Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Vereinbarung
zwischen dem/der

Name oder Firma (inkl. Rechtsform)	
Anschrift	
Geschäftsführer	
Sitz der Gesellschaft	
Handelsregister	

- Verantwortlicher i.S.d. DS-GVO und nachfolgend **Auftraggeber** genannt -

und

Name oder Firma (inkl. Rechtsform)	sprechstunde.online GmbH
Anschrift	Im Teelbruch 118, 45219 Essen
Geschäftsführer	Jochen Roeser (Vorsitzender), Dr. med. Roland Tenbrock
Sitz der Gesellschaft	Essen
Handelsregister	HRB31207

- Auftragsverarbeiter i.S.d. DS-GVO und nachfolgend **Auftragnehmer** genannt -

Präambel

Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und Auftragnehmer im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag. Die in diesem Vertrag verwendeten Begriffe sind entsprechend ihrer Definition in der EU Datenschutz Grundverordnung zu verstehen.

§ 1 Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrags ist die, im nachfolgend benannten Hauptvertrag, beschriebene Verarbeitung personenbezogener Daten (nachstehend „Daten“ genannt), die der Auftragnehmer nur nach Auftrag und nach Weisung des Auftraggebers erheben, verarbeiten oder nutzen darf.

Bezeichnung des Hauptvertrages	Nutzungsvertrag über den Dienst von sprechstunde.online GmbH
Vertragsschluss (Datum)	

(2) Dauer

Der hier vorliegende Vertrag endet spätestens mit der Beendigung des in § 1 (1) genannten Hauptvertrages.

(3) Fristlose Kündigung

Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt hiervon unberührt.

§ 2 Anlagen zum Vertrag

(1) Sämtliche in diesem Vertrag erwähnten Anlagen werden Bestandteil des Vertrages und entfalten Rechtsbindung zwischen den Parteien.

(2) Änderungen der nachfolgend benannten Anlagen werden zwischen den Parteien rechtsverbindlich, sofern diese Anlagen der anderen Partei in Textform i.S.d. § 126b BGB unter der Erklärung, dass es sich um eine Änderung des Vertrages handelt, mitgeteilt werden und die andere Partei nicht innerhalb von 14 Tagen in der Textform widerspricht. Im Übrigen greift § 15 Abs. 2 des Vertrages.

§ 3 Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

Der Zweck und die Form der Datenverarbeitung, die der Auftragnehmer für den Auftraggeber vornimmt, sowie die Art der personenbezogenen Daten und die Kategorien der betroffenen Personen, sind in folgenden Anlagen aufgeführt:

- Leistungsbeschreibung: Anlage 1
- Liste der verarbeiteten Datenkategorien: Anlage 2
- Prozessbeschreibung: Anlage 3

§ 4 Ort der Durchführung der Datenverarbeitung

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb eines Mitgliedstaats der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraums durchgeführt.

§ 5 Technisch-organisatorische Maßnahmen

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

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

(3) Die Maßnahmen sind in der Anlage 5 zu dokumentieren.

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

(5) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

§ 6 Betroffenenrechte

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen, übertragen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen innerhalb von 48 Stunden an den Auftraggeber weiterleiten.

(2) Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Beantwortung von Anträgen von Betroffenen mit geeigneten technischen und organisatorischen Maßnahmen zu unterstützen, soweit es ihm rechtlich möglich ist.

§ 7 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

(1) Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Der Ansprechpartner beim Auftragnehmer wird in Anlage 6 benannt.

(2) Die Wahrung der Vertraulichkeit gemäß der Artt. 28 Abs. 3 b), 29, 32 Abs. 4 DS-GVO. Er setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die

Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

(3) Der Auftragnehmer führt ebenfalls für die Verarbeitung ein Verzeichnis der bei ihm stattfindenden Verarbeitungstätigkeiten i.S.d. Art. 30 DS-GVO. Er stellt auf Anforderung dem Auftraggeber die für die Übersicht nach Art. 30 DS-GVO notwendigen Angaben zur Verfügung. Des Weiteren stellt er das Verzeichnis auf Anfrage der Aufsichtsbehörde zur Verfügung.

