Informationen zum Datenschutz

für die Videokommunikationsplattformen **web.doccura.de**

Der Schutz Ihrer Daten ist uns sehr wichtig. In diesen Datenschutzhinweisen informieren wir Sie entsprechend den gesetzlichen Vorgaben über die Verarbeitung personenbezogener Daten durch die Bayerische TelemedAllianz GmbH. Wir orientieren uns an der EU-Datenschutzgrundverordnung (DSGVO).

1. Allgemeine Informationen

Die Bayerische TelemedAllianz GmbH (BTA) bietet eine mobile Online-, Audio- und Videokommunikationsplattform Doccura an, bei dem Kunden und andere Nutzer in Kontakt treten und miteinander kommunizieren können. Doccura ermöglicht eine sichere, Ende-zu-Ende-verschlüsselte Videoverbindung zwischen zwei oder mehreren Nutzern von beliebigen mobilen oder stationären Endgeräten. Die Videokommunikation kann natürlich auch im Gesundheitswesen eingesetzt werden, dabei ist zu beachten, dass Doccura selbst keine medizinischen Leistungen erbringt, sondern lediglich eine Plattform zur Kommunikation bereitstellt.

Wir, die Bayerische TelemedAllianz GmbH, als die verantwortliche Stelle, nehmen den Schutz Ihrer Daten sehr ernst. Wir möchten, dass Sie wissen, welche Daten wir speichern und wie wir diese verwenden. Selbstverständlich halten wir dabei die gesetzlichen Bestimmungen zum Datenschutz strikt ein.

Personenbezogene Daten werden von uns nur gemäß den Bestimmungen der DSGVO verarbeitet. Nachfolgend informieren wir Sie über die Erhebung und Verwendung Ihrer personenbezogenen Daten. Diese Datenschutzhinweise beziehen sich auf unsere Software-Plattform auf den Webseiten www.web.doccura.de.

Falls Sie auf Links auf andere Seiten hingewiesen werden, informieren Sie sich bitte dort über den jeweiligen Umgang mit Ihren Daten.

ips Gütesiegel

Doccura wurde von der datenschutz cert GmbH für Informationssicherheit und Datenschutz gemäß dem Gütesiegelstandard ips® – internet privacy standards ausgezeichnet. Die umfassende Prüfung anhand der gesetzlichen Vorgaben gemäß Anlage 31b zum Bundesmantelvertrag – Ärzte SGB V erfolgte anhand des ips®-Standards, welcher bundesweit anerkannt wird und z.B. vom Bundesjustizministerium und Verbraucherschutzverbänden empfohlen wird.

Im Folgenden informieren wir Sie über den Umgang mit personenbezogenen Daten bei der Nutzung der Softwareplattform auf den Webseiten www.web.doccura.de. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Beispiele hierfür sind Name, Adresse oder E-Mail-Adresse.

1. Zweckgebundene Daten-Verwendung: Wir beachten den Grundsatz der zweckgebundenen Daten-Verwendung und erheben, verarbeiten und speichern Ihre personenbezogenen Daten nur für die Zwecke, für die Sie sie uns mitgeteilt haben. Eine Weitergabe Ihrer persönlichen Daten an Dritte erfolgt ohne Ihre ausdrückliche Einwilligung nicht, sofern dies nicht zur Erbringung der Dienstleistung oder zur Vertragsdurchführung notwendig ist. Auch die Übermittlung an auskunftsberechtigte staatliche Institutionen und Behörden erfolgt nur im Rahmen der gesetzlichen Auskunftspflichten oder wenn wir durch eine gerichtliche Entscheidung zur Auskunft verpflichtet werden.

2. Den unternehmensinternen Datenschutz nehmen wir sehr ernst. Unsere Mitarbeiter und die von uns beauftragten Dienstleistungsunternehmen sind von uns zur Verschwiegenheit und zur Einhaltung der datenschutzrechtlichen Bestimmungen verpflichtet worden.

2. Verantwortlicher

Verantwortlicher nach den Richtlinien der DSGVO im Zusammenhang mit den Services ist:

Bayerische TelemedAllianz GmbH (haftungsbeschränkt)
Brückenstraße 13 a
85107 Baar-Ebenhausen
Telefon: 0800 36 22 872
E-Mail: info@doccura.de

Weitere Informationen entnehmen Sie bitte unserem Impressum.

3. Datenschutzbeauftragter

Falls Sie fragen zu Ihrer Datensicherheit haben, oder weitergehende Informationen benötigen: schreiben Sie unserem Datenschutzbeauftragten (Dr. Eddie Kohfeldt) eine E-Mail an: datenschutz@doccura.de.

4. Erhebung personenbezogener Daten bei informatorischer Nutzung

1. Die IP-Adresse des Nutzers/Kunden wird (www.web.doccura.de) für max. 90 Tage gespeichert bzw. nach max. 90 Tagen gelöscht.
2. Diese Daten verwenden wir, um die Systemsicherheit sicherzustellen, Ihnen die Nutzung unserer Website zu ermöglichen sowie zur Verbesserung unserer Services.
3. Zweck der Verwendung personenbezogener Daten: Wir verwenden Ihre Daten zur Beantwortung Ihrer Anfragen und der Durchführung der von Ihnen über unsere Webseite angestoßenen Interaktionen.
4. Rechtsgrundlage für die Verwendung personenbezogener Daten: Die Verarbeitung Ihrer personenbezogenen Daten erfolgt daher ausschließlich aufgrund Ihrer Anfrage in einem vorvertraglichen Bereich und somit aufgrund der Rechtsgrundlage des Art. 6 Abs. 1 lit. b) DSGVO.

