Allgemeines

Diese Besonderen Bedingungen zur Auftragsverarbeitung gemäß Art. 28 DS-GVO (nachfolgend: „**Vereinbarung**“) regeln die Rechte und Pflichten des Verantwortlichen und des Auftragsverarbeiters für die Verarbeitung personenbezogener Daten im Rahmen der Nutzung der Digitalen-medudoc-Leistungen für Ärzte und Kliniken. **Auftragsverarbeiter** ist die **medudoc education GmbH**, c/o Mindspace, Münzstraße 12, 10178 Berlin (nachfolgend: „**medudoc**“ genannt), **Verantwortlicher** ist der „**Kunde**“ oder „**Nutzer**“ der Digitalen medudoc-Leistungen für Ärzte und Kliniken (nachfolgend: „**Auftraggeber**“ genannt). (Auftraggeber und medudoc gemeinsam nachfolgend: „**Parteien**“ genannt). Durch den Abschluss eines Nutzungsvertrages über die Digitalen medudoc-Leistungen für Ärzte und Kliniken (nachfolgend: „**Hauptvertrag**“ genannt), beauftragt der Auftraggeber medudoc mit der Erbringung verschiedener Leistungen gemäß § 2 zur Bereitstellung von digitalen und individualisierbaren Inhalten zur Patientenaufklärung. Die Erbringung der Leistung bringt es mit sich, dass medudoc Zugriff auf personenbezogene Daten erhält und diese zur Vertragsdurchführung verarbeitet. Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Diese Vereinbarung ist Bestandteil eines jeden Hauptvertrages über die Nutzung der Digitalen medudoc-Leistungen für Ärzte und Kliniken, sie tritt mit Abschluss des Hauptvertrages in Kraft. Die Erfüllung dieser Vereinbarung wird nicht gesondert vergütet, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Begriffsbestimmungen

In dieser Vereinbarung verwendete Begriffe, die in Art. 4 und 9 DS-GVO definiert werden, sind im Sinne dieser gesetzlichen Definition zu verstehen.

§ 2 Gegenstand der Auftragsverarbeitung

1. medudoc erbringt für den Auftraggeber Leistungen im Bereich der digitalen Patientenaufklärung. Dem Auftraggeber wird dazu Zugang zu einer Webplattform zur Generierung individueller Patientenaufklärungsvideos zur Verfügung gestellt. Auf dieser Plattform wird nach Generierung des Videos dem Auftraggeber ein Weblink zur Verfügung gestellt. Mittels dieses Weblinks kann das generierte Video vom Auftraggeber aufgerufen werden, zudem kann der Auftraggeber den Weblink an den von ihm, aufzuklärenden Patienten weitergeben. Der aufzuklärende Patient kann das Video somit selbst aufrufen und ansehen sowie den Weblink mit weiteren Personen teilen, die ihn bei der Entscheidung über eine medizinische Maßnahme beraten sollen oder ihm sonst bei der Beurteilung dieser Informationen unterstützen sollen. Dabei erhält medudoc Zugriff auf personenbezogene Daten. medudoc verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers, sofern medudoc nicht durch das Recht der Union oder der Mitgliedstaaten, dem sie unterliegt, zu einer anderen Verarbeitung verpflichtet ist. Umfang und Zweck der Datenverarbeitung durch medudoc ergeben sich aus der Anlage 1 zu dieser Vereinbarung.
2. Die Bestimmungen dieser Vereinbarung finden Anwendung auf alle Tätigkeiten, bei denen medudoc und ihre Beschäftigten oder durch medudoc Beauftragte, mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber oder dessen Kunden/Patienten stammen oder für den Auftraggeber erhoben wurden oder auf sonstige Weise in dessen Auftrag verarbeitet werden.
3. Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Hauptvertrages zwischen den Parteien, sofern sich aus den nachfolgenden Bestimmungen nicht darüber hinausgehende Verpflichtungen oder Kündigungsrechte ergeben.
4. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet in Mitgliedstaaten der Europäischen Union, in Vertragsstaaten des Abkommens über den europäischen Vertragsraum (Beschluss 94/1/EG) oder Drittländern statt, sofern die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

§ 3 Art der verarbeiteten Daten, Kreis der betroffenen Personen

Im Rahmen der Durchführung des Hauptvertrages erhält medudoc Zugriff auf die in Anlage 1 näher spezifizierten Arten personenbezogener Daten, der ebenfalls in Anlage 1 näher spezifizierten Kategorien betroffener Personen.