(4) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(5) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(6) Der Auftragnehmer ist verpflichtet, sämtliche Informationen bezogen auf Art. 28 DS-GVO dem Auftraggeber zur Verfügung zu stellen, sofern der Auftraggeber diese in Textform (§ 126b BGB) oder in Schriftform (§ 126 BGB) abfragt und dem Auftragnehmer dieses rechtlich und tatsächlich möglich ist.

(7) Soweit der Auftraggeber seinerseits einer Kontrolle der Datenschutzaufsicht, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

(8) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

(9) Die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 10 dieses Vertrages.

(10) Der Auftragnehmer verpflichtet sämtliche Personen, die in seiner Sphäre mit den personenbezogenen Daten in Kontakt kommen, die in Anlage 8 genannten Vorschriften einzuhalten; dies gilt auch über die Beendigung der Tätigkeit hinaus. Die Verpflichtung erfolgt in Schriftform gemäß der Vorschrift des § 126 BGB und ist durch den Auftragnehmer nach Aufforderung nachzuweisen.

§ 8 Weitere Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung ist allein der Auftraggeber verantwortlich. Der Auftraggeber wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z. B. durch Einholung von Einwilligungserklärungen für die Verarbeitung der Daten) geschaffen werden, damit der Auftragnehmer die vereinbarten Leistungen rechtsverletzungsfrei erbringen kann.

(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 ist hinsichtlich der vom Auftragnehmer eingesetzten und vom Auftraggeber genehmigten Verfahren zur automatisierten Verarbeitung personenbezogener Daten datenschutzrechtlich verantwortlich und hat -neben der eigenen Verpflichtung des Auftragnehmers- ebenfalls die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten.
(4) Dem Auftraggeber obliegen die aus Artt. 33, 34 DS-GVO resultierenden Informationspflichten gegenüber der Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen.
(5) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

§ 9 Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
(2) Um die Dokumentationspflicht zu gewährleisten, ist der Vertrag mit dem Subunternehmer in Schriftform i.S.d. § 126 BGB zu schließen.
(3) Der Auftraggeber stimmt der Beauftragung der in Anlage 7 genannten Unterauftragnehmer, unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO, mit dem Abschluss dieses Vertrages zu.
(4) Die Auslagerung auf weitere Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers ist zulässig, soweit:
- der Auftragnehmer eine solche Auslagerung/Wechsel auf Unterauftragnehmer dem Auftraggeber einen Monat vorab die Auslagerung/ den Wechsel gegenüber dem Auftraggeber in Schriftform (§ 126 BGB) anzeigt und
- der Auftraggeber nicht innerhalb eines Monats gegenüber dem Auftragnehmer schriftlich (§ 126 BGB) Einspruch gegen die geplante Auslagerung/ den Wechsel erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird und
- der neue Unterauftragnehmer wirksamer Bestandteil des Vertrages in der Anlage 7 wird.

(5) Von der genannten Monatsfrist kann abgewichen werden, sofern ein unabwendbares Ereignis den Wechsel des Unterauftragnehmers erforderlich macht. Den Wechsel und die Gründe muss der Auftragnehmer dem Auftraggeber unverzüglich darlegen. Sollte der Auftragnehmer den Wechsel nicht genehmigen, steht beiden Parteien innerhalb von 14 Tagen nach Kenntniserlangung der Gründe des Wechsels ein fristloses Kündigungsrecht zu.
(6) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller

Voraussetzungen für eine Unterbeauftragung gestattet, insbesondere die Einhaltung des Art. 29 und Art. 32 Abs. 4 DS-GVO vollständig zu gewährleisten.

§ 10 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer, Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Der Auftragnehmer kann den Prüfer ablehnen, sofern dieser in einem Wettbewerbsverhältnis zu diesem steht. Der Auftraggeber hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Hierbei sollen Störungen des Betriebsablaufs beim Auftragnehmer vermieden werden.