5. Verwendung von Cookies

1. Auf der Webseite www.web.doccura.de setzen wir Cookies der folgenden Klassifizierungen ein:

- Session-Cookies: Diese Art von Cookies wird mit Beendigung des Browsers gelöscht, sie haben nur für eine Browsersitzung Gültigkeit. Folgende Session-Cookies werden auf der Software-Website www.web.doccura.de gesetzt:

    1. apiCCId
        1. Ablaufzeit: Dauer der Session
        2. Verwendung: Dieses Cookie speichert die von der Kommunikations-API generierten Benutzer-ID.
        3. Beispielhafter Wert: 4
    2. apiKey
        1. Ablaufzeit: Dauer der Session
        2. Verwendung: Dieses Cookie ist der Schlüssel, der den Zugriff auf die Kommunikationsplattform und den Aufbau einer Videositzung mit anderen verbundenen Benutzern mit demselben API-Schlüssel ermöglicht.
        3. Beispielhafter Wert: de7a42c1af2ee2d7c560f2c9b7ba1b09
    3. _eb_token
        1. Ablaufzeit: Dauer der Session
        2. Verwendung: Dieses Cookie speichert das CSRF-Token, um eine Verbindung zwischen verschiedenen Benutzern herzustellen und zwischen verschiedenen Benutzern zu

unterscheiden. Dieses Cookie ist auch für die Betrugsprävention und Betrugserkennung verantwortlich.
3. Beispielhafter Wert: a6cca60e-6a4c-4ca4-b9ca-94ce8191c6f8

4. _sessionID
    1. Ablaufzeit: Dauer der Session
    2. Verwendung: Dieses Cookie wird eingesetzt, um die Sitzung zu verfolgen. In diesem Cookie wird nur ein CSRF-Token gespeichert.
    3. Beispielhafter Wert: d9e87640-2250-11ea-927b-654e0890b70e

Die Erhebung von Daten erfolgt auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO zu Sicherheitszwecken und zur Verfügungstellung des Dienstes. Eine Interessenabwägung wurde durchgeführt. Unser berechtigtes Interesse ist die Gewährleistung der Sicherheit auf dem Webportal

6. Datenverarbeitung im Rahmen der Videosprechstunde

6.1 Zwecke und Rechtsgrundlage der Datenverarbeitung für individuelle Kunden

Individuelle Kunden sind diejenigen natürlichen oder juristischen Personen, die den allgemeinen Nutzungsbestimmungen der Bayerischen TelemedAllianz GmbH zugestimmt haben.

<u>E-Mail-Adresse:</u>

- Zweckbestimmung: Verifizierung der Anmeldung (Double Opt-in-Verfahren)
- Rechtsgrundlage: Art. 6 Abs. 1 b) DSGVO
- Ggf. berechtigtes Interesse: -
- Speicherdauer: Dauer des Vertragsverhältnisses, soweit eine darüber hinaus gehende Verarbeitung der personenbezogenen Daten nicht auf Grund gesetzlicher Pflichten, insbesondere des HGB und der AO, erforderlich ist.

<u>Vollständiger Name, Kontaktdaten, Adressdaten:</u>

- Zweckbestimmung: Identifikation, Kontakt, Verifizierung der Daten, Möglichkeit zur Nachvollziehung erfolgter Registrierungen
- Rechtsgrundlage: Art. 6 Abs. 1 b) DSGVO
- Ggf. berechtigtes Interesse: -
- Speicherdauer: Dauer des Vertragsverhältnisses, soweit eine darüber hinaus gehende Verarbeitung der personenbezogenen Daten nicht auf Grund gesetzlicher Pflichten, insbesondere des HGB und der AO, erforderlich ist.

<u>Vertragsdaten zwischen BTA und individueller Kunde:</u>

- Zweckbestimmung: Vertragsabwicklung, Dokumentation im Rahmen des Vertragsverhältnisses
- Rechtsgrundlage: Art. 6 Abs. 1 b) DSGVO
- Ggf. berechtigtes Interesse: -
- Speicherdauer: Dauer des Vertragsverhältnisses, soweit eine darüber hinaus gehende Verarbeitung der personenbezogenen Daten nicht auf Grund gesetzlicher Pflichten, insbesondere des HGB und der AO, erforderlich ist.

<u>Termindaten von individuellen Kunden:</u>

- Zweckbestimmung: Erbringung des Service von Doccura, Erbringung unserer Services, Dokumentation im Rahmen des Vertragsverhältnisses, vorgeschriebene Dokumentation durch Behandler, Vertragserfüllung
- Rechtsgrundlage: Art. 6, Abs. 2 lit. b DSGVO
- Ggf. berechtigtes Interesse: -
- Speicherdauer: Hier löschen wir Ihre personenbezogenen Daten drei Monate nach Durchführung des Termins. Eine darüber hinaus gehende Speicherung Ihrer personenbezogenen Daten erfolgt ausschließlich, falls diese auf Grund gesetzlicher Pflichten, insbesondere des HGB und der AO, erforderlich ist.

Anmeldedaten, Zugriffsdaten und Nutzungsdaten zu den einzelnen Features des Login-Bereichs:

- Zweckbestimmung: Verbindungsaufbau, Darstellung der Inhalte der Dienstleistung, Entdeckung von Angriffen auf unsere Seite anhand ungewöhnlicher Aktivitäten, Fehlerdiagnose, Erbringung unserer Services
- Rechtsgrundlage: Art. 6 Abs. 1 b), f) DSGVO
- Ggf. berechtigtes Interesse: Ordnungsgemäße Funktion der Services, Sicherheit von Daten und Geschäftsprozessen, Verhinderung von Missbrauch, Verhütung von Schäden durch Eingriffe in Informationssysteme, Verbesserung unserer Services
- Speicherdauer: Dauer der eingeloggten Session

6.2 Zwecke und Rechtsgrundlage der Datenverarbeitung für Organisationen

Vertreter seiner Organisation sind diejenigen natürlichen oder juristischen Personen, die für eine Organisation arbeiten und im Rahmen eines Organisationskontos Mitarbeiter aus der Organisation vertreten. Der Vertreter der Organisation verwaltet die untergeordneten Konten von den Mitarbeitern derselben Organisation, handelt im

Rahmen ihrer Geschäftstätigkeit und hat den allgemeinen Nutzungsbedingen der Bayerischen TelemedAllianz GmbH zugestimmt.