§ 4 Weisungsrecht

1. medudoc darf Daten nur gemäß den Weisungen des Auftraggebers erheben, nutzen oder auf sonstige Weise verarbeiten. Wird medudoc durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem sie unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt sie dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.
2. Die Weisungen des Auftraggebers sind grundsätzlich abschließend in den Bestimmungen dieser Vereinbarung festgelegt und dokumentiert.Ist medudoc der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, informiert sie den Auftraggeber unverzüglich. medudoc ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. medudoc darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 5 Schutzmaßnahmen seitens medudoc

1. medudoc ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.
2. medudoc wird in ihrem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und gewährleistet, dass sie alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO, insbesondere mindestens die in Anlage 2 aufgeführten Maßnahmen getroffen hat. Sofern auch besondere Kategorien personenbezogener Daten verarbeitet werden, trifft medudoc zusätzlich die sich aus § 22 Absatz 2 BDSG ergebenden angemessenen und spezifischen Maßnahmen. medudoc legt auf Anforderung des Auftraggebers die näheren Umstände der Festlegung und Umsetzung der Maßnahmen offen. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt medudoc vorbehalten, wobei sie sicherstellt, dass das vereinbarte Schutzniveau nicht unterschritten wird.
3. Bei medudoc ist als Datenschutzbeauftragter nach Art. 37 Abs. 1 DS-GVO bestellt: Herr Dr. Werner Schäfke-Zell, Caladan GmbH, dpo@medudoc.com
4. Den, bei der Datenverarbeitung durch medudoc beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu nutzen oder auf sonstige Weise zu verarbeiten. medudoc wird alle Personen, die von ihr mit der Bearbeitung und der Erfüllung dieser Vereinbarung betraut werden (im Folgenden Beschäftigte genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO, Verpflichtung zur Verschwiegenheit für sog. sonstige mitwirkende Personen von Berufsgeheimnisträgern gemäß § 203 StGB) und über die sich aus dieser Vereinbarung ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt und angewiesen mit der gebotenen Sorgfalt die Einhaltung der vorgenannten Verpflichtung anstreben. Diese Verpflichtungen sind so gefasst, dass sie auch nach Beendigung dieser Vereinbarung oder des Beschäftigungsverhältnisses zwischen dem Beschäftigten und medudoc bestehen bleiben. Dem Auftraggeber werden die Verpflichtungen auf Verlangen in geeigneter Weise nachgewiesen.

§ 6 Informationspflichten seitens medudoc

1. Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vereinbarter Verpflichtungen, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch medudoc, bei ihr im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird medudoc den Auftraggeber unverzüglich in Textform, z. B. per E-Mail, informieren. Dasselbe gilt für Prüfungen von medudoc durch die Datenschutz-Aufsichtsbehörde. Sämtliche Informationen erhält der Auftraggeber, an die von ihm im Hauptvertrag angegebenen Kontaktdaten. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält soweit möglich folgende Informationen:
    a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze,
    b. eine Beschreibung der wahrscheinlichen Folgen der Verletzung und
    c. eine Beschreibung der von medudoc ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.
2. medudoc trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Person(en), informiert hierüber den Auftraggeber und ersucht diesen um weitere Weisungen.
3. medudoc ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit in angemessenem Umfang Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.
4. medudoc unterstützt den Auftraggeber erforderlichenfalls bei der Erfüllung der Pflichten des Auftraggebers nach Art. 33 und 34 DS-GVO in angemessener Weise (Art. 28 Abs. 3 S. 2 lit. f DS-GVO). Meldungen für den Auftraggeber nach Art. 33 oder 34 DS-GVO darf medudoc nur nach vorheriger Weisung seitens des Auftraggebers gem. § 5 dieser Vereinbarung durchführen.
5. Sollten die Daten des Auftraggebers bei medudoc durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat medudoc den Auftraggeber unverzüglich darüber zu informieren, sofern ihr dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. medudoc wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als Verantwortlichem im Sinne der DS-GVO liegen.
6. medudoc ist es gestattet, technische und organisatorische Maßnahmen während der Laufzeit des Vertrages zu ändern oder anzupassen, solange sie weiterhin den gesetzlichen Anforderungen gemäß Art. 32 DS-GVO genügen.

7. An der Erstellung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden gemäß Art. 36 DS-GVO hat medudoc, soweit erforderlich, in angemessenem Umfang mitzuwirken. medudoc hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.
8. Der Auftraggeber vergütet medudoc den Aufwand, der ihr im Rahmen ihrer Informationspflichten entsteht. Davon sind sämtliche externen Aufwendungen und Kosten in marktüblicher Höhe, sowie auch interne Aufwendungen und Kosten für die damit betrauten Mitarbeiter umfasst.

