Protokoll	
Protokollierung der Zugriffe und Abrufe	
Authentifizierung durch Private Key	
Nutzung von Signaturverfahren	
Kommunikation zwischen EVIDENT des Auftraggebers und der O-TIS Webseite durch Webservice auf SOAP Basis	

Eingabekontrolle

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

Technische Maßnahmen	Organisatorische Maßnahmen

Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
Automatisierte Auswertung der Protokolle	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	Klare Zuständigkeiten für Löschungen

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und im Falle des Falles wiederhergestellt werden können.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Feuer- und Rauchmeldeanlagen	Backup & Recovery-Konzept
Servermonitoring	Kontrolle des Sicherungsvorgangs
Redundante Backups, geografisch getrennt	Stichprobentests zur Datenwiederherstellung und Protokollierung der Ergebnisse
	Benachrichtigungskette für Störungen oder Vorfälle

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Technische Maßnahmen	**Organisatorische Maßnahmen**

Jährliche Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen	Externer Datenschutzbeauftragter: Maak Roberts Datenschutzbeauftragter (TÜV-zertifiziert) Datenschutzauditor (TÜV-zertifiziert) LEROIL Datenschutz Hamburg Berlin Levermann Roberts GbR Holzmarktstraße 25 10243 Berlin ro@leroil.de +49.30.549 094 97
	Mitarbeiter geschult und auf Vertraulichkeit/ Datenschutz verpflichtet
	Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörden)
	Abläufe zum Umgang mit Sicherheitsvorfällen

Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Technische Maßnahmen	**Organisatorische Maßnahmen**
	Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	Abschluss Auftragsverarbeitungsvertrag
	Schriftliche Weisungen an den Auftragnehmer

	Verpflichtung der Mitarbeiter des Auftragnehmers auf Datenschutz & Vertraulichkeit
	Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
	Regelung zum Einsatz weiterer Subunternehmer
	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
	Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers

Anlage 3 - Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende Unternehmen:

Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen
Aufgabenbereich: Server Hosting

seven communications GmbH & Co. KG, Willestr. 4-6, 24103 Kiel, Tel: +49 431 30149270, Fax: +49 431 60049852, Mail: seven.io
Aufgabenbereich: SMS-Dienstleister (Modul SMS-Versand)

RED Medical Systems GmbH, Lutzstraße 2, 80687 München, Tel: 089 954 57 55 20, Fax: 089 954 57 55 21, Mail, info@redmedical.de
Aufgabenbereich: Videosprechstunde

Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin, Irland 18, D18 P521, E-Mail: kunden@microsoft.com
Aufgabenbereich: DokFee Voice, DokFee Dashboard

Azure OpenAI Service, Hosting-Standort: Germany West Central, Bereitstellung von KI-gestützten Funktionen zur Verarbeitung natürlicher Sprache
Azure Speech Service, Hosting-Standort: Germany West Central, Bereitstellung von Funktionen zur Spracherkennung und -synthese

LiveKit Incorporated, USA, E-Mail: privacy@livekit.io
Aufgabenbereich: DokFee Voice, Bereitstellung von Funktionen zur Spracherkennung und -synthese, Hosting-Standort: Deutschland

ElevenLabs Inc., 169 Madison Ave #2484, New York, NY 10016 NYC, USA, E-Mail: legal@elevenlabs.io
Aufgabenbereich: DokFee Voice, Bereitstellung von Funktionen zur Spracherkennung und -synthese