Anlage zu den Nutzungsbedingungen

Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO

§ 1
Anwendungsbereich

Die vorliegende Vereinbarung legt die Bedingungen fest, gemäß derer Doctolib, in der Eigenschaft als Auftragsverarbeiter, sich verpflichtet, für den Abonnenten und/oder Nutzer, in seiner Eigenschaft als Verantwortlicher der Datenverarbeitung, die nachfolgend definierten Auftragsverarbeitungen vornimmt.

Die Parteien verpflichten sich im Rahmen ihrer Vertragsbeziehungen, die geltenden und anwendbaren datenschutzrechtlichen Bestimmungen einzuhalten und insbesondere die DSGVO.

§ 2
Begriffsbestimmungen

Die für die vorliegende Vereinbarung geltenden Begriffsbestimmungen sind hier einsehbar.

§ 3
Gegenstand und Dauer des Auftrags

(1) Gegenstand des Auftrags ist die Verarbeitung der personenbezogenen Daten des Nutzer oder Abonnenten durch Doctolib im Rahmen der in der Leistungsbeschreibung festgelegten Zwecken.

(2) Der Auftrag beschränkt sich auf die Installation, Bereitstellung und das Hosting der Anwendung und des Portals. Auf ausdrücklichen Wunsch des Abonnenten und unter seiner Kontrolle und Verantwortung kann Doctolib ihn zusätzlich dabei unterstützen, die personenbezogenen Daten seiner Patienten in die Anwendung zu importieren.

(3) Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der AGB und ANB.

(4) Der Abonnent kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß von Doctolib gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrags vorliegt, Doctolib eine Weisung des Abonnenten nicht ausführt oder Doctolib Kontrollrechte des Abonnenten vertragswidrig verweigert.

§ 4
Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten (Art. 4 Nr. 2 DSGVO) sowie die von Doctolib eingerichteten technischen und organisatorischen Massnahmen sind in den Anhängen zu diesem Vertrag festgelegt, welche vollständiger Vertragsbestandteil des vorliegenden Auftragsverarbeitungsvertrages sind.

(2) Die in **Anhang 1 und 2** festgelegten Datenarten oder -kategorien sind Gegenstand der Verarbeitung durch Doctolib (Art. 4 Nr. 1 DSGVO):

- **Anhang 1**: Terminkalenderverwaltung
- **Anhang 2**: Videosprechstunde

(3) Der Kreis der durch den Umgang mit ihren personenbezogenen Daten Betroffenen ergibt sich aus **Anhang 1 und 2**.

(4) Sofern nicht ausdrücklich abweichend vereinbart, findet die Erbringung der vertraglich vereinbarten Datenverarbeitung ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland erfolgt nur, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z.B. Angemessenheitsbeschluss, Binding Corporate Rules oder Standardvertragsklauseln). Bei einer nachträgliche Verlagerung ins EU-Ausland wird Doctolib den Nutzer im Vorfeld informieren.

§ 5
Verantwortlichkeit und Weisungsbefugnis

(1) Der Nutzer ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an Doctolib sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich. Er kann jederzeit die Herausgabe, Berichtigung, Löschung und Sperrung der Daten verlangen.

(2) Doctolib darf Daten ausschließlich im Rahmen der Weisungen des Abonnenten erheben, verarbeiten oder nutzen. Eine Weisung ist die auf einen bestimmten Umgang von Doctolib mit personenbezogenen Daten gerichtete schriftliche Anordnung des Abonnenten. Die Weisungen werden zunächst durch die ANB oder AGB definiert und können von dem Nutzer danach in der Regel schriftlich oder in einem dokumentierten elektronischen Format durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden.

(3) Doctolib hat den Nutzer unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Doctolib ist berechtigt, die

Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Nutzer bestätigt oder geändert wird.

(4) Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf Doctolib nur nach vorheriger schriftlicher Zustimmung durch den Nutzer erteilen.

(5) Doctolib verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Abonnenten nicht erstellt. Doctolib darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Abonnenten berichtigen, löschen oder deren Verarbeitung einschränken.

(6) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Abonnenten unmittelbar durch Doctolib sicherzustellen.

(7) Doctolib stellt dem Nutzer auf dessen Wunsch Informationen zur Aufnahme in das von ihm zu führende Verarbeitungsverzeichnis zur Verfügung.

(8) Eine Verarbeitung von personenbezogenen Daten in Privatwohnungen der Mitarbeiter von Doctolib (Fernzugriff, VPN, etc.) ist nicht zulässig.

§ 6
Beachtung zwingender gesetzlicher Pflichten durch Doctolib

(1) Neben den vertraglichen Regelungen dieser Vereinbarung und der AGB und ANB treffen Doctolib die nachfolgenden gesetzlichen Pflichten.

