Vereinbarung zur Auftragsverarbeitung

Als Anlage für den Nutzungs- und Supportvertrag für die DOCMAiTE Software inkl. optionaler Hardwarebereitstellung – nachfolgend „Leistungsvereinbarung“ –

Version 11, Stand 15.10.2026

zwischen

dem Kunden der DOCMAiTE GmbH

(im Folgenden „Auftraggeber“)

und

der DOCMAiTE GmbH
mit Sitz in der Geismar Landstraße 11,
37085 Göttingen

vertreten durch Dr. Christoph Prinz (im Folgenden „Auftragnehmer“)

- beide nachfolgend gemeinsam „Vertragsparteien“ -

wird die folgende Vereinbarung zur Auftragsverarbeitung geschlossen:

Präambel

Die Vertragsparteien haben im Rahmen einer Leistungsvereinbarung ein Auftragsverarbeitungsverhältnis begründet. Zur Regelung der sich daraus ergebenden datenschutzrechtlichen Pflichten schließen sie die nachfolgende Vereinbarung gemäß Art. 28 DS-GVO.

§ 1 Anwendungsbereich

(1) Im Rahmen der Leistungsvereinbarung ist es erforderlich, dass der Auftragnehmer Zugriff auf personenbezogene Daten des Auftraggebers oder sonstiger Dritter erhält. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien bei der Durchführung der Leistungsvereinbarung. Sie findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers, die von ihm eingesetzten Partner (i. d. R. Systemhauspartner

im Sinne von § 10) oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.

(2) Im Falle eines Widerspruchs zwischen den Bestimmungen dieser Vereinbarung und denjenigen der Leistungsvereinbarung gehen die Bestimmungen dieser Vereinbarung denjenigen der Leistungsvereinbarung vor.

§ 2 Gegenstand und Dauer der Vereinbarung

(1) Der Auftragnehmer stellt dem Auftraggeber das Patienten-Informations- und Organisations-System DOCMAiTE bereit. Der Auftragnehmer übernimmt für das System:

- die Erstinstallation,
- die Prüfung auf Updates und deren Installation,
- den telefonischen Service und Support,
- die Fehlerbehebung,
- sowie die Abrechnung der Softwarenutzung.

Diese Leistungen können auch durch vom Auftragnehmer eingesetzte Dritte – nachfolgend „Partner“ (§ 10) genannt – erbracht werden. Diese Partner werden über einen separaten Partnervertrag auf die Einhaltung der hier vereinbarten Standards und Prozesse zur Erbringung dieser Leistungen verpflichtet. Zur Erbringung dieser Leistungen ist der Partner im Rahmen der jeweiligen Leistungsvereinbarung berechtigt, Zugriff auf personenbezogene Daten des Auftraggebers oder sonstiger betroffener Personen zu erhalten.

(2) Die Datenerhebung erfolgt durch persönliche Übergabe der Daten, durch Remote-Zugriff, per Telefon oder per E-Mail.

(3) Die Laufzeit der Vereinbarung ist an die Laufzeit der Leistungsvereinbarung gekoppelt.

§ 3 Konkretisierung des Auftragsinhalts

(1) Gegenstand der Auftragsverarbeitung ist die Abrechnung, Pflege und der Support im Zusammenhang mit dem Einsatz des Patienten-Informations- und Organisations-Systems DOCMAiTE. Der Auftragnehmer und die von ihm eingesetzten Partner haben zur Vertragserfüllung ein berechtigtes Interesse personenbezogene Daten zu erheben, erfassen, organisieren, speichern, anpassen, verändern, auslesen, abfragen, verwenden, übermitteln, verknüpfen oder löschen.

(2) Folgende Arten personenbezogener Daten sind Gegenstand der Verarbeitung durch den Auftragnehmer und die von ihm zur Durchführung von Leistungen beauftragten Partner:

- Personenstammdaten (z. B. Name, Geburtsdatum, Adresse, Kontaktdaten)
- Bankdaten (z. B. IBAN)
- Gesundheitsdaten im Sinne von Art. 9 Abs. 1 DS-GVO, insbesondere: ärztliche Dokumente, Befunde, Überweisungen, Medikationspläne, Anamnesen, Arztbriefe, Entlassungsbriefe, Befundberichte, Laborberichte, Diagnosen, Therapiemaßnahmen

- weitere medizinische und administrative Unterlagen, die im Rahmen der haus- oder fachärztlichen Versorgung im System verwaltet werden