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

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

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

(4) Dem Auftraggeber steht eine kostenfreie Kontrolle des Auftragnehmers pro Jahr zu. Weitere Kontrollen, sofern sie nicht anlassbezogen sind, hat der Auftraggeber nach den Stundensätzen der durch die Kontrolle eingebundenen Mitarbeiter des Auftragnehmers zu vergüten.

§ 11 Mitteilung bei Verstößen des Auftragnehmers

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

- die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich gem. § 121 BGB an den Auftraggeber zu melden

- die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
- die Unterstützung des Auftraggebers für dessen Datenschutzfolgenabschätzung
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

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

§ 12 Weisungsbefugnis des Auftraggebers

(1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.
(2) Sofern der Auftraggeber mündliche Weisungen erteilt, bestätigt er diese unverzüglich in Schriftform gemäß § 126 BGB.
(3) Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 4.
(4) Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei der Nachfolger bzw. Vertreter unverzüglich mitzuteilen.
(5) 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. Bestätigt der Auftraggeber die, aus Sicht des Auftragnehmers rechtswidrige Weisung, ist der Auftragnehmer berechtigt eine Stellungnahme der zuständigen Aufsichtsbehörde einzuholen und bis zu dem Zeitpunkt der Entscheidung durch die Behörde, die Verarbeitung einzustellen.
(6) Der Auftragnehmer hat die ihm erteilte Weisungen und deren Umsetzung selbstständig zu dokumentieren.

§ 13 Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen

Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 14 (Fern-)Zugriffe bei Wartung eines Systems oder anderen Dienstleistungen

Für die Durchführung von (Fern-)Zugriffen bei der Prüfung und/oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen oder bei (Fern-)Zugriffen für andere Dienstleistungen gelten ergänzend folgende Rechte/Pflichten des Auftraggebers/Auftragnehmers:

(1) (Fern-)Zugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten an Arbeitsplatzsystemen werden erst nach Freigabe durch den jeweiligen Berechtigten / zuständigen Mitarbeiter des Auftraggebers durchgeführt.
(2) (Fern-)Zugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten von automatisierten Verfahren oder von Datenverarbeitungsanlagen werden, sofern hierbei ein Zugriff auf personenbezogene Daten nicht sicher ausgeschlossen werden kann, ausschließlich mit Zustimmung des Auftraggebers ausgeführt.
(3) Die Mitarbeiter des Auftragnehmers verwenden angemessene Identifizierungs- und Verschlüsselungsverfahren.
(4) Vor Durchführung von (Fern-)Zugriffen werden sich Auftraggeber und Auftragnehmer über etwaig notwendige Datensicherheitsmaßnahmen in ihren jeweiligen Verantwortungsbereichen verständigen.
(5) (Fern-)Zugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten werden dokumentiert und protokolliert. Der Auftraggeber ist berechtigt, Prüfungs- und Wartungsarbeiten vor, bei und nach Durchführung zu kontrollieren. Bei (Fern-)Zugriffen ist der Auftraggeber - soweit technisch möglich - berechtigt, diese von einem Kontrollbildschirm aus zu verfolgen und jederzeit abzubrechen.
(6) Der Auftragnehmer wird von den ihm eingeräumten Zugriffsrechten auf automatisierte Verfahren oder von Datenverarbeitungsanlagen (insb. IT-Systeme, Anwendungen) des Auftraggebers nur in dem Umfang - auch in zeitlicher Hinsicht - Gebrauch machen, wie dies für die ordnungsgemäße Durchführung der beauftragten Wartungs- und Prüfungsarbeiten notwendig ist.
(7) Soweit bei der Leistungserbringung Tätigkeiten zur Fehleranalyse erforderlich sind, bei denen eine Kenntnisnahme (z. B. auch lesender Zugriff) oder ein Zugriff auf Wirkdaten (Produktions-/Echtdaten) des Auftraggebers notwendig ist, wird der Auftragnehmer die vorherige Einwilligung des Auftraggebers einholen.
(8) Tätigkeiten zur Fehleranalyse, bei denen ein Datenabzug der Wirkbetriebsdaten erforderlich ist, bedürfen der vorherigen Einwilligung des Auftraggebers. Diese muss im Vorfeld mindestens in Textform i.S.d. § 126b BGB oder Schriftform i.S.d. § 126 BGB erfolgen. Bei Datenabzug der Wirkbetriebsdaten wird der Auftragnehmer diese Kopien, unabhängig vom verwendeten Medium, nach Bereinigung des Fehlers löschen. Wirkdaten dürfen nur zum Zweck der Fehleranalyse und ausschließlich auf dem bereitgestellten Equipment des Auftraggebers oder auf solchem des Auftragnehmers verwendet werden, sofern die vorherige Einwilligung des Auftraggebers vorliegt. Wirkdaten dürfen nicht ohne Zustimmung des Auftraggebers auf mobile Speichermedien (PDAs, USB-Speichersticks oder ähnliche Geräte) kopiert werden.
(9) (Fern-)Zugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten sowie sämtliche in diesem Zusammenhang erforderlichen Tätigkeiten, insbesondere Tätigkeiten wie