(2) Doctolib stellt sicher, dass die mit der Verarbeitung der Daten des Abonnenten befassten Mitarbeiter die Vertraulichkeit der Daten gemäß Art 28 Abs. 3, 29, 32 DSGVO wahren und diese entsprechend auf das Datengeheimnis verpflichtet und in die für sie relevanten Bestimmungen zum Datenschutz eingewiesen worden sind. Dies umfasst auch die Belehrung über die in diesem Auftragsverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.

(3) Sofern Doctolib verpflichtet ist nach den anwendbaren Vorschriften einen Datenschutzbeauftragten zu bestellen, wird er die Kontaktdaten des Datenschutzbeauftragten dem Nutzer zum Zwecke der direkten Kontaktaufnahme mitteilen.

(4) Doctolib informiert den Nutzer unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde wegen Verletzungen gegen datenschutzrechtliche Bestimmungen bei Doctolib ermittelt.

§ 7
Technisch-organisatorische Maßnahmen und deren Kontrolle

(1) Die Vertragsparteien vereinbaren die in dem **Anhang 1 und Anhang 2** zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen. Er ist Gegenstand dieser Vereinbarung.

(2) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es Doctolib gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in dem in **Anhang 1 und Anhang 2** festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(3) Doctolib wird dem Abonnenten auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte geben und die entsprechenden Nachweise verfügbar machen. Aufgrund der Kontrollverpflichtung des Abonnenten vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt Doctolib sicher, dass sich der Abonnent von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist Doctolib dem Abonnenten auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen nach. Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann dabei auch durch Vorlage eines aktuellen Testats, von Berichten unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden.

(4) Der Abonnent kann sich jederzeit zu Prüfzwecken in den von Doctolib zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsverarbeitung einschlägigen Datenschutzgesetze überzeugen.

§ 8
Mitteilung bei Verstößen durch Doctolib

(1) Doctolib unterstützt den Abonnenten bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen.

(2) Zu den Pflichten, bei denen Doctolib den Abonnenten unterstützt gehören u.a.

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;

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Nutzer zu melden;

c) die Verpflichtung, dem Nutzer im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;

d) die Unterstützung des Abonnenten für dessen Datenschutz-Folgenabschätzung sowie

e) die Unterstützung des Abonnenten im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

§ 9
Löschung und Rückgabe von Daten

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Abonnenten. Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Abonnenten bei Doctolib durch Maßnahmen Dritter (etwa durch Pfändungen oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat Doctolib den Nutzer unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist ausgeschlossen.

(2) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch des Abonnenten, jedoch spätestens mit Beendigung der ANB und AGB hat Doctolib sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigten Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Nutzer auszuhändigen oder nach vorheriger Zustimmung des Abonnenten datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Ein Löschungsprotokoll ist dem Nutzer auf Anforderung vorzulegen.

(3) Doctolib kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Nutzer übergeben.

§ 10
Unterauftragnehmer

(1) Doctolib ist berechtigt Unterauftragnehmer einzuschalten. Vor dem Einsatz von Unterauftragnehmern wird Doctolib den Nutzer hiervon unterrichten.

(2) Nicht als Leistungen von Unterauftragnehmern im Sinne dieser Regelung gelten Dienstleistungen, die Doctolib bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsdienstleistungen und Wartungen. Doctolib ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Abonnenten auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(3) Wenn Unterauftragnehmer durch Doctolib eingeschaltet werden, hat Doctolib sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem Unterauftragnehmer so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Nutzer und Docotlib entspricht und alle gesetzlichen und vertraglichen Pflichten beachtet werden und die Verantwortlichkeiten klar abgrenzt.

(4) Dem Nutzer sind in der vertraglichen Vereinbarung mit dem Unterauftragnehmer Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Ebenso ist der Nutzer berechtigt, auf schriftliche Anforderung von Doctolib Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten.

§ 11
Nebenleistungen

Die §§ 1 bis 8 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

§ 12
Datenschutzkontrolle

Doctolib verpflichtet sich, dem/der betrieblichen Datenschutzbeauftragten des Abonnenten zur Erfüllung seiner jeweiligen gesetzlichen Aufgaben im Zusammenhang mit diesem Auftrag jederzeit Zugang zu den üblichen Geschäftszeiten zu gewähren.