(3) Der Kreis der durch den Umgang mit ihren Daten betroffenen Personen ist (Kategorien betroffener Personen):

- Der Auftraggeber, dessen Stammdaten und Bankdaten er zur Abwicklung der Zahlungs- und Buchhaltungsprozesse übermittelt,
- Patientinnen und Patienten der Arztpraxis, deren personenbezogene und gesundheitsbezogene Daten im Rahmen der ärztlichen Versorgung verarbeitet werden,
- Beschäftigte der Arztpraxis, sofern personenbezogene Daten (z. B. Kontaktdaten, Nutzerkonten, Bearbeitungshistorien) im Rahmen der Systemnutzung gespeichert oder protokolliert werden
- Externe medizinische Leistungserbringer, deren Daten im Rahmen der ärztlichen Dokumentation (z. B. Überweisungen, Facharztberichte) verarbeitet werden,
- Kontaktpersonen der Patienten, soweit ihre Daten (z. B. Erziehungsberechtigte, Angehörige) im Zusammenhang mit der Patientenakte erfasst werden.

(4) Im Rahmen der Auftragsverarbeitung werden besondere Kategorien von Daten gemäß Art. 9 Abs. 1 DS-GVO verarbeitet.

(5) Die verarbeiteten personenbezogenen Daten haben einen hohen Schutzbedarf.

(6) Darüber hinaus werden zur Sicherstellung des Betriebs, zur Fehleranalyse und zur Weiterentwicklung der Software Telemetriedaten erhoben. Diese umfassen ausschließlich technische Systemdaten (z. B. Softwareversion, Systemzustände, Fehlermeldungen). Die Telemetriedaten enthalten keine personenbezogenen Daten; insbesondere erfolgt keine Übermittlung von Patienten- oder Gesundheitsdaten. Soweit technisch bedingt personenbezogene Merkmale (z. B. IP-Adressen) anfallen, werden diese vor jeder weiteren Verwendung anonymisiert. Diese Telemetriedaten werden zum Zweck der Zusammenarbeit sowie zur Verbesserung der Produkt- und Servicequalität mit dem jeweiligen Partner geteilt.

§ 4 Weisungen

(1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor. Er erteilt alle Weisungen in der Regel schriftlich oder in Textform. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

(2) Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 1. Die vom Auftragnehmer eingesetzten Partner, die für Einrichtung, Pflege und Support der Software bestellt bzw. zugeordnet werden – in der Regel das den Kunden bereits anderweitig betreuende Systemhaus – benennen dem Auftraggeber in Textform die zur Annahme von Weisungen befugten Personen. Weisungen des Auftraggebers an den Partner des Auftragnehmers sind für den Partner im Rahmen seiner Tätigkeit nach § 10 Abs. 4 verbindlich, sofern sie in Textform erfolgen; Abs. 4 gilt für den Partner entsprechend. Der

Partner hat den Auftragnehmer über Weisungen des Auftraggebers unverzüglich zu informieren, soweit diese den Auftragnehmer betreffen.

(3) Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Vertragspartei Nachfolger bzw. Vertreter unverzüglich mitzuteilen. Dies gilt entsprechend für die vom Auftragnehmer eingesetzten Partner.

(4) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

§ 5 Rechte und Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

(2) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen. Der Auftragnehmer wird die von ihm eingesetzten Partner im Sinne von § 10 über Verfahrensänderungen und deren Auswirkungen auf die Tätigkeit des Partners für den Auftraggeber informieren.

(3) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind. Dies erstreckt sich entsprechend auf Auskünfte und Abläufe des beteiligten Partners.

(4) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle zwölf (12) Monate statt.

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

§ 6 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); 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 (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

(3) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, müssen zur Wahrung der Vertraulichkeit verpflichtet sein. Der Auftragnehmer sorgt dafür, dass dies auch für den beauftragten bzw. angeschlossenen Partner und dessen Mitarbeiter gilt.

(4) Der Auftragnehmer sichert zu, dass die bei ihm und bei den von ihm eingesetzten Partnern zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieser Vereinbarung vertraut gemacht wurden.

(5) Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

(6) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

(7) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten. Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung von Anträgen auf Wahrnehmung der in Kapitel III der Datenschutz-Grundverordnung genannten Betroffenenrechte.

(8) Der Auftragnehmer bestellt eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz.

(9) Die Auftragsverarbeitung erfolgt grundsätzlich nur innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieser Vereinbarung erfolgen.

§ 7 Technisch-organisatorische Maßnahmen und deren Kontrolle

(1) Die in Anlage 2 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum.