E-Mail-Adresse:

- Zweckbestimmung: Verifizierung der Anmeldung (Double Opt-in-Verfahren)
- Rechtsgrundlage: Art. 6 Abs. 1 litb. b DSGVO
- Ggf. berechtigtes Interesse: -
- Speicherdauer: Dauer des Vertragsverhältnisses, soweit eine darüber hinaus gehende Verarbeitung der personenbezogenen Daten nicht auf Grund gesetzlicher Pflichten, insbesondere des HGB und der AO, erforderlich ist.

Vollständiger Name, Organisationsname, Kontaktdaten der Organisation, Adressdaten der Organisation:

- Zweckbestimmung: Identifikation, Kontakt, Verifizierung der Daten, Möglichkeit zur Nachvollziehung erfolgter Registrierungen
- Rechtsgrundlage: Art. 6 Abs. 1 b) DSGVO
- Ggf. berechtigtes Interesse: -
- Speicherdauer: Dauer des Vertragsverhältnisses, soweit eine darüber hinaus gehende Verarbeitung der personenbezogenen Daten nicht auf Grund gesetzlicher Pflichten, insbesondere des HGB und der AO, erforderlich ist.

Vertragsdaten zwischen BTA und Organisation:

- Zweckbestimmung: Vertragsabwicklung, Dokumentation im Rahmen des Vertragsverhältnisses
- Rechtsgrundlage: Art. 6 Abs. 1 b) DSGVO
- Ggf. berechtigtes Interesse: -
- Speicherdauer: Dauer des Vertragsverhältnisses, soweit eine darüber hinaus gehende Verarbeitung der personenbezogenen Daten nicht auf Grund gesetzlicher Pflichten, insbesondere des HGB und der AO, erforderlich ist.

Termindaten von Organisationen:

- Zweckbestimmung: Erbringung des Services von Doccura
- Rechtsgrundlage: Art. 6, Abs. 2 lit. a DSGVO
- Ggf. berechtigtes Interesse: -
- Speicherdauer: Hier löschen wir Ihre personenbezogenen Daten drei Monate nach Durchführung des Termins. Eine darüber hinaus gehende Speicherung Ihrer personenbezogenen Daten erfolgt ausschließlich, falls diese auf Grund gesetzlicher Pflichten, insbesondere des HGB und der AO, erforderlich ist.

Anmeldedaten, Zugriffsdaten und Nutzungsdaten zu den einzelnen Features des Login-Bereichs:

- Zweckbestimmung: Verbindungsaufbau, Darstellung der Inhalte der Dienstleistung, Entdeckung von Angriffen auf unsere Seite anhand ungewöhnlicher Aktivitäten, Fehlerdiagnose, Erbringung unserer Services

- Rechtsgrundlage: Art. 6 Abs. 1 b), f) DSGVO
- Ggf. berechtigtes Interesse: Ordnungsgemäße Funktion der Services, Sicherheit von Daten und Geschäftsprozessen, Verhinderung von Missbrauch, Verhütung von Schäden durch Eingriffe in Informationssysteme, Verbesserung unserer Services
- Speicherdauer: Dauer der eingeloggten Session

6.3 Zwecke und Rechtsgrundlage der Datenverarbeitung für Nutzer

Ein Nutzer ist eine natürliche oder juristische Person, die im Namen des individuellen Kunden oder der Organisation handelnd die Software verwendet oder im Rahmen der vom Kunden angenommenen allgemeinen Nutzungsbedingungen der Bayerischen TelemedAllianz GmbH zugestimmt hat.

Name, E-Mail-Adresse und/oder Telefonnummer:

- Zweckbestimmung: Identifizierung, Kontaktaufnahme zur Versendung einer Einladung zu einer Chat-/Videosession
- Rechtsgrundlage: Art. 6 Abs. 1 a), b) DSGVO
- Ggf. berechtigtes Interesse:
- Speicherdauer: Dauer der Chat-/Videosession, bzw. Dauer des Vertragsverhältnisses mit Kunden (bei Auswahl zur Hinzufügung in die Kontaktliste des Kunden)

Anmeldedaten, Zugriffsdaten und Nutzungsdaten zu den einzelnen Features des Login-Bereichs:

- Zweckbestimmung: Verbindungsaufbau, Darstellung der Inhalte des Services, Entdeckung von Angriffen auf unsere Seite anhand ungewöhnlicher Aktivitäten, Fehlerdiagnose, Erbringung unserer Services
- Rechtsgrundlage: Art. 6 Abs. 1 b), f) DSGVO
- Ggf. berechtigtes Interesse: Ordnungsgemäße Funktion der Services, Sicherheit von Daten und Geschäftsprozessen, Verhinderung von Missbrauch, Verhütung von Schäden durch Eingriffe in Informationssysteme, Verbesserung unserer Services
- Speicherdauer: Dauer der eingeloggten Session