Anlage 1 zur Vereinbarung zur Auftragsverarbeitung

Konkretisierung des Auftrags - Kalenderservice

Die nachstehende Tabelle konkretisiert den an Doctolib erteilten Auftrag für den Kalenderservice, gibt die technischen und organisatorischen Maßnahmen von Doctolib wider, und stellt ein Musterdatenverarbeitungsblatt dar, welches Ärzte, Krankenhäuser, MVZ und Kliniken in ihr eigenes Verzeichnis von Verarbeitungstätigkeiten einpflegen können (Artikel 30 DSGVO). Wird diese Anlage für das eigene Verzeichnis der Verarbeitungstätigkeiten genutzt, können die farblich markierten Zellen je nach den Besonderheiten der Einrichtung ausgefüllt werden.

Allgemeine Informationen	
Name der Verarbeitung	Verwaltung von Terminen und Kalendern
Datum des Beginns der Verarbeitungstätigkeit	
Aktualisierung	
Datenschutzrechtl. Einordnung des Unternehmens	Verantwortlicher für die Verarbeitung
genutzte Anwendung	Doctolib
Betroffene Abteilungen	

Verantwortlicher für die Datenverarbeitung	
Name des Unternehmens	
Handelsregisternummer	
Handelsregister	
Adresse	
Telefon	
E-Mail Adresse	

Datenschutzbeauftragter	
Name Vorname	
Adresse	
Telefon	
E-Mail Adresse	
Externer DPO	
Name des Unternehmens	
Handelsregisternummer	
Handelsregister	

Vertreter	
Name Vorname	
Adresse	
Telefon	
E-Mail Adresse	

Gemeinsam Verantwortlicher für die Datenverarbeitung	
Name des Unternehmens	
Handelsregisternummer	
Adresse	
Telefon	

E-Mail Adresse	
Kontakt	

Zwecke der Verarbeitung	
Hauptzweck	**Verwalten eines Online-Terminkalenders und von Terminen**
Weiterer Zweck 1	Möglichkeit für Patienten und ihre Angehörigen, Termine online zu vereinbaren
Weiterer Zweck 2	Online-Tool zur Terminkalenderverwaltung
Weiterer Zweck 3	Patienten über Ärzte informieren
Weiterer Zweck 4	E-Mail und SMS-Benachrichtigungen verschicken

Technische und organisatorische Maßnahmen	
	<u>Sicherheit der Doctolib Anwendung</u> ● starke Authentifizierung (2FA oder multiple Faktoren): ein Identifikationscode wird bei jeder Anmeldung auf das Telefon geschickt ● starke Passwortpolitik: mind. 8 Zeichen, darunter Zahlen, Symbole, Buchstaben, Großbuchstaben. Naheliegende Passwörter sind verboten (z.B. Login, Name, einfache Zahlenfolgen). ● Sitzungsschutz: Neben manueller Schließung laufen offene Sitzungen ohne Interaktionen automatisch nach einer definierten Zeit ab. Diese können danach nur mit einem Pincode entsperrt werden. ● Sicherer Wiederherstellungsprozess: Vor jeder Datenwiederherstellung werden zuerst alle Kontoinformationen überprüft. ● Rollenbasierte Zugriffskontrolle: Administratoren können jedem Benutzer innerhalb ihrer Organisation spezifische Rechte zuweisen. ● Rückverfolgbarkeit: Protokollierung aller Aktionen auf dem Konto / Organisation / Tagesordnung ● Kontoabsicherung: Das Konto wird gegen unerlaubte Zugriffe gesichert, indem Logins nach 10 falschen Versuchen blockiert werden **<u>Sicherheit der Doctolib Plattform</u>** ● Automatische Sicherheitsupdates ● Modernste und voll aktualisierte Betriebssysteme ● Sicherheitsüberwachung: Kontinuierliche Überwachung von Bedrohungen, Schwachstellen oder Angriffsmuster ● Firewalls und dedizierte Zugangsfiltersysteme (Proxy, vpn....) ● Schutz von Systemen gegen DDoS-Angriffe (Distributed Denial of Service) ● Schutz gegen Angriffe auf Webanwendungen (WAF) ● Rückverfolgbarkeit: Aufzeichnung aller Aktionen; Überwachung und Alarmierung aller Sicherheitsereignisse

- Sichere Rechenzentren: HDS, ISO 27001, Tier 3, starke physische Sicherheit, Mitarbeiter vor Ort 24 Stunden/Tag 7 Tage /Woche.