(2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.

(3) Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

(4) Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

(5) Der Auftraggeber ist für die Umsetzung der technisch-organisatorischen Maßnahmen in Anlage 3 zum Betrieb der im Rahmen der optionalen Hardwarebereitstellung überlassenen lokalen Hardware („KI-Box“) selbst verantwortlich.

§ 8 Regelungen zur Berichtigung, Löschung und Einschränkung der Verarbeitung von Daten

(1) Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken.

(2) Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieser Vereinbarung hinaus Folge leisten. Zu denselben Pflichten verpflichtet der Auftragnehmer auch den Partner.

§ 9 Unterauftragsverhältnisse

(1) Die Beauftragung von Subunternehmern ist dem Auftraggeber im Einzelfall schriftlich anzuzeigen.

(2) Der Auftraggeber hat das Recht, der Subbeauftragung mit Begründung innerhalb von 14 Tagen ab Anzeige zu widersprechen. Erfolgt innerhalb dieser Zeit kein begründeter Widerspruch, gilt der Subunternehmer als genehmigt. Bei rechtzeitigem Widerspruch versuchen die Vertragsparteien innerhalb von 7 Tagen eine Einigung zu erreichen. Gelingt dies nicht, sind beide Vertragsparteien zur außerordentlichen Kündigung dieser Vereinbarung und der Leistungsvereinbarung berechtigt.

(3) Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

(4) Dem Subunternehmer sind vertraglich mindestens Datenschutzpflichten aufzuerlegen, die den in dieser Vereinbarung festgelegten vergleichbar sind. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.

(5) Die Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Auftraggeber berechtigt sein, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.

(6) Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.

(7) Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, ist nur bei Beachtung der in § 6 Abs. 9 dieser Vereinbarung genannten Bedingungen möglich. Sie ist insbesondere nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet. Der Auftragnehmer teilt dem Auftraggeber mit, welche konkreten Datenschutzgarantien der Subunternehmer bietet und wie ein Nachweis hierüber zu erlangen ist.

(8) Zurzeit sind die in Anlage 4 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Auftraggeber genehmigt. Die hier niedergelegten sonstigen Pflichten des Auftragnehmers gegenüber Subunternehmern bleiben unberührt.

(9) Unterauftragsverhältnisse im Sinne dieser Vereinbarung sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

§ 10 Regelungen zur Einsetzung von Partnern

(1) Zur Erfüllung dieses Vertrages bedient sich der Auftragnehmer angeschlossener Partnerunternehmen (Systemhauspartner). Als Partner ist generell jeweils das Unternehmen definiert, welches den fortlaufenden Kunden-Support und die Softwarepflege übernimmt. Dies ist i. d. R. das IT-Systemhaus, welches bereits eine unmittelbare Kundenbeziehung zum Auftraggeber als betreuendes Systemhaus für PVS Software Support und Wartung unterhält.

(2) Mit Abschluss dieser Vereinbarung stimmt der Auftraggeber der Beauftragung des jeweiligen Partners durch den Auftragnehmer als Subunternehmer im Sinne dieser Vereinbarung allgemein zu. Der Auftragnehmer teilt dem Auftraggeber den eingesetzten Partner (Name und Anschrift) vor Beginn der Verarbeitung in Textform mit; § 9 Abs. 2 gilt entsprechend.

(3) Für die Tätigkeiten nach Abs. 4 ist ein gesonderter Auftragsverarbeitungsvertrag zwischen dem Partner und dem Auftraggeber nicht erforderlich, vielmehr verpflichtet der Auftragnehmer den Partner (Subunternehmer) gemäß § 9 Abs. 4 vertraglich zur Einhaltung der Pflichten dieser Vereinbarung. § 9 Abs. 9 findet auf die Tätigkeit des Partners keine Anwendung.

(4) Der Partner übernimmt im Normalfall für den Auftragnehmer:

- die technische Anbindung von DOCMAiTE an das PVS des Kunden,
- die Personalisierung und Anpassung der Software an die Bedarfe des Kunden,

- die Softwarepflege und Wartung,
- den fortlaufenden 1st-Level-Kunden-Support,
- sowie im Auftrag der DOCMAiTE GmbH die Fakturierung von Hardware und Softwarekomponenten gegenüber dem Auftraggeber.

(5) Über Abs. 4 hinausgehende Supportleistungen kann der Partner auf Grundlage einer eigenen Vereinbarung mit dem Auftraggeber zu eigenen Preisen und Konditionen erbringen; Art und Weise der Abrechnung sowie der Erbringung dieser Leistungen liegen im Ermessen des Partners.