Löschen, Datentransfer oder eine Fehleranalyse, werden unter Berücksichtigung von technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten durchgeführt. In diesem Zusammenhang wird der Auftragnehmer die technischen und organisatorischen Maßnahmen wie im Anhang beschrieben ergreifen.

§ 15 Informationspflicht, Schriftformklausel, Zurückbehaltungsrecht, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren 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 Stelle« liegen.

(2) Änderungen und Ergänzungen dieses Vertrages mit seinen Anlagen und aller Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer Vereinbarung in Textform (§126b BGB) 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) Bei etwaigen Widersprüchen gehen Regelungen dieses Vertrages zum Datenschutz den Regelungen des Hauptvertrages vor. Sollten einzelne Teile dieses Vertrages mit den Anlagen unwirksam sein, so berührt dies die Wirksamkeit der weiteren Klauseln nicht.

(4) Die Einrede des Zurückbehaltungsrechts, gleich aus welchem Rechtsgrund, an den vertragsgegenständlichen Daten sowie an evtl. vorhandenen Datenträger wird ausgeschlossen.

(5) Es gilt deutsches Recht.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift /Stempel Auftraggeber	Unterschrift /Stempel Auftragnehmer

Anlage A

Anlage 1 Leistungsbeschreibung

Nr.	Leistung	Beschreibung (Zweck und Form der Datenverarbeitung)
1.	Bereitstellung der Funktionalität	Bereitstellung der Funktionalität des Terminkalenders mit der Pflege von onlinesprechstunden Terminen im Rahmen der Software sprechstunde.online, sowie Versand der Zugangstoken per E-Mail und SMS

Anlage 2 Liste aller verarbeiteten Datenkategorien

Bezeichnung des Dokuments	Version / Datum
Beschreibung der Verarbeitungstätigkeit, siehe: sprechstunde.online GmbH_VT_Onlinesprechstunde	11.11.2020

Anlage 3 Prozessbeschreibung

Die zu erbringende(n) Leistung(en) durch den Auftragnehmer ergibt sich aus dem oben referenzierten Hauptvertrag.

Der Auftragnehmer verfügt für den oben beschriebenen Vertragsgegenstand über kein Datenschutz- und Datensicherheitskonzept. Er sichert zu, dass er die nachfolgend beschriebenen Maßnahmen zum Datenschutz- und Datensicherheit ergriffen hat.

Anlage 4 Liste aller berechtigten Personen

Auftraggeber

Nr.	Name	Kontaktdaten (Name, Telefon, E-Mail)	Funktion
1.			
2.			