Verfügbarkeit der Plattform Doctolib

- Alle Daten werden in mehreren Rechenzentren repliziert.
- Jedes Rechenzentrum verfügt über mehrere externe Netzwerkverbindungen.
- Alle Dienste und Komponenten sind durch Business Recovery Verfahren abgedeckt, die meist automatisch ablaufen.
- Fehler werden automatisch erkannt und lösen dank eines kompletten Überwachungssystems für jede technische Komponente und jeden Business Service eine Warnung aus.
- Implementierung einer Backup- und Wiederherstellungsguideline

Verschlüsselung der Daten durch Doctolib

- Kommunikation und Datentransfer: Alle mit und zwischen den Systemen ausgetauschten Daten werden mit dem Protokoll TLS 1.2 und einem großen Schlüssel (4096 Bit) verschlüsselt, bei Bedarf nutzt Doctolib darüber hinaus einen IPSec-Tunnel.
- Datenspeicherung: Doctolib verwendet AES 256, einen robusten und anerkannten Verschlüsselungsalgorithmus.
- End-to-End-Verschlüsselung: Verschlüsselung vertraulicher Arzt-/Patientendaten, so dass kein Doctolib-Mitarbeiter oder eine andere Person diese Daten lesen, ändern oder abrufen kann.

Zugriff der Mitarbeiter von Doctolib

- Alle gewährten und widerrufene Zugriffe werden gemäß einem strengen und aktuellen zentralisierten Prozess überwacht und zentral gespeichert.
- Support-, Vertriebs- oder Engineering-Teams haben keinen Zugriff auf Bankdaten oder Video-Feeds
- Bei Gesundheitsdaten kann der Arzt oder der Patient selbst einem Mitglied des Supportteams vorübergehend Zugriff zu den Daten gewähren, falls dies erforderlich ist oder im Falle einer Untersuchung oder eines Streitverfahrens.
- Speziell geschulte Mitglieder des Doctolib-Infrastrukturteams können, falls erforderlich und in Abstimmung mit dem Abonnenten, auf die Daten für den Betrieb der Plattform zugreifen.

Physischer Zugang der Mitarbeiter von Doctolib

- Die Büroräume von Doctolib sind alarmgesichert und mit modernsten Sicherheits- und Zugangskontrollsystemen versehen.
- Jeder berechtigte Zugang zu den Räumlichkeiten wird protokolliert
- Besucher dürfen die Räumlichkeiten nur nach Anmeldung betreten und sich nur in Begleitung eines Doctolib Mitarbeiter dort aufhalten. Während des Besuches eines Dritten wird dieser Dritte nie unbeobachtet oder allein gelassen.
- Alle Systeme werden in zertifizierten Hochsicherheitsrechenzentren betrieben. Diese sind neben Sicherheitssystemen videoüberwacht und mit einem Wachdienst

	ausgestattet. Nur eine kleine Gruppe speziell geschulter Doctolib Spezialisten haben hier eine Zugangsberechtigung. Jeder dieser Zugänge wird protokolliert. **Zugriff der Mitarbeiter des Arztes** ● Die Maßnahmen der Zugriffssicherung, die der Arzt getroffen hat, sind vom Arzt selbst darzustellen. **Best practices im Bereich Sicherheit** ● Doctolib Passwörter werden mit einer sehr robusten Hash-Funktion (bcrypt) gehasht. ● Systematische Risikominimierung: Doctolib schützt seine Dienste und deren Benutzer systematisch vor Angriffen, wie z.B. die Reduzierung der Systemverfügbarkeit durch Denial-of-Service Attacken, Brut-Force Angriffe um sich unerlaubt Zugänge zu den Systemen zu verschaffen. Hierbei kommen aktuelle Systeme wie z.B. Intrusion Detection Systems (zur Alarmierung und Verhinderung von unerlaubten Zugriffen) und automatisierte Datensicherungssysteme zum Einsatz. ● Vorgabe von Security Headern ● Quellcode-Überprüfung: Der Quellcode von Doctolib wird von Code-Validierungstools und unserem Sicherheitsteam permanent überprüft, um Schwachstellen zu erkennen. ● Intrusionstests: Doctolib beauftragt regelmäßig anerkannte Unternehmen, Intrusionstests auf seinen Anwendungen und Plattformen durchzuführen. ● Geschultes Sicherheitsbewusstsein, Training: Doctolib Entwickler und Mitarbeiter werden regelmäßig zum Thema Informationssicherheit geschult und überprüft. ● Doctolib wendet das Prinzip des geringst nötigsten Zugang an: Es wird nur ein minimaler Zugang gewährt. **Verbindung mit der Software des Arztes** Die Verbindung mit der Software des Arztes kann auf mehrere Arten hergestellt werden (Zutreffendes ankreuzen) Schnittstelle zwischen dem Doctolib Kalender und dem Kalender des Informatiksystems ❑ lokale Schnittstelle, Doctolib Kalender ermöglicht, die Patientendaten aus dem Informatiksystem einzupflegen ❑ VPN IP Sec zwischen dem Server und Doctolib (zur Bestätigung der Verfügbarkeit)