6.4 Datenverarbeitung bei Login und in der Doccura-Software

1. Für den Login-Prozess verschlüsselt die Doccura-Software das Passwort und die Benutzereingabe mithilfe der kryptologischen Hashfunktion bcrypt und vergleicht die eingegebenen Daten mit den Daten in der Datenbank. bcrypt verwendet einen modifizierten Schlüssel-Setup-Algorithmus, der recht zeitaufwendig ist. Dies wird als Schlüsselverstärkung bezeichnet und macht ein Kennwort sicherer vor Brute-Force-Angriffen. Dieser komplette Prozess erfolgt über https und ssl-security.
2. Innerhalb des Login-Bereiches von Doccura gibt es folgende Funktionen: Chat mit Datenaustausch, Audio- oder Videoanrufe und Gruppenkonferenzen.
    a) Im Rahmen der Chatfunktion mit Datenaustausch speichert Doccura keine Chats oder Dokumente. Jegliche Eingabe von Text und Dokumenten werden lokal im Browser der Kunden und Nutzer gespeichert. Die Kunden und Nutzer haben am Ende einer Chat-/Videosession die Möglichkeit den Chatverlauf als PDF zu exportieren oder per E-Mail zu versenden. Beim Ausloggen oder aktualisieren der Seite geht auch der Chatverlauf verloren.
    b) Der Audio- oder Videoanruf entsteht über eine Peer-to-Peer-Verbindung und ist somit Ende-zu-Ende-verschlüsselt. Ein Peer-to-Peer-Netzwerk (P2P) wird erstellt, wenn zwei oder mehr Endgeräte verbunden sind und Ressourcen gemeinsam nutzen, ohne einen separaten Server-Computer zu verwenden. Somit werden keine Daten auf den Doccura-Servern gespeichert.
    c) Im Rahmen einer Gruppenkonferenz können alle Beteiligten in einem Chatroom Texte und Dokumente austauschen, sowie Gruppen-Audio- und Videocalls machen. Gruppen-Audio- und Videocalls basieren ebenfalls auf einer Peer-to-Peer-Verbindung und sind auf 20 Teilnehmer limitiert.
3. Zu Dokumentationszwecken und zur Einsicht der Aktivitäten werden individuellen Kunden und Organisationen die Aktivitäten des jeweiligen Kontos angezeigt, beispielsweise die Dokumentation von einem Videocall mit einem Nutzer zu einem bestimmten Zeitpunkt für eine bestimmte Dauer.
4. In Doccura beziehen sich die Metadaten nur auf die Logs. Es gibt eine zeitlich festgelegte Aufgabe auf dem Server. Die Aufgabe löscht die entsprechenden Protokolle alle drei Monate. Dritte können nicht auf unsere Server zugreifen.

6.5 Sichtbarkeit Ihres Profils für registrierte Kunden und eingeladene Nutzer

Doccura unterscheidet zwischen Konten für individuellen Kunden (1), Organisationen (2) und eingeladene Nutzer (3).

1. Ein individueller Kunde ist ein Kunde, der für sich selbst ein Konto bei Doccura anlegt. Bei der Registrierung werden folgende Daten zur Identifikation und Verifizierung abgefragt: Vor- und Nachname, Geburtsdatum, E-Mail-Adresse, Postadresse (Straße, Hausnummer, Postleitzahl, Stadt, Land) und Telefonnummer. Ein individueller Kunde kann nicht-registrierte Nutzer einladen, um mit diesen über Doccura zu kommunizieren. Diese nicht-registrierten Nutzer können aus Gründen der Bequemlichkeit in die Kontaktliste der individuellen Kunden hinzugefügt werden.
2. Ein Vertreter seiner Organisation ist ein Kunde, der im Namen seiner Organisation ein Konto für sich und optional für eine unbegrenzte Anzahl an Mitarbeitern / Kollegen derselben Organisation anlegt. Bei der Registrierung werden folgende Daten zur Identifikation und Verifizierung abgefragt: Vor- und Nachname, Geburtsdatum, Organisations-E-Mail-Adresse, Organisationsname, Organisations-Postadresse (Straße, Hausnummer, Postleitzahl, Stadt, Land) und Organisations-Telefonnummer. Jede angemeldete Organisation findet in seiner Kontaktliste seine Mitarbeiter / Kollegen derselben Organisation und kann mit diesen kommunizieren. Eine Organisation kann nicht-registrierte Nutzer einladen, um mit diesen über Doccura zu kommunizieren. Diese nicht-registrierten Nutzer können aus Gründen der Bequemlichkeit in die Kontaktliste der individuellen Kunden hinzugefügt werden.
3. Ein eingeladener Nutzer kann im Rahmen eines von einem individuellen Kunden oder einer Organisation registrierten Kontos über verschiedene Kontaktmöglichkeiten (beispielsweise SMS oder E-Mail) eingeladen werden und in einem von dem Kunden angegebenen Zeitraum (beispielsweise 1 Stunde) mit dem Kunden eine Chat-/Videosession durchführen. Dabei muss der eingeladene Nutzer auf den ihm zugeschickten Link in einem Internet-Browser oder in der Doccura-App öffnen.

Jeder Kunde und jeder Nutzer kann im Rahmen einer Chat-/Videosession den Namen von allen beteiligten in der Chat-/Videosession sehen. Alle anderen personenbezogenen Daten können nicht eingesehen werden.

6.6 Freiwillige Daten

Die Erhebung und Verarbeitung freiwilliger Daten stehen unter Vorbehalt einer Einwilligung. Für die Durchführung der Videosprechstunde und den Besuch der Webseite werden keine freiwilligen Daten benötigt bzw. erhoben und verarbeitet..

7. Datenverarbeitung für Mitarbeiter der Bayerischen TelemedAllianz GmbH

Mitarbeiter:

- Zweckbestimmung: Durchführung von Beschäftigungsverhältnissen
- Betroffenen Daten: Anschreiben, Lebenslauf, Zeugnisse, Empfehlungsschreiben und andere übermittelte Bewerbungsunterlagen, Personenstammdaten, Adressdaten, Kontaktdaten, Arbeitsvertrag
- Rechtsgrundlage: Art. 6 Abs. 1 b) DSGVO
- Ggf. berechtigtes Interesse: -
- Speicherdauer: 10 Jahre nach Beendigung des Beschäftigungsverhältnisses

8. Empfänger

8.1 Empfänger der personenbezogenen Daten von individuellen Kunden und Organisationen

Zahlungsdienstleister:

- Betroffene Daten: Personenstammdaten, Kontaktdaten, Adressdaten, Vertragsdaten, Zahlungsdaten, Identitätsnachweis
- Rechtsgrundlage: Art. 6 Abs. 1 b) DSGVO
- Ggf. berechtigtes Interesse: -

Dienstleister für Buchhaltung:

- Betroffene Daten: Personenstammdaten, Adressdaten, Kontaktdaten, Zahlungsdaten, Vertragsdaten
- Rechtsgrundlage: Auftragsverarbeitung (Art. 28 DSGVO)
- Ggf. berechtigtes Interesse: -

8.2 Empfänger der personenbezogenen Daten von Nutzern

Individuelle Kunden oder Organisation:

- Betroffene Daten: Name, E-Mail-Adresse und/oder Telefonnummer
- Rechtsgrundlage: Art. 6 Abs. 1 a), b) DSGVO
- Ggf. berechtigtes Interesse: -

8.3 Empfänger der personenbezogenen Daten in dem Kontaktformular

Telefonprovider:

- Betroffene Daten: Telefonnummer, Verbindungsdaten
- Rechtsgrundlage: Auftragsverarbeitung (Art. 28 DSGVO)
- Ggf. berechtigtes Interesse: -

E-Mail-Provider:

- Betroffene Daten: E-Mail-Adresse, Anfragetext
- Rechtsgrundlage: Auftragsverarbeitung (Art. 28 DSGVO)
- Ggf. berechtigtes Interesse: -

Website-Provider:

- Betroffene Daten: E-Mail-Adresse, Anfragetext
- Rechtsgrundlage: Auftragsverarbeitung (Art. 28 DSGVO)
- Ggf. berechtigtes Interesse: -

8.4 Datenverarbeitung bei externen Dienstleistern

Unsere Website nutzt Funktionen des Videositzungsanbieters APIZEE. Anbieter ist Apizee, 11 rue Blaise Pascal, 22300 Lannion, Frankreich. Jedes Mal, wenn eine unserer Seiten APIRTC-Funktionen abruft, wird eine Verbindung zu APIZEE-Servern hergestellt. Eine Speicherung personenbezogener Daten erfolgt nicht. Insbesondere werden keine IP-Adressen gespeichert oder das Nutzungsverhalten ausgewertet. Weitere Informationen zum Datenschutz finden Sie in der APIZEE-Datenschutzrichtlinie unter https://www.apizee.com/privacy.
Wir bieten Ihnen die Möglichkeit zur Einladung zu einer Videosprechstunde per SMS. Dazu setzen wir Sendinblue ein. Bei Sendinblue handelt es sich um einen Dienst der Firma Sendinblue GmbH, Köpenicker Str. 126, 10179 Berlin, nachfolgend „Sendinblue“ genannt. Rechtsgrundlage für den SMS-Versand ist Art. 6 Abs. 1 lit. a.) DSGVO.
Unsere Website wird gehostet bei unserem Auftragsverarbeiter IONOS SE, Elgendorfer Str. 57, 56410 Montabaur, Deutschland. Über diesen Anbieter erfolgt auch die Versendung und Empfang von E-Mails. Zum Zweck der Bereitstellung und der Auslieferung der Website werden Verbindungsdaten verarbeitet. Zum bloßen Zweck der Auslieferung und Bereitstellung der Website werden die Daten über den Aufruf hinaus nicht gespeichert. Die Rechtsgrundlage für die Datenverarbeitung ist das berechtigte Interesse (unbedingte technische Notwendigkeit zur Bereitstellung und Auslieferung des von ihnen durch ihren Aufruf ausdrücklich gewünschten Dienstes „Website“) gemäß Art. 6 Abs. 1 lit. f DSGVO. Für diesen Service wurde ein Auftragsverarbeitungsvertrag (AVV) geschlossen. Weitere Informationen zum Datenschutz finden Sie in der IONOS-Datenschutzrichtlinie unter https://www.ionos.de/terms-gtc/terms-privacy.
Für die technische Infrastruktur zum Betrieb von Doccura nutzen wir Server der Telekom Deutschland GmbH. Für diese Services wurde ein Auftragsverarbeitungsvertrag (AVV) geschlossen. Weitere Informationen zum Datenschutz finden Sie in der Datenschutzrichtlinie der Telekom Deutschland GmbH unter https://open-telekom-cloud.com/de/datenschutz
Unsere Datenverarbeitung erfolgt unter Einschaltung sog. Hostingdienstleister, die uns Speicherplatz und Verarbeitungskapazitäten in ihren Rechenzentren zur Verfügung stellen und nach unserer Weisung auch personenbezogene Daten in unserem Auftrag verarbeiten. Alle personenbezogenen Daten der Software Doccura sind in einer verschlüsselten virtuellen Maschine gespeichert. Somit haben unsere Hostingdienstleister keinen Zugriff auf personenbezogene Daten der bei Doccura registrierten Kunden. Die Dienstleister verarbeiten Daten entweder ausschließlich in der EU auf Basis individuell vereinbarter Auftragsverarbeitungsverträge gem. Art. 28 DSGVO, wobei insbesondere sichergestellt ist, dass die Datenverarbeitung ausschließlich auf Grundlage unserer Weisungen erfolgt.

Nachfolgend beschreiben wir, wie Ihre personenbezogenen Daten verarbeitet werden, wenn sie sich an unseren Kundenservice wenden (z.B. über ein Online-Kontaktformular oder via Telefon). Im Rahmen der Bearbeitung Ihrer Kundenanfrage ist die Verarbeitung Ihrer personenbezogenen Daten zwingend erforderlich. Durch die Bearbeitung Ihrer personenbezogenen Daten möchten wir Ihre Anfrage bearbeiten und zur Verbesserung unserer Services beitragen. Soweit es im Zusammenhang mit der Bearbeitung Ihrer Anfrage zu einem ergänzenden Vertragsabschluss kommt, dient die Bearbeitung Ihrer Anfrage zugleich auch der Vertragsanbahnung respektive Vertragserfüllung. Dies betrifft Personenstammdaten, Kontaktdaten, Inhalte der Anfragen/Beschwerden, Zugriffsdaten. Gesetzliche Grundlagen sind: Art. 6 Abs. 1 Satz 1 lit. a DSGVO Art. 6 Abs. 1 Satz 1 lit. b DSGVO Art. 6 Abs. 1 Satz 1 lit. f DSGVO. Eine Löschung erfolgt 1 Jahr nach abgeschlossener Bearbeitung der Anfrage, soweit eine darüber hinaus gehende Verarbeitung der personenbezogenen Daten nicht auf Grund gesetzlicher Pflichten, insbesondere des HGB und der AO, erforderlich ist.