(6) Soweit der Partner Leistungen nach Abs. 5 erbringt, handelt er nicht als Subunternehmer des Auftragnehmers; die hierfür erforderliche datenschutzrechtliche Vereinbarung schließen Auftraggeber und Partner unmittelbar. Insoweit haftet der Auftragnehmer nicht. Für die Tätigkeit des Partners als Subunternehmer nach Abs. 4 haftet der Auftragnehmer gegenüber dem Auftraggeber nach Art. 28 Abs. 4 Satz 2 DS-GVO.

§ 11 Mitteilungspflichten

(1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich, möglichst innerhalb von 48 Stunden nach Kenntniserlangung, mit. Der Auftraggeber hat hierfür einen Ansprechpartner zu benennen. Die Mitteilung muss mindestens folgende Angaben enthalten:

- 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;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

(2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder des von ihm eingesetzten Partners oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in dieser Vereinbarung getroffenen Festlegungen.

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

(4) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 32 bis 36 DS-GVO im erforderlichen Umfang zu unterstützen.

§ 12 Kündigung, Folge der Beendigung

(1) Der Auftraggeber ist berechtigt, diese Vereinbarung jederzeit ohne Einhaltung einer Frist zu kündigen, wenn der Auftragnehmer schwerwiegend gegen eine Bestimmung dieser Vereinbarung verstößt, eine Weisung nicht umsetzt oder Kontrollen durch den Auftraggeber verweigert. Das Recht der Vertragsparteien zur Kündigung aus wichtigem Grund bleibt unberührt. Jede Kündigung hat schriftlich zu erfolgen. Fehlverhalten eines Partners im Rahmen seiner Tätigkeit nach § 10 Abs. 5 begründet für sich genommen kein Recht des Auftraggebers zur außerordentlichen Kündigung dieser Vereinbarung gegenüber dem Auftragnehmer; Ansprüche des Auftraggebers gegenüber dem Partner selbst bleiben hiervon unberührt.

(2) Bei Beendigung dieser Vereinbarung oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist.

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

§ 13 Vergütung

Die Vergütung des Auftragnehmers ist abschließend in der Leistungsvereinbarung geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieser Vereinbarung erfolgt nicht.

§ 14 Haftung

(1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner. Für die Tätigkeit des Partners als Subunternehmer nach § 10 Abs. 4 haftet der Auftragnehmer gegenüber dem Auftraggeber nach Art. 28 Abs. 4 Satz 2 DS-GVO; für Tätigkeiten des Partners nach § 10 Abs. 5 gilt § 10 Abs. 6.

(2) Soweit ein Schaden durch die korrekte Umsetzung des Auftrags oder einer Weisung des Auftraggebers entstanden ist, stellt dieser den Auftragnehmer und die von ihm eingesetzten Partner im Sinne von § 10 auf erste Anforderung von sämtlichen Forderungen Dritter frei und erstattet ihnen ebenfalls sämtliche Kosten der notwendigen Rechtsverteidigung.

(3) Der Auftragnehmer haftet nur für Schäden, soweit er diese wenigstens grob fahrlässig herbeigeführt hat.

§ 15 Geheimhaltung, Berufsgeheimnis

(1) Die Vertragsparteien sind verpflichtet, alle im Rahmen der Vereinbarung erlangten Kenntnisse von persönlichen Daten, Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung der Vereinbarung vertraulich zu

behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

(2) Der Auftraggeber unterliegt als Berufsgeheimnisträger der Berufsverschwiegenheit nach Maßgabe der einschlägigen Bestimmungen des jeweiligen Berufsrechts und des Strafrechts. Der Auftragnehmer wahrt daher unter Belehrung über die und in Kenntnis der strafrechtlichen Folgen einer Verletzung der Verschwiegenheitspflicht gemäß § 203 StGB (Freiheitsstrafe bis zu einem Jahr oder Geldstrafe) und sonst anwendbaren rechtlichen Vorschriften strikte Vertraulichkeit hinsichtlich fremder Geheimnisse, die ihm durch den Auftraggeber zugänglich gemacht werden.

(3) Ferner ist der Auftragnehmer verpflichtet, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist.

(4) Der Auftragnehmer ist – vorbehaltlich der anderen in dieser Vereinbarung getroffenen Regelungen – berechtigt, mit Zustimmung des Auftraggebers Dritte zur Vertragserfüllung heranzuziehen. Für die Beauftragung des Partners gilt die Zustimmung nach § 10 Abs. 2.