Verarbeitete Daten		
Kategorie der Daten	**Beschreibung**	**Löschfrist**
Familienstand, Identität, Identifikationsdaten, Bilder....	**Benutzerkonto des Arztes:** Name, Vorname, Geburtsdatum, Position, E-Mail-Adresse, Mobiltelefon **Profildaten des Arztes :**	**Kontodaten und Profil des Arztes:** 3 Monate im Falle einer Vertragsbeendigung **Innerhalb des Patientenkontos:**

	Nachname, Vorname, Personenstand, Titel, Kurzname für SMS, Adresse des Behandlungsortes, Fotografien, Arztnummer **Patientendaten:** Name, Vorname, Geburtsdatum, Telefonnummer, E-Mail-Adresse Herkunft (sofern erforderlich), ggf. überweisender Arzt, durch den Arzt eingegebene Notizen	Löschung des Kontos auf Verlangen des Nutzers, Erinnerung an die Möglichkeit, die Daten nach 3 Jahren Inaktivität zu löschen **Innerhalb des Arztkontos:** 10 Jahre nach dem Termin für selbständige Ärzte, 20 Jahre für Gesundheitseinrichtungen. Die Daten werden jedoch innerhalb von 3 Monaten nach Ende der Vertragsbeziehung mit dem Arzt gelöscht.
Vita	**Profildaten des Arztes :** Medizinische und universitäre Ausbildung, Titel (in Krankenhäusern oder Kliniken), Werke und Publikationen, Preise und Auszeichnungen, Verbände, Fachgebiete, Präsentation, gesprochene Sprache, Link zur Website, konventioneller Bereich, Behandlungsangebot ohne Voranmeldung	3 Monate im Falle der Vertragsbeendigung
Zahlungsinformationen	**Profildaten des Arztes** akzeptierte Zahlungsmittel, Honorar	3 Monate im Falle der Vertragsbeendigung
Verbindungsdaten (IP, logs, etc.)	IIP-Adressen, Sitzungs-IDs, Client-Terminal-IDs	2 Monate
Ortungsdaten		

Besondere Kategorien personenbezogener Daten		
Kategorie der Daten	**Beschreibung**	**Löschfrist**
Daten über die rassische und ethnische Herkunft		
Daten über die politische Meinung		
Religion und Weltanschauung		
Gewerkschaftszugehörigkeit		
Genetische Daten		
Biometrische Daten		

Gesundheitsdaten	**Patientendaten** : Grund für die Terminvereinbarung mit dem Arzt, Häufigkeit der vom Arzt durchgeführten Termine, durch den Arzt eingetragene Notizen, Fachgebiet des Arztes, ggf. überweisender Arzt	**Innerhalb des Patientenkontos:** Löschung des Accounts auf Wunsch des Nutzers, Erinnerung an die Möglichkeit der Löschung seiner Daten nach 3 Jahren Inaktivität. **Innerhalb des Arzt-Kontos:** 10 Jahre nach dem Termin für selbständige Ärzte, 20 Jahre für Gesundheitseinrichtungen. Die Daten werden jedoch innerhalb von 3 Monaten nach Ende der Vertragsbeziehung mit dem Arzt gelöscht.
Daten über das Sexualleben oder die sexuelle Orientierung		
Daten über strafrechtliche Verurteilungen oder Rechtsverstöße		
Identifikationsnummer des Arztes		

Kreis der Betroffenen	
Kreis der Betroffenen 1	Patienten
Kreis der Betroffenen 2	Personal/Mitarbeiter des Arztes

Auftragnehmer, Unterauftragnehmer, Empfänger	
Auftragnehmer	Doctolib GmbH
Beschreibung	Plattformbetreiber
Adresse	Wilhelmstr. 118, Aufgang C
Datenschutzbeauftrager	Justine Bourdeu
E-Mail	datenschutz@doctolib.com
Unterauftragnehmer	1. Doctolib SAS 2. AZ Network ; Coreye; AWS 3. Mailjet, SMS Mode; Balthazar et Compagnie,
Beschreibung	1. Muttergesellschaft von Doctolib GmbH 2. Hosting-Unternehmen speziell für Gesundheitsdaten (Health Data Hosting) 3. Dienstleister für Terminerinnerungen

Anlage 2 zur Vereinbarung zur Auftragsverarbeitung

Konkretisierung des Auftrags - Telekonsultationsservice

Die nachstehende Tabelle konkretisiert den an Doctolib erteilten Auftrag für den Telekonsultationsservice, gibt die technischen und organisatorischen Maßnahmen von Doctolib wider, und stellt ein Musterdatenverarbeitungsblatt dar, welches Ärzte, Krankenhäuser, MVZ und Kliniken in ihr eigenes Verzeichnis von Verarbeitungstätigkeiten einpflegen können (Artikel 30 DSGVO). Wird diese Anlage für das eigene Verzeichnis der Verarbeitungstätigkeiten genutzt, können die farblich markierten Zellen je nach den Besonderheiten der Einrichtung ausgefüllt werden.