§ 7 Kontrollrechte des Auftraggebers

1. medudoc wird dem Auftraggeber auf dessen Anforderung alle erforderlichen und bei medudoc vorhandenen Informationen zum Nachweis der Einhaltung ihrer Pflichten nach dieser Vereinbarung zur Verfügung stellen.
2. Der Auftraggeber ist berechtigt, medudoc bezüglich der Einhaltung der Regelungen dieser Vereinbarung, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen, zu überprüfen; einschließlich durch Inspektionen.
3. Zur Durchführung von Inspektionen nach § 7 Abs. 2 ist der Auftraggeber berechtigt, im Rahmen der üblichen Geschäftszeiten (montags bis freitags von 10 bis 18 Uhr, außer Feiertags am Ort der Betriebsstätte) nach rechtzeitiger Vorankündigung gemäß § 7 Abs. 5 auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen von medudoc die Geschäftsräume von medudoc zu betreten, in denen Auftraggeber-Daten verarbeitet werden.
4. medudoc ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte von medudoc sind oder wenn medudoc durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden von medudoc, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten von medudoc, die nicht unmittelbar relevant für die vereinbarten Überprüfungszwecke sind, zu erhalten.
5. Der Auftraggeber hat medudoc rechtzeitig (in der Regel mindestens zwei Wochen vorher) über alle mit der Durchführung der Überprüfung zusammenhängenden Umstände zu informieren. Der Auftraggeber darf eine Überprüfung pro Kalenderjahr durchführen. Überprüfungen erfolgen gegen Kostenerstattung und nach Abstimmung mit medudoc.
6. Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Überprüfung, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund von dieser Ziffer dieser Vereinbarung gegenüber medudoc verpflichtet ist. Zudem hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen von medudoc hat der Auftraggeber ihm die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Wettbewerber von medudoc mit der Kontrolle beauftragen.
7. Nach Wahl von medudoc kann der Nachweis der Einhaltung der Pflichten nach dieser Vereinbarung anstatt durch eine Inspektion auch durch die Vorlage eines geeigneten, aktuellen Testats oder Berichts einer unabhängigen Instanz (z. B. Datenschutzbeauftragter oder Datenschutzauditor) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit („Prüfungsbericht“) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.
8. Der Auftraggeber vergütet medudoc den Aufwand, der ihr im Rahmen der Kontrolle und für die Einholung der Nachweise entsteht. Davon sind sämtliche externen Aufwendungen und Kosten in marktüblicher Höhe, sowie auch interne Aufwendungen und Kosten für die damit betrauten Mitarbeiter umfasst.

§ 8 Einsatz von Subunternehmern

1. Der Auftraggeber erteilt medudoc hiermit die allgemeine Genehmigung, weitere Auftragsverarbeiter hinsichtlich der in Anlage 1 beschriebenen Verarbeitungen personenbezogener Daten hinzuzuziehen.
2. Die zum Zeitpunkt des Abschlusses dieser Vereinbarung hinzugezogenen weiteren Auftragsverarbeiter ergeben sich aus Anlage 3. Eine jeweils aktuelle Liste der eingesetzten weiteren Auftragsverarbeiter kann der Auftraggeber unter www.medudoc.com einsehen.
3. medudoc informiert den Auftraggeber per E-Mail, wenn sie eine Änderung oder ein Hinzuziehen weiterer Auftragsverarbeiter beabsichtigt. Die Änderungen kann der Auftraggeber auch jederzeit unter www.medudoc.com einsehen. Der Auftraggeber kann gegen die Änderungen binnen 14 Tagen nach Zugang der Information Einspruch erheben. Der Auftraggeber kann gegen die Änderungen nur dann Einspruch erheben, wenn wichtige Gründe der Änderungen oder Hinzuziehung entgegenstehen, insbesondere das Schutzniveau des § 8 (4) unterschritten wird, medudoc ist die Begründung mit dem Einspruch in Textform mitzuteilen. Im Fall des Einspruchs kann medudoc ihre Leistungen entweder ohne die beabsichtigte Änderung erbringen oder - sofern ihr die Leistungserbringung ohne die beabsichtigte Änderung nicht zumutbar ist - den Hauptvertrag innerhalb von 2 Wochen nach Zugang des Einspruchs kündigen.

4. medudoc wird bei einem Hinzuziehen weiterer Auftragsverarbeiter, nur solche weiteren Auftragsverarbeiter hinzuziehen, die hinreichenden Garantien dafür bieten, dass die Verarbeitung entsprechend den Anforderungen der einschlägigen geltenden rechtlichen Bestimmungen erfolgt.

§ 9 Anfragen und Rechte betroffener Personen

1. medudoc wird den Auftraggeber mit technischen und organisatorischen Maßnahmen im Rahmen des Zumutbaren dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der, den betroffenen Personen zustehenden Rechte nachzukommen.
2. Macht eine betroffene Person Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich der auf sie beziehbaren Daten, unmittelbar gegenüber medudoc geltend, so reagiert diese nicht selbstständig, sondern verweist die betroffene Person unverzüglich an den Auftraggeber.

§ 10 Haftung

1. Auftraggeber und medudoc haften gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung. medudoc stimmt eine etwaige Erfüllung von Haftungsansprüchen mit dem Auftraggeber ab.
2. Der Auftraggeber stellt medudoc auf erstes Anfordern von sämtlichen Ansprüchen frei, die betroffene Personen gegen medudoc wegen (i) der Verletzung einer dem Auftraggeber durch die DS-GVO auferlegten Pflicht oder (ii) wegen der Umsetzung einer vom Auftraggeber in dieser Vereinbarung oder gesondert erteilten rechtswidrigen Anweisung geltend machen.
3. Der Auftraggeber trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstandes ist. Solange dieser Beweis nicht erbracht wurde, stellt der Auftraggeber medudoc auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftraggeber oder medudoc erhoben werden. Unter diesen Voraussetzungen ersetzt der Auftraggeber medudoc sämtliche entstandenen Kosten der Rechtsverteidigung.

§ 11 Kündigung

Die Laufzeit und Kündigung dieser Vereinbarung richten sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieser Vereinbarung. Eine isolierte Kündigung dieser Vereinbarung ist ausgeschlossen.