Auftragnehmer

Nr.	Name	Kontaktdaten (Name, Telefon, E-Mail)	Funktion
1.	Jochen Roeser		Geschäftsführer
2.	Jörg Sälzer		Leitung operatives Geschäft

Anlage 5 Datenschutzbeauftragte

Auftraggeber

Der Auftraggeber ist gesetzlich nicht verpflichtet einen Datenschutzbeauftragten zu benennen. Die Erfüllung dieser Aufgaben obliegt folgendem Ansprechpartner:

Name	
Abteilung	
E-Mail	
Telefon	
Telefax	

Auftragnehmer

Der Auftragnehmer hat nachfolgend benannte Person als Datenschutzbeauftragten benannt:

Name	Prof. Dr. Thomas Jäschke
Firmenname (sofern extern benannt)	DATATREE AG
Anschrift	Heubesstraße 10 40597 Düsseldorf
E-Mail	dsb@datatree.eu
Telefon	+49 211 93190 - 798
Telefax	+49 211 93190 - 799

Anlage 6 Liste aller Unterauftragnehmer (weitere Auftragsverarbeiter)

Entsprechend den Regelungen von § 9 dieses Vertrages sind in die Vertragserfüllung nachfolgend angegebene Unterauftragnehmer eingebunden.

Nr.	Unterauftragnehmer
1.	pangenia systems GmbH, Im Teelbruch 122, 45219 Essen
2.	K&P Computer Service-und Vertriebs-GmbH, Berta-Cramer-Ring 10, 65205 Wiesbaden
3.	ApizeeSAS, 22300 Lannion, Frankreich
4.	Stripe Payments Europe Ltd., 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, Irland

Anlage 7 Regelung zur Wahrung der Verschwiegenheitspflicht

Die Wahrung der Pflichten obliegt, ungeachtet der mit diesem Vertrag getroffenen Bestimmungen zum Datenschutz, immer beim Auftraggeber. Er hat mit geeigneten Maßnahmen sicherzustellen, dass keine unberechtigte Kenntnisnahme von personenbezogenen Daten erfolgen kann. Der Auftragnehmer ist verpflichtet seine Mitarbeiter auf die folgenden Vorschriften, schriftlich dokumentiert, zu verpflichten und sie darauf hinzuweisen, dass diese auch nach Beendigung der Verarbeitung weiterbestehen:

Verpflichtungen	• § 203 StGB (Verschwiegenheitspflicht) Bei einer Verpflichtung nach § 203 StGB sind die Mitarbeiter auf die gesetzlichen Bestimmungen des Zeugnisverweigerungsrechts (§ 53 a StPO) und des Beschlagnahmeverbots bestimmter Aufzeichnungen nach (§ 97 StPO) zu belehren. Die Mitarbeiter dürfen ohne vorherige Genehmigung des Auftraggebers nicht aussagen oder auf andere Weise Auskunft erteilen. • § 206 StGB (Verletzung des Post- oder Fernmeldegeheimnisses) • § 53 BDSG neu (Datengeheimnis) • Art. 28 Abs. 3 b DSGVO (Verschwiegenheitsverpflichtung) • § 35 SGB I (Sozialgeheimnis) • § 78 Abs. 1 SGB X i.V.m. § 35 SGB I (Geheimhaltungspflicht eines Dritten, an den Daten übermittelt werden) • § 88 TKG (Telekommunikationsgesetz)

Änderungsverzeichnis

Version	Datum	Autor	Änderungsgrund/Bemerkungen
2.0	2021-01-06	Susann Zorbach	Überarbeitung

Anlage B

Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DS-GVO

Inhaltsverzeichnis

1 Pseudonymisierung

Die Erbringung der Kerndienstleistung „Videosprechstunde“ erfordert durch die Vorgaben der KBV eine namentliche Nennung der Person und darf nicht in pseudonymer Form erbracht werden.
In den anderen Datenverarbeitungen erfolgt, soweit diese keinen Personenbezug erfordern eine Pseudonymisierung (z.B. bei IP-Adressen durch Löschung einzelner Oktetts)

2 Verschlüsselung

Alle Datenübermittlungen zwischen den Browsern der Endnutzer und der Deutsche Arzt AG Applikation werden nach dem Stand der Technik verschlüsselt (Transportverschlüsslung). Bei dieser Form der Verschlüsselung kommen Sessionschlüssel zum Einsatz, die dynamisch zwischen dem Webbrowser und Webserver ausgehandelt werden.