Allgemeine Informationen	
Name der Verarbeitung	Telekonsultationsservice
Datum des Beginns der Verarbeitungstätigkeit	
Aktualisierung	
Datenschutzrechtl. Einordnung des Unternehmens	Verantwortlicher für die Verarbeitung
genutzte Anwendung	Doctolib
Betroffene Abteilungen	

Verantwortlicher für die Datenverarbeitung	
Name des Unternehmens	
Handelsregisternummer	
Handelsregister	
Adresse	
Telefon	
E-Mail Adresse	

Datenschutzbeauftragter	
Name Vorname	
Adresse	
Telefon	
E-Mail Adresse	
Externer DPO	
Name des Unternehmens	
Handelsregisternummer	
Handelsregister	

Vertreter	
Name Vorname	
Adresse	
Telefon	
E-Mail Adresse	

Gemeinsam Verantwortlicher für die Datenverarbeitung	
Name des Unternehmens	
Handelsregisternummer	
Adresse	

Telefon	
E-Mail Adresse	
Kontakt	

Zwecke der Verarbeitung	
Hauptzweck	**Ermöglichen der Telekonsultation**
Weiterer Zweck 1	Möglichkeit für Patienten und ihre Angehörigen, Termine für die Telekonsultation online zu vereinbaren
Weiterer Zweck 2	Telekonsultations-Tool mit Videoübertragung
Weiterer Zweck 3	Erlaubt die Übermittlung von Dokumenten an Patienten über das Ärzteprofil (Rezepte, ärztliche Berichte, Gebührenrechnungen)

Technische und organisatorische Maßnahmen	
	<u>Sicherheit der Doctolib Anwendung</u> ● starke Authentifizierung (2FA oder multiple Faktoren): ein Identifikationscode wird bei jeder Anmeldung auf das Telefon geschickt ● starke Passwortpolitik: mind. 8 Zeichen, darunter Zahlen, Symbole, Buchstaben, Großbuchstaben. Naheliegende Passwörter sind verboten (z.B. Login, Name, einfache Zahlenfolgen). ● Sitzungsschutz: Neben manueller Schließung laufen offene Sitzungen ohne Interaktionen automatisch nach einer definierten Zeit ab. Diese können danach nur mit einem Pincode entsperrt werden. ● Sicherer Wiederherstellungsprozess: Vor jeder Datenwiederherstellung werden zuerst alle Kontoinformationen überprüft. ● Rollenbasierte Zugriffskontrolle: Administratoren können jedem Benutzer innerhalb ihrer Organisation spezifische Rechte zuweisen. ● Rückverfolgbarkeit: Protokollierung aller Aktionen auf dem Konto / Organisation / Tagesordnung ● Kontoabsicherung: Das Konto wird gegen unerlaubte Zugriffe gesichert, indem Logins nach 10 falschen Versuchen blockiert werden **<u>Sicherheit der Doctolib Plattform</u>** ● Automatische Sicherheitsupdates ● Modernste und voll aktualisierte Betriebssysteme ● Sicherheitsüberwachung: Kontinuierliche Überwachung von Bedrohungen, Schwachstellen oder Angriffsmuster ● Firewalls und dedizierte Zugangsfiltersysteme (Proxy, vpn....) ● Schutz von Systemen gegen DDoS-Angriffe (Distributed Denial of Service) ● Rückverfolgbarkeit: Aufzeichnung aller Aktionen; Überwachung und Alarmierung aller Sicherheitsereignisse ● Sichere Rechenzentren: HDS, ISO 27001, Tier 3, starke physische Sicherheit, Mitarbeiter vor Ort 24 Stunden/Tag 7 Tage /Woche. **<u>Verfügbarkeit der Plattform Doctolib</u>**

- Alle Daten werden in mehreren Rechenzentren repliziert.
- Jedes Rechenzentrum verfügt über mehrere externe Netzwerkverbindungen.
- Alle Dienste und Komponenten sind durch Business Recovery Verfahren abgedeckt, die meist automatisch ablaufen.
- Fehler werden automatisch erkannt und lösen dank eines kompletten Überwachungssystems für jede technische Komponente und jeden Business Service eine Warnung aus.
- Implementierung einer Backup- und Wiederherstellungsguideline