§ 12 Beendigung des Hauptvertrages

1. medudoc wird dem Auftraggeber nach Beendigung des Hauptvertrages und nach Beendigung eventueller nachvertraglicher Pflichten oder jederzeit auf dessen Anforderung alle ihr überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen oder vernichten. Dies betrifft auch etwaige Datensicherungen bei medudoc. medudoc hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen.
2. medudoc ist verpflichtet, auch über das Ende des Hauptvertrages hinaus die ihr im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende der Hauptvertrages hinaus so lange gültig, wie medudoc über personenbezogene Daten verfügt, die ihr vom Auftraggeber zugeleitet wurden oder die sie für diesen erhoben hat.

§ 13 Inkrafttreten dieser Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Diese Vereinbarung tritt auf einem der nachfolgenden Wege in Kraft:

- der Auftraggeber schließt mit medudoc einen Hauptvertrag ab, in diesem Hauptvertrag ist diese Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO als dessen Bestandteil ausdrücklich mit einbezogen. In diesem Fall tritt diese Vereinbarung mit Abschluss des Hauptvertrages in Kraft; oder
- der Auftraggeber schließt auf elektronischem Wege einen Hauptvertrag über den Online-Shop ab und stimmt im Bestellprozess dem Abschluss dieser Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO zu.

§ 14 Schlussbestimmungen

1. Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform oder eines dokumentierten elektronischen Formats. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Abreden bleibt hiervon unberührt.
2. Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.
3. Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Berlin.
4. Folgende Anlagen sind Bestandteil dieser Vereinbarung:

Anlage 1 – Beschreibung der betroffenen Personen/Betroffenengruppen sowie der besonders schutzbedürftigen Daten/Datenkategorien (Version in deutscher und englischer Sprache)

Anlage 2 – Technische und organisatorische Maßnahmen von medudoc (Version in deutscher und englischer Sprache)

Anlage 3 – Genehmigte Subunternehmer (Version in deutscher und englischer Sprache)

Anlage 1 - Beschreibung der betroffenen Personen/Betroffenengruppen sowie der besonders schutzbedürftigen Daten/Datenkategorien

Annex 1 - Description of the data subjects/groups of data subjects as well as the data/data categories requiring special protection

Beschreibung der Datenverarbeitung	**Data Processing Description**
Gegenstand und Zweck der Verarbeitung: Bereitstellung der Dienste zur digitalen Patientenaufklärung von medudoc sowie jeglicher damit verbundener Kundensupport.	**Subject and purpose of processing:** Provision of medudoc's digital patient education services and any related customer support.
Kategorien betroffener Personen: Die übermittelten personenbezogenen Daten betreffen die folgenden Kategorien von betroffenen Personen: • Angehörige der Gesundheitsberufe, d.h. Ärzte und Beschäftigte von Unternehmen, die die medudoc-Leistungen verwenden. • Patienten von Angehörigen der Gesundheitsberufe, die die medudoc- Leistungen verwenden.	**Categories of Data Subjects:** The personal data transferred concern the following categories of data subjects: • Healthcare professionals, i.e., doctors and employees of companies who use the medudoc service. • Patients of healthcare professionals who use the medudoc service.
Kategorien personenbezogener Daten: (Angehörige der Gesundheitsberufe): Die übermittelten personenbezogenen Daten umfassen die folgenden Kategorien von Daten: • Kontaktinformationen • Daten des Endgeräts • Anwendungsnutzungsdaten	**Categories of Personal Data: (Healthcare professionals):** Transferred personal data includes the following categories of data: • Contact information • User device connection data • Application usage data
Kategorien personenbezogener Daten: (Patienten): Die übermittelten personenbezogenen Daten umfassen die folgenden Kategorien von Daten: • Patientenaufklärungsplan • Video-URL • Video-Inhaltsdaten • Daten des Endgeräts • Anwendungsnutzungsdaten	**Categories of Personal Data: (Patients):** Transferred personal data includes the following categories of data: • Patient education plan • Video URL • Video content data • User device connection data • Application usage data

Häufigkeit der Übertragung: Kontinuierlich	**Frequency of the Transfer:** Continuous
Art der Verarbeitung: medudoc führt folgende Verarbeitungstätigkeiten durch: • Verarbeitung zur Erbringung der Dienstleistungen gemäß der Vereinbarung; • Verarbeitung zur Durchführung von Maßnahmen, die für die Vertragserfüllung erforderlich sind; • Verarbeitung zur Erfüllung zusätzlicher Anweisungen des Kunden (z. B. Support- Tickets), die im Rahmen des Zumutbaren und im Einklang mit den Bedingungen der Vereinbarung stehen.	**Nature of the Processing:** medudoc will perform the following processing activities: • Processing in order to provide the Services in line with the Agreement; • Processing in order to perform any actions required for the performance of the Agreement • Processing in order to comply with any additional instructions provided by the Customer (e.g., support tickets) which are within reason & consistent with the terms of the Agreement.