Beim Einsatz von Dritten verpflichtet sich der Auftragnehmer, diese in Textform unter Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung zur Verschwiegenheit zu verpflichten, soweit diese im Rahmen ihrer Tätigkeit Kenntnis von fremden Geheimnissen im Sinne dieses Paragraphen erlangen könnten. In Bezug auf sein Personal erfüllt der Auftragnehmer die rechtlichen Anforderungen.

§ 16 Schlussbestimmungen

(1) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(2) Sämtliche Änderungen oder Ergänzungen dieser Vereinbarung sind schriftlich zu dokumentieren.

(3) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Anlage 1 Weisungsbefugnis zu § 4

Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie von Seiten des Auftraggebers bestätigt oder geändert wird. Die weisungsberechtigten Personen auf Seiten des Auftraggebers sowie die zum Empfang der Weisungen berechtigten Personen auf Seiten des Auftragnehmers sowie die vorgesehenen Informationswege sind nachfolgend festgelegt.

Weisungsberechtigte Personen auf Seiten des Auftraggebers:

- Der Auftraggeber selbst oder von ihm benannte Personen

Zum Empfang der Weisungen berechtigte Personen auf Seiten des Auftragnehmers:

- Dr. Christoph Prinz

Vorgesehene Informationswege, wenn eine Weisung nach Meinung des Auftragnehmers gegen datenschutzrechtliche Vorschriften verstößt:

- schriftliche und/oder
- elektronische und/oder
- mündliche Information

Weisungen (auch mündliche Weisungen) sind durch die Vertragsparteien zu dokumentieren.

Änderungen bei den weisungsbefugten Personen, den zum Weisungsempfang berechtigten Personen und bei den vorgesehenen Informationswegen sind dem Vertragspartner entsprechend unverzüglich anzuzeigen.

Anlage 2 Technisch-organisatorische Maßnahmen (TOM) des Auftragnehmers zu § 7

Maßnahme	**Umsetzung beim Auftragnehmer**
1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)	
Zutrittskontrolle	• Klingelanlage mit Kamera • Manuelles Schließsystem • Besuchende in Begleitung durch Mitarbeitende
Zugangskontrolle	• Login mit Accountname + Passwort • Login mit biometrischen Daten • Multi-Faktor-Authentisierung bei Remote-Anmeldungen • Verschlüsselung von Datenträgern • Verschlüsselung von Smartphones

	• „Clean-Desk“ Richtlinie • „Sicheres Passwort“ Richtlinie • De-Registrierung von Benutzern
Zugriffskontrolle	• Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten • Berechtigungskonzepte • Verwaltung der Benutzerrechte durch Administratoren
Trennungskontrolle	• Trennung von Produktiv- und Testumgebungen • Ausführung von Applikationen in isolierten Anwendungscontainern
2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)	
Weitergabekontrolle	• Bereitstellung über verschlüsselte Verbindungen (https)
Eingabekontrolle	• Zentrale Logging Infrastruktur
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)	
Verfügbarkeitskontrolle	• Fehler- und Verfügbarkeitsmonitoring
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)	
Incident-Response-Management	• Fehler- und Verfügbarkeitsmonitoring
Datenschutzfreundliche Voreinstellungen	• Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich ist • Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt

Anlage 3 Technisch-organisatorische Maßnahmen (TOM) des Auftraggebers zu § 7

Der Auftraggeber stellt sicher, dass die KI-Box innerhalb seiner IT-Infrastruktur unter angemessenen technischen und organisatorischen Sicherheitsmaßnahmen betrieben wird. Die KI-Box ist in den Räumlichkeiten des Auftraggebers so zu betreiben, dass physischer Zugriff nur autorisierten Personen möglich ist. Der Betrieb erfolgt ausschließlich innerhalb des internen Praxisnetzwerks; eine direkte Erreichbarkeit aus öffentlichen Netzwerken ist zu vermeiden.

Zugriffe auf das System erfolgen nur über autorisierte Benutzerkonten, die individuell vergeben und angemessen geschützt sind. Nicht mehr benötigte Zugänge sind unverzüglich zu deaktivieren.