Bei der persistenten Datenhaltung in dem eingesetzten Datenbanksystem und dem Dateispeicher kommt ebenfalls eine Verschlüsselung zum Einsatz. Diese Verschlüsselung erfolgt durch die eingesetzte Infrastruktur automatisch. Die Nutzer der Plattform haben keinen Zugriff auf diese Schlüssel.

Für die Fernwartung der Deutsche Arzt AG Plattform kommt das SSH (Secure Shell) Protokoll mit zertifikatsbasierter Authentifizierung zum Einsatz.

3 Vertraulichkeit

3.1 Physikalische Sicherheit

Die Datenverarbeitung erfolgt ausschließlich in geeigneten Rechenzentren, die nach der ISO 27001 zertifiziert sind (siehe Anlagen zu den Lfd.Nr. 26 & 28). Die Rechenzentren verfügen über geeignete bauliche, technische und organisatorische Maßnahmen, so dass ein

unbefugter Zutritt zu den Datenverarbeitungs-, Datenspeicherungs- und Netzwerksystemen auf angemessene Weise reduziert wird.

3.2 Authentifizierung
Alle Systeme verfügen über Zugangskontrollsystem (Userkennung, Passwort) und für administrative Zugänge kommen zusätzliche Softwarezertifikate zum Einsatz. Die Authentifizierung erfolgt gegen ein zentrales Nutzerverzeichnis.

3.3 Berechtigungskonzept
Jeder Nutzer (Arzt /Patient) erhält mit seinem Account nur den Zugang zu seinen Daten. Eine Weitergabe dieser Daten ist untersagt. Für administrative Aufgaben werden gesonderte Accounts auf Systemebene genutzt.

3.4 Weitergabe von Daten
Eine Weitergabe von Daten außerhalb der Plattform erfolgt nicht. Für alle technischen Datenübertragungen gelten die oben genannten Vorgaben zur Verschlüsslung.

3.5 Löschen von Daten
Alle Daten werden nach Vorgaben der Auftraggeber (Ärzte) oder der Patienten (mit Schließen des Accounts), soweit deren Aufbewahrung nicht mehr zur Erfüllung des Vertrages oder auf Grundlage anderer Gesetze erforderlich sind, gelöscht. Die Metadaten der Verbindungen werden spätestens nach 29 Tagen gelöscht.

3.6 Datenportabilität
Der Nutzer hat jederzeit das Recht die von ihm bereitgestellten Daten an einen anderen Anbieter zu übertragen. Derzeit bestehen noch keine standardisierten Schnittstellen für eine direkte Datenübertragung an einen andren Anbieter. Die Daten werden den Nutzern als csv- Datei zur Verfügung gestellt.

4 Integrität
In der Online Videosprechstunde ist die Kommunikation durch die Transportverschlüsslung hinsichtlich der Integrität gesichert. Für die persistente Datenhaltung kommt ein Datenbankmanagementsystem, über das die Integrität der Daten gewährleistet wird, zur Anwendung.

5 Verfügbarkeit
Die Infrastruktur der eingesetzten IT -Systeme (Virtualisierungsplattform, Datenbanksystem, Dateispeicher, usw.) wird durch die genutzten Rechenzentren bereitgestellt. Die Anbieter garantieren eine hohe Verfügbarkeit (von min. 99,95% im Jahresmittel).

Alle geplanten Wartungsarbeiten werden in angekündigt und Zeiten geplant, bei denen von einer geringen Nutzung der Plattform auszugehen ist.