Anlage 2 - Technische und organisatorische Maßnahmen von medudoc

Annex 2 - Technical and organisational measures by medudoc

Ziele des Informationsschutzes	**Information security objectives**
Wir setzen eine Reihe von Maßnahmen um, um die organisatorische Informationssicherheit zu erfüllen, wie sie sich aus den Bestimmungen des Art. 5 Abs. 1 DS- GVO ergeben: • Transparenz für von der Verarbeitung personenbezogener Daten betroffene Personen (Art. 5 Abs. 1 lit. a DS-GVO), • Zweckbindung der Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 lit. b DS-GVO), • Datensparsamkeit bei der Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 lit. c DS-GVO), • Richtigkeit personenbezogener Daten (Art. 5 Abs. 1 lit. d DS-GVO), • Speicherbeschränkung für personenbezogene Daten (Art. 5 Abs. 1 lit. e DS-GVO), • Integrität personenbezogener Daten (Art. 5 Abs. 1 lit. f DS-GVO, Art. 32 Abs. 1 lit. b DS- GVO), • Vertraulichkeit personenbezogener Daten (Art. 5 Abs. 1 lit. f DS-GVO, Art. 32 Abs. 1 lit. b DS- GVO), Die übergreifende Anforderung besteht darin, die Einhaltung von Absatz 1 nachzuweisen: • Rechenschaftspflicht und Nachprüfbarkeit (Art. 5 Abs. 2, Art. 24 Abs. 1 DS-GVO).	We implement a range of measures in order to fulfill organisational information security objectives as derived from the provisions of Art. 5 para. 1, GDPR, as follows: • Transparency for data subjects affected by the processing of personal data (Art. 5 para. 1 lit. a GDPR), • Purpose limitation for the processing of personal data (Art. 5 para. 1 lit. b GDPR), • Data minimisation in the processing of personal data (Art. 5 para. 1 lit. c GDPR), • Accuracy of personal data (Art. 5 para. 1 lit. d GDPR), • Storage limitation for personal data (Art. 5 para. 1 lit. e GDPR), • Integrity of personal data (Art. 5 para. 1 lit. f GDPR, Art. 32 para. 1 lit. b GDPR), • Confidentiality of personal data (Art. 5 para. 1 lit. f GDPR, Art. 32 para. 1 lit. b GDPR), The overall requirement is to demonstrate compliance with paragraph 1: • Accountability and verifiability (Art. 5 para. 2, Art. 24 para. 1 GDPR).
Technische und organisatorische Maßnahmen	**Technical & Organisational measures**
1. Allgemeine technische und organisatorische Maßnahmen zur DS-GVO-Compliance Wir ergreifen die folgenden technischen und organisatorischen Maßnahmen, soweit dies für die Organisation relevant und machbar ist, um sicherzustellen, dass die Verarbeitung der Daten der DS- GVO entspricht;	**1. General technical and organisational measures for GDPR compliance** We implement the following technical and organisational measures, where relevant and viable for the organisation, in order to ensure that processing of data complies with GDPR;
1.1 Technische Maßnahmen	**1.1 Technical measures**

1. Netzwerkisolation • Unsere datensensiblen Dienste verwenden Heroku Private Spaces, um die Isolierung unserer Daten auf Netzwerk- und Softwareebene innerhalb der EU – und damit Ländern mit angemessenem Datenschutzniveau gemäß DS-GVO – zu gewährleisten.	1. Network isolation • Our data critical services use Heroku Private Spaces ensuring network & software level isolation of our data within the EU, i.e., countries with an adequate level of data protection according to GDPR.
1.1.2. Datentrennung • Gesundheitsdaten (z.B. die Behandlung, Video) werden, soweit möglich, getrennt von anderen Nutzerdaten (z.B. Name, Geburtsdatum) verarbeitet und gespeichert. Dies bedeutet, dass die Gesundheitsdaten selbst keine personenbezogenen Gesundheitsdaten darstellen, bis sie von den Benutzern über die Frontend-Anwendungen kombiniert werden.	1.1.2. Data separation • Health data (e.g. procedure, video) is, where possible, processed & stored separately from other user data (e.g. name, d.o.b). This means that the health data does not, by itself, constitute PHI, until combined by users via the front end applications
1.1.3. Rollenbasierte Zugriffskontrolle (RBAC) • Weitere Informationen zur Zugriffsverwaltung finden Sie in Abschnitt 5.	1.1.3. Role Based Access Control (RBAC) • For more information about access management see Section 5.
1.1.4 Patienten-API-Proxy • Wir leiten relevante API-Anfragen des Patienten über einen von uns kontrollierten Dienst an externe Dienste weiter, um zu verhindern, dass externe Unternehmen Zugriff auf die IP-Adresse des Patienten erhalten.	1.1.4 Patient API proxy • We proxy relevant API requests from the patient to external services through a service we control in order to limit external companies from getting access to the patient's IP address.
1.1.5 Datenverschlüsselung • Siehe Abschnitt 7.	1.1.5 Data encryption • See section 7.
1.1.6. Mehrschichtige Architektur • Der externe Zugriff erfolgt über unser API- Gateway mit zusätzlichen Sicherheitsprozessen • Auf interne Dienste kann von außerhalb des privaten Netzwerks nicht zugegriffen werden • Dienste mit hohem Risiko verfügen über zusätzliche Kontrollen, um die Sicherheit zu erhöhen	1.1.6. Layered architecture • External access is via our API gateway which has additional security processes in place • Internal services cannot be accessed from outside the private network • High risk services have additional controls in place to enhance security