Technischen Support erhalten Sie, indem Sie eine Anfrage an das eMail-Postfach info@doccura.de senden.

8.5 Übermittlung personenbezogener Daten an Drittländer

Er erfolgt keine Übermittlung von Daten in Drittstaaten durch die Bayerische TelemedAllianz GmbH. Für den Fall, dass personenbezogenen Daten auf Grund gesetzlicher Anforderung an Drittländer übermittelt werden müssten, findet diese Übermittlung ausschließlich unter Einhaltung der gesetzlichen Zulässigkeitsvoraussetzungen statt. Das bedeutet insbesondere, dass Ihre personenbezogenen Daten ausschließlich unter Einbeziehung der Voraussetzungen der Art. 44 ff. DSGVO in ein Drittland übermittelt würden.
Des Weiteren sind zum Schutz personenbezogener Daten im Zusammenhang mit dem Drittländerbezug (Art. 44 ff DSGVO) bei uns sowie bei unseren Dienstleistern entsprechende technische und organisatorische Sicherheitsmaßnahmen umgesetzt, durch die insbesondere durch geeignete Verschlüsselungsverfahren nach aktuellstem Stand der Technik auch bei etwaiger Übermittlung keine Dateneinsicht genommen werden kann.

8.6 Bezahlmöglichkeiten individueller Kunden und Organisationen

Die in unserem Angebot mögliche Bezahlungsmethode ist Stripe. Stripe wird von Stripe Payment Europe Ltd. 1 Grand Canal Street Lower Dublin 2 Ireland als verantwortliche Stelle abgewickelt. Ausführungen zum Datenschutz von Stripe finden Sie unter https://stripe.com/de/privacy

8.7 Übermittlung an staatliche Behörden

Wir übermitteln Ihre personenbezogenen Daten an staatliche Behörden (einschließlich Strafverfolgungsbehörden), wenn dies zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der wir unterliegen (Art. 6 Abs. 1 Satz 1 lit. c DSGVO). Darüber hinaus verarbeiten wir Ihre personenbezogenen Daten auch, wenn die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist. Die Verarbeitung Ihrer personenbezogenen Daten erfolgt in diesem Fall auf Basis unserer überwiegenden berechtigten Interessen an der Rechtsdurchsetzung im Sinne des Art. 6 Abs. 1 Satz 1 lit. f DSGVO.

9. Betroffenenrechte

9.1 Auskunftsrecht

Auskunftsrecht gemäß Art. 15 DSGVO: Sie haben jederzeit das Recht auf unentgeltliche Auskunft über Ihre bei uns gespeicherten personenbezogenen Daten, deren Herkunft und Empfänger und den Zweck der Datenverarbeitung. Wenn Sie Fragen hierzu haben, die Ihnen diese Datenschutzhinweise nicht beantworten konnte, können Sie sich jederzeit unter folgender E-Mail-Adresse oder über die im Impressum angegebenen Kontaktdaten an uns wenden: info@doccura.de.

9.2 Widerspruchsrecht

Recht auf Widerruf erteilter Einwilligungen gemäß Art. 6 Abs. 3 DSGVO:
Sie haben das Recht, eine einmal erteilte Einwilligung in die Verarbeitung von Daten jederzeit ohne die Nennung von Gründen mit Wirkung für die Zukunft ganz oder zu Teilen zu widerrufen. Im Falle des Widerrufs werden wir die betroffenen Daten unverzüglich löschen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit, der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung, nicht berührt.

9.3 Rechte

1. Wir verwenden die von Ihnen mitgeteilten Daten ausschließlich zur Erfüllung und Abwicklung der von uns bereit gestellten Dienstleistungen, soweit nicht eine weitergehende Verwendung durch das Gesetz zugelassen wird oder Sie gesondert einwilligen.
2. Recht auf Löschung gemäß Art. 17 DSGVO: Sie haben das Recht, die Löschung Ihrer personenbezogenen Daten bei Vorliegen der Voraussetzungen des Art. 17 Abs. 1 DSGVO zu verlangen. Dieses Recht besteht jedoch insbesondere dann nicht, wenn die Verarbeitung zur Ausübung des Rechts auf freie Meinungsäußerung und Information, zur Erfüllung einer rechtlichen Verpflichtung, aus Gründen des öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.
3. Recht auf Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. a bis d DSGVO: Sie haben das Recht, die Einschränkung der Verarbeitung Ihrer personenbezogenen Daten zu verlangen, solange die von Ihnen bestrittene Richtigkeit Ihrer Daten überprüft wird, wenn Sie eine Löschung Ihrer Daten wegen unzulässiger Datenverarbeitung ablehnen und stattdessen die Einschränkung der Verarbeitung Ihrer Daten verlangen, wenn Sie Ihre Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigen, nachdem wir diese Daten nach Zweckerreichung nicht mehr benötigen oder wenn Sie Widerspruch aus Gründen Ihrer besonderen Situation eingelegt haben, solange noch nicht feststeht, ob unsere berechtigten Gründe überwiegen.
4. Recht auf Berichtigung gemäß Art. 16 DSGVO: Sie haben das Recht, umgehend die Berichtigung der betreffenden unrichtigen personenbezogenen Daten zu fordern. Sie haben unter Berücksichtigung der Zwecke der Verarbeitung das Recht, die Vervollständigung unvollständiger personenbezogener Daten zu fordern.
5. Recht auf Datenübertragbarkeit gemäß Art. 20 DSGVO: Sie haben das Recht, Ihre personenbezogenen Daten, die Sie uns bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesebaren Format zu erhalten oder die Übermittlung an einen anderen Verantwortlichen zu verlangen, soweit dies technisch machbar ist.
6. Recht auf Unterrichtung gemäß Art. 19 DSGVO: Haben Sie das Recht auf Berichtigung, Löschung oder Einschränkung der Verarbeitung gegenüber dem Verantwortlichen geltend gemacht, ist dieser verpflichtet, allen Empfängern, denen die Sie betreffenden personenbezogenen Daten offengelegt wurden, diese Berichtigung oder Löschung der Daten oder Einschränkung der Verarbeitung mitzuteilen, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Ihnen steht das Recht zu, über diese Empfänger unterrichtet zu werden.
7. Zudem haben Sie das Recht der Datenverarbeitung zu widersprechen, sofern die Voraussetzungen des Art. 21 DSGVO gegeben sind.