6 Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

Die von Deutsche Arzt AG genutzten Rechenzentren treffen Maßnahmen um die Systemstabilität bei einem Ausfall in angemessener Zeit widerherzustellen. Die

Verfügbarkeit, auch bei einem Ausfall, ist über entsprechende Service Level Agreement seitens der Infrastrukturbetreiber abgesichert.

7 Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Die Deutsche Arzt AG lässt den Betrieb der Videoplattform hinsichtlich des Datenschutzes und der IT-Sicherheit durch eine externe Stelle zertifizieren. Die Aufrechterhaltung der Maßnahmen zum Datenschutz und zur IT-Sicherheit wird durch regelmäßige interne Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen gewährleistet.

Langfristig ist geplant ein Managementsystem zur Informationssicherheit zu etablieren. Die genutzten Rechenzentren sind gemäß ISO / IEC 27001 zertifiziert.

7.1 Prüfung der Eignung von Dienstleistern
In der Auswahl von Dienstleistern für den Betrieb der Infrastruktur wird deren Eignung zum Datenschutz und zur IT-Sicherheit ebenfalls berücksichtigt. Ein Kriterium bei der Wahl der Dienstleister stellt die Zertifizierung zur Informationssicherheit nach ISO / IEC 27001 dar.

Das Zertifikat zur Informationssicherheit wird als ausreichende Garantie für die Eignung des Dienstleisters angesehen. Davon unberührt behalten wir uns anlassbezogene Überprüfung vor.

Anlage C

Angaben der Verarbeitungstätigkeit (Art. 30 Abs.1 EU-DSGVO)

1. Zweckbestimmung und Rechtsgrundlage

Kennung	Bezeichnung der Verarbeitungstätigkeit
	Onlinesprechstunde

Zweckbestimmung der Datenverarbeitung	
Plattformbetrieb zur Durchführung einer digitalen ärztlichen Sprechstunde auf Basis einer Videoübertragung per Internet. Sowie eine damit verbundene Terminkoordinierung / -Verarbeitung.	
Zuständige/r für die Verarbeitungstätigkeit	Geschäftsbereich
Jörg Säzer	Digital

Rechtsgrundlage für die Datenverarbeitung					
X	Einwilligung (Art. 6 Abs. 1 lit. a DS-GVO)		Vertragserfüllung / Vorvertragliche Maß. (Art. 6 Abs. 1 lit. b DS-GVO)		Rechtliche Verpflichtung (Art. 6 Abs. 1 lit c DS-GVO)
	Schutz lebenswichtiger Interessen (Art. 6 Abs. 1 lit. d DS-GVO)		Öffentlichen Interesse / Gewalt (Art. 6 Abs. 1 lit. e DS-GVO)		Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DS-GVO)

Erläuterung/Angabe der Rechtsgrundlage (nur zutreffende Grundlage angeben)
Die Deutsche Arzt AG stellt dem Vertragspartner die Nutzung der online Plattform zur Verfügung. Die Verantwortung für die Rechtmäßigkeit der Datenverarbeitung obliegt dem Vertragspartner, der die Onlineplattform nutzt.

2. Betroffene Personengruppen und diesbezügliche Datenkategorien

Lfd. Nr.	Beschreibung der Personen oder Kategorien von Personen
1	Vertragspartner (i.d.R. Arzt)
2	Patient

Lfd. Nr.	Daten oder Datenkategorien	bKpD (ja/nein)	Zuordnung Personen
1	Videodaten (verschlüsselt)	Ja	Patient / Arzt
2	Personaldaten	Ja	Patient / Arzt
3	Termindaten	Ja	Patient
4	Kontaktdaten	Ja	Patient / Arzt