1.1.7. EU-Lokalisierung • Identifizierbare Patienten- und klinische Daten werden innerhalb der EU verarbeitet und gespeichert • Anonyme Nutzungsdaten können außerhalb der EU verarbeitet und gespeichert werden	1.1.7. EU localisation • Identifiable patient & clinical data is processed & stored within the EU • Anonymous usage data may be processed & stored outside the EU

1.1.8 Trennungskontrolle • Trennung von Produktions- und Test-(Staging-)Leistungen • Software und Infrastruktur basierte mandantenfähige Sicherheitskontrollen relevanter Anwendungen • Domain-driven Design-Ansatz für die Architektur, um eine Trennung von Zugriff, Daten und Logik zu schaffen	1.1.8 Separation Control • Separation of production and test (staging) services • Software & infrastructure based multi-tenant security controls of relevant applications • Domain driven design approach to architecture, to create separation of access, data, & logic
1.1.9 Verwendung von Spam-Filtern	1.1.9 Use of spam filters
2. Audit-Trail zur Datenmanipulation Die folgenden Maßnahmen stellen sicher, dass im Nachhinein überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt wurden;	2. Data manipulation audit trail The following measures ensure that it is subsequently possible to verify and establish whether and by whom personal data were input, altered or removed;
2.1 Technische Maßnahmen 2.1.1 Protokollierung von Änderungen an Produktionsdiensten 2.1.2 Protokollierung von Abfragen für 30 Tage 2.1.3 Protokollierung von Änderungen an Datenbanken	2.1 Technical measures 2.1.1 Logging of changes to production services 2.1.2 Logging of requests for 30 days 2.1.3 Logging of changes to databases
2.2 Organisatorische Maßnahmen 2.2.1 Eine Übersicht für welche Systeme welche Daten eingegeben, geändert oder gelöscht werden können, ist in der Information Asset Audit Dokumentation enthalten 2.2.2 Nachvollziehbarkeit der Eingabe, Änderung und Löschung von Daten durch individuelle Mitarbeiterkonten	2.2 Organizational measures 2.2.1 Overview for which systems which data can be entered, changed or deleted is included in the information asset audit documentation 2.2.2 Traceability of input, change and deletion of data through individual employee accounts

2.2.3 Klare Verantwortung für Datenlöschungen	2.2.3 Clear responsibility for data deletions
3. Sensibilisierung und Schulung der Mitarbeiter Zur Sensibilisierung der an Verarbeitungsvorgängen beteiligten Mitarbeiter ergreifen wir folgende Maßnahmen; • Allgemeine Informationssicherheit und DS-GVO-Übersicht im Rahmen des Mitarbeiter-Onboardings • Relevante Mitarbeiter werden in den Prozessen zur Prüfung und Überwachung von Datenbeständen geschult • Datenschutz-Risikobewertung als Standardbestandteil von Software Development Life-Cycle (SDLC)-Prozessen • Schulung zur Bedrohungsmodellierung für alle Softwareentwickler	3. Staff awareness & training We take the following measures to increase awareness of staff involved in processing operations; • General Information Security & GDPR overview included as part of staff onboarding • Relevant staff members are trained on data asset auditing & monitoring processes • Data privacy risk assessment as standard part of Software Development Lifecycle (SDLC) processes • Training on Threat Modelling for all software developers

4. Zugangskontrolle Wir schränken den Zugriff auf personenbezogene Daten intern und durch unsere Auftragsverarbeiter ein, basierend auf den Anforderungen unserer Datenbestandsprüfung.	4. Access Control We impose restrictions on access to personal data internally and by our processors, based on the requirements outlined by our data asset audit.
4.1 Technische Maßnahmen Wir implementieren die folgenden technischen Maßnahmen, sofern relevant und machbar; • Login mit Benutzername und Passwort • Multi-Faktor-Authentifizierung • Einbruchserkennungssystem • Mobile Geräteverwaltung • Verschlüsselung von Datenträgern • Nutzung eines Service Accounts für sicheres und auditierbares Deployment • Nutzung einer Virtual Private Connection zwischen Heroku und der MongoDB-Datenbanken	4.1 Technical measures We implement the following technical measures where relevant & viable; • Login with username and password • Multi-factor authentication • Intrusion Detection System • Mobile device management • Encryption of data carriers • Service account for deployments in a secure and auditable way • Virtual Private Connection between Heroku and MongoDB databases