Verschlüsselung der Daten durch Doctolib

- Kommunikation und Datentransfer: Alle mit und zwischen den Systemen ausgetauschten Daten werden mit dem TLS Protokoll verschlüsselt. Dieses Protokoll ist so konfiguriert, dass es den besten Kompromiss zwischen Kompatibilität und Sicherheit bietet. Bei Bedarf nutzt Doctolib darüber hinaus einen IPSec-Tunnel.
- Datenspeicherung: Alle unsere Datenbanken sind at rest verschlüsselt. Die sensibelsten Daten unterliegen einer zusätzlichen Verschlüsselungsebene, so dass sie für Datenbankadministratoren nicht lesbar sind.
- Ende zu Ende Verschlüsselung: Die Vertraulichkeit von Videokonsultationen, die über den Doctolib-Dienst durchgeführt werden, wird durch die Verschlüsselung der End-to-End-Ströme von Patient und Arzt gewährleistet. Diese Ströme gehen nicht durch die Infrastruktur von Doctolib. Beim Start der Videosprechstunde wird eine Peer-to-Peer Verbindung zwischen Arzt und Patient aufgebaut. In äußerst seltenen Fällen, in denen dies nicht möglich ist, wird die Verbindung durch einen innerhalb Deutschlands betriebenen TURN-Server initiiert. In beiden Fällen handelt es sich um eine Ende-zu-Ende verschlüsselte Verbindung ausschließlich zwischen Doktor und Patient, die von keinem Dritten abgehört oder eingesehen werden kann.

Zugriff der Mitarbeiter von Doctolib

- Alle gewährten und widerrufene Zugriffe werden gemäß einem strengen und aktuellen zentralisierten Prozess überwacht und zentral gespeichert.
- Support-, Vertriebs- oder Engineering-Teams haben keinen Zugriff auf Bankdaten oder Video-Feeds
- Bei Gesundheitsdaten kann der Arzt oder der Patient selbst einem Mitglied des Supportteams vorübergehend Zugriff zu den Daten gewähren, falls dies erforderlich ist oder im Falle einer Untersuchung oder eines Streitverfahrens.
- Speziell geschulte Mitglieder des Doctolib-Infrastrukturteams können, falls erforderlich und in Abstimmung mit dem Auftraggeber, auf die Daten für den Betrieb der Plattform zugreifen.

Physischer Zugang der Mitarbeiter von Doctolib

- Die Büroräume von Doctolib sind alarmgesichert und mit modernsten Sicherheits- und Zugangskontrollsystemen versehen.

- Jeder berechtigte Zugang zu den Räumlichkeiten wird protokolliert
- Besucher dürfen die Räumlichkeiten nur nach Anmeldung betreten und sich nur in Begleitung eines Doctolib Mitarbeiter dort aufhalten. Während des Besuches eines Dritten wird dieser Dritte nie unbeobachtet oder allein gelassen.
- Alle Systeme werden in zertifizierten Hochsicherheitsrechenzentren betrieben. Diese sind neben Sicherheitssystemen videoüberwacht und mit einem Wachdienst ausgestattet. Nur eine kleine Gruppe speziell geschulter Doctolib Spezialisten haben hier eine Zugangsberechtigung. Jeder dieser Zugänge wird protokolliert.

Zugriff der Mitarbeiter des Arztes

- Hier sind die Maßnahmen der Zugriffssicherung des Arztes darzustellen (MFAs)

Best practices im Bereich Sicherheit

- Doctolib Passwörter werden mit einer sehr robusten Hash-Funktion (bcrypt) gehasht.
- Systematische Risikominimierung: Doctolib schützt seine Dienste und deren Benutzer systematisch vor Angriffen, wie z.B. die Reduzierung der Systemverfügbarkeit durch Denial-of-Service Attacken, Brut-Force Angriffe um sich unerlaubt Zugänge zu den Systemen zu verschaffen. Hierbei kommen aktuelle Systeme wie z.B. Intrusion Detection Systems (zur Alarmierung und Verhinderung von unerlaubten Zugriffen) und automatisierte Datensicherungssysteme zum Einsatz.
- Vorgabe von Security Headern
- Quellcode-Überprüfung: Der Quellcode von Doctolib wird von Code-Validierungstools und unserem Sicherheitsteam permanent überprüft, um Schwachstellen zu erkennen.
- Intrusionstests: Doctolib beauftragt regelmäßig anerkannte Unternehmen, Intrusionstests auf seinen Anwendungen und Plattformen durchzuführen.
- Geschultes Sicherheitsbewusstsein, Training: Doctolib Entwickler und Mitarbeiter werden regelmäßig zum Thema Informationssicherheit geschult und überprüft.
- Doctolib wendet das Prinzip des geringst nötigsten Zugang an: Es wird nur ein minimaler Zugang gewährt.