Der Auftraggeber stellt sicher, dass sicherheitsrelevante Updates des Betriebssystems und der Systemsoftware regelmäßig installiert werden, soweit diese nicht automatisch durch den Auftragnehmer bereitgestellt werden. Der Betrieb erfolgt hinter geeigneten Netzwerksicherheitsmaßnahmen, insbesondere einer Firewall, wobei nur die für den Betrieb erforderlichen Dienste und Netzwerk-Ports freigeschaltet werden. Soweit technisch vorgesehen, werden Zugriffe und administrative Änderungen protokolliert, um eine Nachvollziehbarkeit sicherzustellen.

Der Auftraggeber stellt ferner sicher, dass im Rahmen seiner IT-Sicherheitsstrategie regelmäßige Datensicherungen (Backups) der für den Praxisbetrieb relevanten Daten erfolgen, sofern diese auf der KI-Box gespeichert oder verarbeitet werden und eine Sicherung technisch möglich und erforderlich ist.

Administrative Zugriffe auf die KI-Box erfolgen ausschließlich durch autorisierte Personen des Auftraggebers, durch von ihm beauftragte IT-Dienstleister oder durch den Auftragnehmer. Der Auftraggeber überprüft die Wirksamkeit dieser Maßnahmen regelmäßig und passt sie bei Bedarf an organisatorische Änderungen sowie den Stand der Technik an.

Anlage 4 Subunternehmen zu § 9

Die Beauftragung von Systemhauspartnern (Partnern im Sinne von § 10) ist bereits gemäß § 10 Abs. 2 umfassend gestattet; der jeweils eingesetzte Partner wird dem Auftraggeber nach § 10 Abs. 2 gesondert in Textform mitgeteilt und bedarf keiner Einzelaufführung in dieser Anlage.

Nach § 9 Abs. 8 der Vereinbarung sind die zur Erfüllung dieses Vertrages bereits hinzugezogenen Subunternehmen zu bezeichnen. Der Auftraggeber erklärt sich mit der Beauftragung der folgenden Unternehmen durch den Auftragnehmer einverstanden. Für Subunternehmen mit Sitz in den USA erfolgt die Übermittlung auf Grundlage eines Angemessenheitsbeschlusses (EU-U.S. Data Privacy Framework, Art. 45 DS-GVO) bzw. der EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DS-GVO):

Unternehmen	**Standort**	**Leistung**
Zur Bereitstellung der Funktionalität von DOCMAiTE und Verarbeitung von Patientendaten		
Die Funktionalität der Anwendungslogik ist nicht auf externe Dienste oder Subunternehmen angewiesen, sondern funktioniert ausschließlich mit lokalen Ressourcen.		
Zur Erfüllung der Einrichtung, des Supports, Beratung und der Pflege		
TeamViewer Germany GmbH	Bahnhofsplatz 2, 73033 Göppingen	Fernwartung

STRATO GmbH	Otto-Ostrowski-Straße 7, 10249 Berlin	Hosting von virtuellen Servern zur Ausführung von Telemetrie-Software und Bereitstellung von Ausführungspaketen
Crisp IM SAS	Boulevard de Launay, 44100 Nantes, Frankreich	Kundenkommunikation über die Eingangskanäle E-Mail, Chat und WhatsApp
Restly, Inc. (Produkt Fillout)	9450 SW Gemini Dr, PMB 39088 Beaverton, OR 97008, USA	Hosting der Fragebögen zu Ersteinrichtungsterminen
Pipedrive	Pipedrive OÜ, Mustamäe tee 3a, 10615 Tallinn, Estland	CRM
Zur Organisation und Realisierung der Abrechnung- und Kommunikation		
STRATO GmbH	Otto-Ostrowski-Straße 7, 10249 Berlin	Webhosting, E-Mail-Kommunikation, Hosting von virtuellen Servern zur Speicherung von Kundendaten
Microsoft Deutschland GmbH	Walter-Gropius-Straße 5, 80807 München	Office 365, Teams
WhatsApp Ireland Limited	Merrion Road, Dublin 4, D04 X2K5, Irland	WhatsApp Business
Haufe-Lexware GmbH & Co. KG	Munzinger Straße 9, 79111 Freiburg	Lexware Office
Stripe	Stripe Payments Europe, Limited, 1 Grand Canal Street Lower, Grand Canal Dock Dublin, D02 H210, Irland	Zahlungsabwicklung, Kundenportal und Rechnungserstellung
Zapier, Inc.	548 Market St. San Francisco, CA 94104, USA	Plattformübergreifende Prozessautomatisierung
PartnerPortal.io	PartnerPortal LLC, 300 Center Drive, Suite G, Superior, CO 80027, USA	Partnerportal