4.2 Organisatorische Maßnahmen Wir implementieren die folgenden organisatorischen Maßnahmen, sofern relevant und sinnvoll; • Berechtigungsverwaltung mit RBAC (rollenbasierte Zugriffskontrolle) durch Administratoren nach dem Prinzip der geringsten Berechtigung • Mindestanzahl an Administratoren • Datenschutz-Tresor • Sichere Passwortrichtlinie und Automatisierung • „Clean Desk"-Bestimmung • Allgemeine Datenschutz- & Sicherheitsrichtlinien • Anweisung zur manuellen Desktop-Sperre • Zugangsmanagement-Training • Richtlinie zum Löschen digitaler Assets • Löschrichtlinie für analoge Dateien	4.2 Organizational measures We implement the following organizational measures where relevant & viable; • Permission management using RBAC by admins, following the principle of least privilege • Minimum number of administrators • Data protection safe • Secure password policy & automation • "Clean desk" policy • General data protection & security guidelines • Manual desktop lock instructions • Access management training • Digital asset deletion policy • Analog files deletion policy

4.3 Informationen zu den Zugangskontrollen von Dienstanbietern Weitere Informationen zu Zugangskontrollen für wichtige Diensteanbieter (wie in Anlage 3 beschrieben) finden Sie auf den jeweiligen Websites.	4.3 Information regarding service provider access controls Additional information regarding access controls for key service providers (as outlined in Annex 3.) can be found on the respective websites.
5. Pseudonymisierung personenbezogener Daten Wir konzentrieren uns darauf, die Verarbeitung und Speicherung von Daten zu minimieren, wir unternehmen jedoch auch die folgenden Schritte, um Daten nach Möglichkeit zu pseudonymisieren; • Trennung der Verarbeitung von Gesundheitsdaten und Patientenprofildaten (personenbezogene Daten), soweit möglich, um die Verarbeitung von Gesundheitsdaten zu vermeiden • Allgemeiner Patientenschulungsplan und Übergabe-URL anstelle einer individualisierten URL *Hinweis: Dies gilt nur bei Verwendung eines generischen (nicht individualisierten) Patientenschulungsplans*	5. Pseudonymisation of personal data We focus on minimizing the processing & storage of data; however we also take the following steps to pseudonymize data where possible; • Separation of processing of health data and patient profile data (PII), where possible, to avoid processing PHI • Generic Patient Education Plan & handover URL, rather than an individualized URL *note: this only applies when using a generic (non-individualized) Patient Education Plan*

6. Verschlüsselung personenbezogener Daten 6.1.Strikte Durchsetzung der Transport Layer Security (TLS) 6.2.Verschlüsselung im Ruhezustand für ephemere (flüchtige) Daten 6.3.Datenspeicherung (Mongo-Atlas): 6.3.1. VPC-Sharing zwischen Infrastruktur und Daten 6.3.2. E2E-Verschlüsselung/RBAC/Netzwerkisolierung 6.3.3. Restdatenverschlüsselung 6.3.4. Verschlüsselung auf Feldebene	6. Encryption of personal data 6.1 Strict Transport Layer Security (TLS) enforcement 6.2.Encryption at rest for ephemeral data 6.3.Data storage (Mongo Atlas): 6.3.1. VPC sharing between infrastructure & data 6.3.2. E2E encryption/RBAC/Network Isolation 6.3.3. Rest data encryption 6.3.4. Field level Encryption
7. Vertraulichkeit, Integrität, Verfügbarkeit Dieser Abschnitt enthält zusätzliche Informationen darüber, wie wir und unsere Serviceanbieter die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit unterstützen. 7.1.Vertraulichkeit 7.1.1.Implementierung eines sicheren Authentifizierungsverfahrens • Gemäß Abschnitt 5 7.1.2 Schutz vor äußeren Einflüssen • Gemäß Abschnitt 1.1. 7.1.3. Tools und Prozesse zur Datenverschlüsselung • Offenlegung ggf. in anonymisierter oder pseudonymisierter Form • gemäß Abschnitt 7. 7.1.4 Überwachung von organisatorischen Abläufen, internen Regelungen und vertraglichen Verpflichtungen	7. Confidentiality, Integrity, Availability This section outlines additional information regarding how we & our service providers support the security goals of Confidentiality, Integrity, and Availability. 7.1 Confidentiality 7.1.1 Implementation of a secure authentication procedure • As per section 5 7.1.2 Protection against external influences • As per section 1.1. 7.1.3 Data encryption tools & processes • Disclosure in anonymous or pseudonymized form where relevant • as per section 7. 7.1.4 Monitoring of organisational processes, internal regulations, and contractual obligations

• Verwendung von Vanta als Tool zur Überwachung von Informationssicherheitsprozessen	• Use of Vanta as an information security process monitoring tool