Sicherer Software-Entwicklungslebenszyklus (S-SDLC)

Awareness, Sicherheitstraining: Entwickler werden geschult und auf die Best Practices im Bereich Sicherheit hingewiesen.

- Sicherheit ab der Entwurfsphase: Jede neue Funktion des Doctolib-Produkts wird in Zusammenarbeit mit Experten für IT-Sicherheit entworfen.
- Überprüfung des Quellcodes :
    - Jede Änderung des Quellcodes von Doctolib wird automatisch analysiert.
    - Manuelle Überprüfungen des Quellcodes werden durchgeführt, wenn die Änderung eine sensible Komponente betrifft.
- Suche nach Schwachstellen :
    - Penetrationstests: Doctolib beauftragt regelmäßig anerkannte Unternehmen mit der

	Durchführung von Penetrationstests für unsere Anwendungen und Plattformen. ○ Programm zur Entdeckung von Schwachstellen (Bug-Bounty): Mitarbeiter und externe Forscher werden belohnt, wenn sie einen Sicherheitsmangel in Doctolibs Produkt identifizieren.

Verarbeitete Daten		
Kategorie der Daten	**Beschreibung**	**Löschfrist**
Familienstand, Identität, Identifikationsdaten, Bilder....	**Benutzerkonto des Arztes:** Name, Vorname, Scan des Personalausweises **Patientendaten:** Name, Vorname, durch den Arzt eingegebene Notizen Videozuspielungen, die eine Videoübertragung zwischen Patient und Arzt während der Telekonsultation ermöglichen	**Kontodaten und Profil des Arztes:** 3 Monate im Falle einer Vertragsbeendigung **Innerhalb des Arztkontos:** 10 Jahre nach dem Termin für selbständige Ärzte, 20 Jahre für Gesundheitseinrichtungen. Die Daten werden jedoch innerhalb von 3 Monaten nach Ende der Vertragsbeziehung mit dem Arzt gelöscht.
Zahlungsinformationen	**Profildaten des Arztes** akzeptierte Zahlungsmittel, Drittzahler, Honorar, Gebühren	3 Monate im Falle der Vertragsbeendigung
Verbindungsdaten (IP, logs, etc.)	Verbindungsprotokolle der Videokonsultation	
Ortungsdaten		

Besondere Kategorien personenbezogener Daten		
Kategorie der Daten	**Beschreibung**	**Löschfrist**
Daten über die rassische und ethnische Herkunft		
Daten über die politische Meinung		
Religion und Weltanschauung		
Gewerkschaftszugehörigkeit		
Genetische Daten		
Biometrische Daten		
Gesundheitsdaten	**Patientendaten** : An den Patienten adressiertes Rezept, Telekonsultationsbericht oder andere Dokumente, die der Arzt	**Innerhalb des Patientenkontos:** Löschung des Accounts auf Wunsch des Nutzers, Erinnerung an die Möglichkeit

	über sein Doctolib-Konto an den Patienten übermittelt hat.	der Löschung seiner Daten nach 3 Jahren Inaktivität. **Innerhalb des Arzt-Kontos:** 10 Jahre nach dem Termin für selbständige Ärzte, 20 Jahre für Gesundheitseinrichtungen. Die Daten werden jedoch innerhalb von 3 Monaten nach Ende der Vertragsbeziehung mit dem Arzt gelöscht.
Daten über das Sexualleben oder die sexuelle Orientierung		
Daten über strafrechtliche Verurteilungen oder Rechtsverstöße		
Identifikationsnummer des Arztes		

Kreis der Betroffenen	
Kreis der Betroffenen 1	Patienten
Kreis der Betroffenen 2	Personal/Mitarbeiter des Arztes

Auftragnehmer, Unterauftragnehmer, Empfänger	
Auftragnehmer	Doctolib GmbH
Beschreibung	Plattformbetreiber
Adresse	Wilhelmstr. 118, Aufgang C, 10963 Berlin
Datenschutzbeauftrager	Justine Bourdeu
E-Mail	datenschutz@doctolib.de
Unterauftragnehmer	1. Doctolib SAS 2. AZ Network ; Coreye; AWS 3. Vonage (Tokbox Service) (nur Verbindungsprotokolle)
Beschreibung	1. Muttergesellschaft von Doctolib GmbH 2. Hosting-Unternehmen speziell für Gesundheitsdaten (Health Data Hosting) 3. Anbieter von Videoübertragungen