3. Datenübermittlungen und Empfänger

Interne Empfänger	Staus (t/p)	Zuordnung (PG | DK)	
Keine			

Externe Empfänger	Status (t/p)	Zuordnung (PG | DK)	
Anlage A			

Drittlandübermittlung oder Übermittlung an internationale Organisation	
	Es ist eine Übermittlung in/an nachfolgend genannte Länder/Organisationen geplant
X	Eine Übermittlung in ein Drittland oder eine internationale Organisation ist nicht geplant
Daten oder Kategorien von Daten	
Angabe der Länder oder Organisationen	
Beschreibung der Rechtsgrundlage	
Erläuterungen der geeigneten Garantien	

4. Aufbewahrungspflichten und Löschfristen

Fristen	Rechtsgrundlage und Erläuterung	Zuordnung Datenkategorie
3 Monate	Art. 6 Abs. 1 lit. b) DSGVO	2-4
10 Jahre	Ggf. erhoben Zahlungsdaten müssen nach HGB mit dieser Frist gespeichert werden.	2

5. Datenschutz-Folgeabschätzung (Risikoanalyse)

Durchführung einer Datenschutz-Folgeabschätzung (DSFA)	
	Für die Verarbeitungstätigkeit ist die Durchführung einer DSFA nicht notwendig (ggf. erläutern)
	Die Durchführung einer DSFA ist notwendig, ist jedoch nicht erfolgt (bitte begründen)
X	Die DSFA wurde mit nachfolgendem Ergebnis durchgeführt (bitte erläutern)
Erläuterung / Begründung	
Die analysierten Risiken werden durch die getroffenen Maßnahmen wirksam beherrscht. Mögliche Restrisiken sind minimal und werden durch den Verantwortlichen akzeptiert. Das Verfahren wurde durch den Verantwortlichen freigegeben.	
Referenz zur Datenschutz-Folgeabschätzung / Risikoanalyse	
Reviewprotokoll_ZV48_dsc_Anlage_Lfd.Nr. 25	

6. Auftragsverarbeitung

Einbindung von Dienstleistern	
	Eine Auftragsverarbeitung durch eingebundene Dienstleister erfolgt nicht.
X	Die gesamte Verarbeitungstätigkeit oder Teilaufgaben werden von Dritten erbracht.
Dokumentation der eingebundenen Dienstleister und Ihrer Leistungen	
Die Dokumentation der Verarbeitungstätigkeit ist in **Anlage A** beschrieben.	

7. Maßnahmen zur Wahrung von Personenrechten

Beschreibung spezifischer Maßnahmen zur Wahrung der Personenrechte
Es sind keine spezifischen Maßnahmen erforderlich. Die Deutsche Arzt AG verarbeitet nur verschlüsselte Videodaten.

8. Maßnahmen zur Sicherheit der Datenverarbeitung

Beschreibung spezifischer technischer und organisatorischer Maßnahmen für das Verfahren
Die Dokumentation der TOMs ist in **Anlage B** beschrieben.

Änderung der Verarbeitungstätigkeit

Datum	Durchführender	Vorgang (Einführung, Erstellung, Aktualisierung, Prüfung)
04.03.2020	Thorben Beer	Erstellung

Anlage D

datenschutz cert

Urkunde

Die datenschutz cert GmbH
bestätigt, dass das Webangebot

https://sprechstunde.online
inklusive der Online Video-Sprechstunde unter
https://app.sprechstunde.online

des Antragstellers

sprechstunde.online GmbH
Im Teelbruch 118, 45219 Essen

den Anforderungen gemäß ips und §§ 2 und 5 der Anlage 31b zum Bundesmantelvertrag - Ärzte SGB V und §§ 2 und 5 der Anlage 16 zum Bundesmantelvertrag - Zahnärzte SGB V genügt.

ID: **DSC.960.11.2020**

ips datenschutz cert GÜTESIEGEL

Ausstellungsdatum: **16. November 2020** gültig bis: **15. November 2022**

datenschutz certified

Dr. Sönke Maseberg
Zertifizierungsstelle

02/dsc

datenschutz cert GmbH · Konsul-Smidt-Straße 88a · 28217 Bremen · zertifizierung@datenschutz-cert.de · www.datenschutz-cert.de