7.2 Integrität 7.2.1 Einschränkung der Schreib- und Änderungsrechte • RBAC (rollenbasierte Zugriffsrechte) für Heroku & Mongo Atlas (Produktion) beschränkt auf Service- und Betriebsentwickler • Berechtigungen zum Ändern von Datenbanken sind auf einen einzelnen Mikrodienst beschränkt • Änderungsanträge für sichere Daten, die gegebenenfalls auf bestimmte Dienste beschränkt sind 7.2.2 Schutz vor äußeren Einflüssen • Arbeitsinstrumente → Google Workspace-Sicherheit • Infrastruktur → Heroku Private Space • Daten → Mongo Atlas Sicherheit 7.2.3 Zugriffsprotokolle • Siehe Abschnitt 2.	7.2 Integrity 7.2.1 Restriction of write and modification permissions • RBAC for Heroku & Mongo Atlas (production) limited to services & operations developers • Database modification permissions are limited to a single micro-service • Modification requests for secure data limited to specific services where relevant 7.2.2 Protection against external influences • Tools → Google Workspace Security • Infrastructure → Heroku Private Space • Data → Mongo Atlas Security 7.2.3 Access Logs • See section 2.
7.3 Verfügbarkeit 7.3.1 Automatisierte Backups • Daten → Mongo-Atlas • Infrastruktur → Heroku • Transaktionen → SumoLogic (über Heroku) 7.3.2 Schutz vor äußeren Einflüssen	7.3 Availability 7.3.1 Automated backups • Data → Mongo Atlas • Infrastructure → Heroku • Transactions → SumoLogic (via Heroku) 7.3.2 Protection against external influences

• API-Dienste sind mit Heroku geschützt • JWT-Authentifizierung und -autorisierung mit Auth0 7.3.3 Redundanz Einige Redundanzen werden von unseren Dienstleistern bereitgestellt • Daten → Mongo-Atlas • Infrastruktur → Heroku 7.3.4 Plan für die Wiederherstellung der Verarbeitungsaktivität • Notfallwiederherstellungs Plan 7.3.5 Dokumentation der Datensyntax • Dokumentation der Erstellung und Änderung von inhaltlichen Datenmodellen • Ubiquitäres Sprachglossar	• API services are protected using Heroku • JWT authentication & authorisation using Auth0 7.3.3 Redundancy Some redundancy is provided by our service providers • Data → Mongo Atlas • Infrastructure → Heroku 7.3.4 lan for restoring processing activity • Disaster Recovery Plan 7.3.5 Data syntax documentation • Documentation of content data model creation & modification • Ubiquitous Language Glossary

8. Lieferantenmanagement Wir verwenden die folgenden technischen und organisatorischen Maßnahmen, um sicherzustellen, dass unsere Lieferanten (einschließlich Dienstleister und Auftragnehmer) unsere Informationssicherheitsziele erfüllen; 8.1.Anwendung von Lieferanten-managementpraktiken • Sorgfältige Auswahl der Lieferanten hinsichtlich Datenschutz und Informationssicherheit • Verpflichtung der Mitarbeiter des Lieferanten zur Wahrung des Datengeheimnisses • Prüfung der vom Lieferanten getroffenen Sicherheitsmaßnahmen und deren Dokumentation 8.2 Abschluss von Auftragsverarbeitungsverträgen, falls erforderlich • Abschluss der erforderlichen Vereinbarung zur Auftragsverarbeitung oder EU-Standardvertragsklauseln • Vereinbarung über wirksame Kontrollrechte gegenüber dem Lieferanten 8.3 Regelmäßige Überprüfung von Lieferanten & und deren Informationssicherheitspolitik & -standards	8. Supplier Management We use the following technical & organizational measures to ensure that our suppliers (including services providers & contractors) fulfill our information security objectives; 8.1 Use of supplier management practices • Careful Selection of suppliers with regard to data protection and information security • Obligation of the supplier's employees to maintain data secrecy • Examination of the security measures taken by the supplier and their documentation 8.2 Use of Data Processing Agreements where required • Completion of the necessary agreement for order processing or EU - standard contractual clauses • Agreement on effective control rights vis-à-vis the supplier 8.3 Regular review of suppliers & and their information security policy & standards

Anlage 3 – Weitere Auftragsverarbeiter

Annex 3 - Other processors

In dieser Anlage sind die zugelassenen weiteren Auftragsverarbeiter aufgeführt, die von medudoc zur Durchführung der Auftragsabwicklung eingesetzt werden:

This annex specifies the other processors who are used by the medudoc to perform the order processing:

Name, legal form, contact details and address of the subcontractor	Description of the partial service	Beschreibung der Teilleistung
medudoc education GmbH Address :medudoc education, c/o Mindspace, Münzstraße 12, 10178 Berlin, Germany Contact person: dpo@medudoc.com	medudoc education GmbH is an affiliated company of medudoc education GmbH and medudoc ag, it provides all technical services within the medudoc-group. All other processors listed on our website provide their services for and on behalf of medudoc education GmbH	medudoc education GmbH ist eine mit der medudoc education GmbH und medudoc ag verbundene Gesellschaft, sie erbringt alle technischen Dienstleistungen innerhalb der medudoc-Gruppe. Alle auf unserer Website aufgeführten weiteren Auftragsverarbeiter erbringen ihre Dienstleistungen für und im Auftrag der medudoc education GmbH

Der jeweils aktuelle Stand der weiteren Auftragsverarbeiter nach Änderungen oder weiterer Hinzuziehungen kann unter www.medudoc.com eingesehen werden.

Dort können zudem die weiteren Auftragsverarbeiter der vorgenannten weiteren Auftragsverarbeiter eingesehen werden.

The current status of the other processors after changes or further involvement can be viewed at www.medudoc.com.

The other processors of the aforementioned other processors can also be viewed there.