9.4 Beschwerderecht

Ihnen steht, unbeschadet anderer Rechtsbehelfe, jederzeit das Recht zu, sich bei einer Aufsichtsbehörde aufgrund einer Verletzung der Datenschutzgrundverordnung zu beschweren (Art. 77 DSGVO): Bayerisches Landesamt für Datenschutzaufsicht, Promenade 18, 91522 Ansbach, https://www.lda.bayern.de Telefon: +49 (0) 981 180093-0 Telefax: +49 (0) 981 180093-800 E-Mail: poststelle@lda.bayern.de

10. Datensicherheit

1. Wir haben technische und organisatorische Maßnahmen zur Gewährleistung der Datensicherheit getroffen. Diese Maßnahmen dienen unter anderem der Vermeidung eines unerlaubten Zugriffs auf die von uns genutzten technischen Einrichtungen und dem Schutz Ihrer personenbezogenen Daten vor unerlaubter Kenntnisnahme durch Dritte. Die technischen und organisatorischen Maßnahmen werden beständig weiterentwickelt und dem aktuellen Stand der Technik entsprechend jeweils angepasst.
2. Um unberechtigte Zugriffe Dritter auf Ihre persönlichen Daten zu verhindern, wird die Kommunikation mit unserer Website verschlüsselt.

11. Datenpannen

Gemäß Art. 33 DSGVO ist eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden bei der zuständigen Aufsichtsbehörde zu melden. Die Aufsichtsbehörden haben hierfür größtenteils online umfangreiche Eingabemasken eingerichtet die wir benutzen werden. Von einer Meldung kann nur dann abzusehen sein, wenn die Verletzung „voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen“ führt und setzt demnach die Beschäftigung mit einer dahingehenden Prognoseentscheidung des Verantwortlichen voraus. Zur Abschätzung des Risikos hat die Datenschutzkonferenz (Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – DSK) in ihrem Kurzpapier Nr. 18 eine Hilfestellung veröffentlicht das im Internet einsehbar ist und das wir anwenden. Stellt sich bei der Risikobewertung heraus, dass voraussichtlich ein hohes Risiko für die

persönlichen Rechte und Freiheiten natürlicher Personen besteht, so sind gemäß Art. 34 DSGVO auch die betroffenen Personen deren Daten Gegenstand des Notfalls waren zu benachrichtigen. Der Umgang mit einer Datenpanne endet nicht mit der Meldung bei der Aufsichtsbehörde und ggfs. der Wiederherstellung des Normalbetriebs. Bei der Meldung werden wir angeben, welche Maßnahmen zur Eindämmung des Risikos akut unternommen wurden. Teil der Dokumentation des Datenschutznotfalls ist daher auch die Aufarbeitung und das Implementieren von Maßnahmen, die einen weiteren Datenschutznotfall dieser Art verhindern können. Auch wenn die durchgeführte Risikobewertung nicht in einer Meldung des Vorfalls an die zuständige Aufsichtsbehörde endet, werden wir den erkannten Vorfall nach Art. 33 Abs. 5 DSGVO entsprechend dokumentieren. Dies dient der Information der Aufsichtsbehörde im Falle einer Prüfung, was Grundlage dieser Entscheidung war. Ein zentraler Punkt ist bei Doccura bei Datenpannen die rechtzeitige Einbindung des Datenschutzbeauftragten. Dieser kann aus neutraler Sicht entscheidende Hilfestellungen zur Risikobewertung geben und letztlich in der Funktion als weißungsunabhängige Kontrollinstanz zur richtigen Handhabe des Vorfalls durch Doccura einen wichtigen Beitrag leisten.

12. Datenschutzhinweise für Leistungserbringer (Ärzte)

Der Vertragsarzt hat für die Verarbeitung personenbezogener Patientendaten die rechtlichen Rahmenbedingungen zu beachten, die sich insbesondere aus den Vorschriften der Datenschutzgrundverordnung (DSGVO), des Bundesdatenschutzgesetzes (BDSG) sowie des Fünften Sozialgesetzbuchs (SGB V) und – soweit anwendbar – des Zehnten Sozialgesetzbuchs (SGB X) ergeben. Bei der konkreten Umsetzung kann sich der Vertragsarzt an den „Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung orientieren. Im Hinblick auf die Sicherheit der Verarbeitung der Daten hat der Vertragsarzt in seinen Räumlichkeiten und IT-Systemen zu gewährleisten, dass die erforderlichen technischen und organisatorischen Maßnahmen eingehalten werden. Die Videosprechstunde hat zur Gewährleistung der Datensicherheit und eines störungsfreien Ablaufes in geschlossenen Räumen, die eine angemessene Privatsphäre sicherstellen, stattzufinden. Zu Beginn der Videosprechstunde hat auf beiden Seiten eine Vorstellung aller im Raum anwesenden Personen zu erfolgen. Aufzeichnungen jeglicher Art sind während der Videosprechstunde nicht gestattet. Die Videosprechstunde darf nur von einem Vertragsarzt durchgeführt werden. Der Vertragsarzt darf für die Videosprechstunde ausschließlich gemäß § 5 zertifizierte Videodienstanbieter nutzen.

Die zunehmende elektronische Kommunikation und Vernetzung der Ärzte bietet Chancen, birgt aber auch Gefahren hinsichtlich der Datensicherheit. Als Arzt bzw. Psychotherapeut sind Sie deshalb beim beruflichen Einsatz von EDV verpflichtet, die Sicherheit der Patientendaten zu gewährleisten. Zusätzlich zu den Regelungen der ärztlichen Schweigepflicht gelten für Sie auch die Datenschutzgesetze, allen voran die Bestimmungen der Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG-neu). Diese regeln die verschiedenen Phasen der Datenverarbeitung und die Anforderungen an die Datensicherheit. Vor diesem Hintergrund haben die Bundesärztekammer und die Kassenärztliche Bundesvereinigung schon im Jahre 2008 „Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ und eine zugehörige technische Anlage veröffentlicht die laufend aktualisiert werden. Darin enthalten sind rechtliche, technische und organisatorische Orientierungshilfen bei der Umsetzung von Datenschutz und Datensicherheit in der Praxis. Ein Schwerpunkt betrifft die ärztliche Dokumentation, die Datenkommunikation in der Praxis und die Online-Anbindung. Sehr viel detaillierter als die Empfehlungen geht die Technische Anlage auf erforderliche IT-Schutzmaßnahmen ein. Das inhaltliche Spektrum reicht vom Umgang mit Passwörtern über die Nutzung des Internets und Intranets, das Einrichtungen von lokalen und drahtlosen Netzwerken bis hin zur Entsorgung von Datenträgern und Archivierung. Teilweise existieren Überschneidungen mit dem Thema der Informationssicherheit. Einige wichtige Punkte haben wir nachfolgend zusammengestellt: Erstellen Sie Regeln für die Verwendung von effektiven und individuellen Passwörtern durch ihre Mitarbeiter. Dazu zählen auch Schreibweisen (zum Beispiel mindestens 6 Buchstaben und 1 Zeichen) und eine begrenzte Gültigkeit. Die Option „Speicherung von Passwörtern“ sollte im Betriebssystem deaktiviert werden. Viren-Schutz: Die meisten IT-Sicherheitsvorfälle ereignen sich im Zusammenhang mit Computerviren. Daher sind aktuelle Viren-Schutzprogrammeunverzichtbar. Schadprogramme können über Datenträger oder über Netze (Internet, Intranet) verbreitet werden. Auch für Rechner ohne Internetanschluss sind Schutzprogramme erforderlich. Es empfiehlt sich, E-Mails und jegliche Kommunikation über das Internet zentral auf Viren zu untersuchen. Zusätzlich sollte jeder Computer mit einem lokalen Viren-Schutzprogramm ausgestattet sein, das ständig im Hintergrund läuft. In der Regel genügt es, nur ausführbare Dateien, Skripte, Makrodateien etc. zu überprüfen. Ein vollständiges Durchsuchen aller Dateien empfiehlt sich trotzdem in regelmäßigen Abständen, zum Beispiel vor einer Tages- oder Monatssicherung, und ist bei einem festgestellten Befall durch Schadprogramme immer notwendig. Aktuelle Empfehlungen und ausführliche Hintergrundinformationen finden Sie auf www.bsi.deunter dem Stichwort Schadprogramme. Sie sollten Strategien zur Datensicherung und Datenwiederherstellung erarbeiten, damit Sie im Notfall kurzfristig zumindest eine eingeschränkte Funktionsfähigkeit herstellen können. Vergeben Sie rollen-bzw. personenbezogenen Zugriffsrechte auf das EDV-System

und prüfen Sie deren Vergabe. Die Konfiguration der Datenzugriffsrechte sollte für jeden Benutzer auf das Notwendige beschränkt werden. Es sollten keine Administratorrechte für normale Benutzer vergeben werden. Informieren Sie die Mitarbeiter über die sichere Verwendung von Passwörtern (siehe oben) und machen Sie deutlich, dass diese konsequent einzuhalten ist. Nutzen Sie z.B. Chip-Karten, wenn Sie elektronische Patientendaten für den Transport verschlüsseln oder sich zum Beispiel gegenüber einem Web-Portal als Arzt authentisieren wollen. Informieren Sie Ihre Mitarbeiter über die nach der Berufsordnung geltende gesetzliche Schweigepflicht. Alle Praxismitarbeiter, aber auch externe Personen wie EDV-Berater, Support-Mitarbeiter und Reinigungspersonal, welche Zugang zu personenbezogenen Daten haben, müssen die Regelungen zum Datenschutz kennen und Datenschutzhinweise unterschreiben. Wenn Sie eine elektronische Patientenverwaltung per PVS führen, sind alle Mitarbeiter im Arbeitsvertrag oder durch eine separate Verpflichtungserklärung auch auf das Datengeheimnis nach § 5 BDSG zu verpflichten. Externe Dienstleister dürfen nur bei Bedarf Zugang zu diesen Daten erhalten. Weisen Sie nicht nur bei der Einstellung neuer Mitarbeiter auf die gesetzlichen Vorgaben hin, nutzen Sie dazu auch die regelmäßigen Teamsitzungen und Mitarbeitergespräche. Überprüfen Sie, ob sie, ob sie einen internen oder externen Datenschutzbeauftragten bestellen müssen. Weiterhin sind alle Verfahrensregeln einzuhalten, die von Seiten der Telematikinfrastruktur vorgegeben werden (www.gematik.de).

13. Schlussbestimmungen

Es gilt deutsches Recht, Gerichtsstand ist soweit zulässig Ingolstadt. Sollten einzelne Bestimmungen dieser allgemeinen Geschäftsbedingungen einschließlich dieser Bestimmung ganz oder teilweise unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Regelungen unberührt. Anstelle der unwirksamen oder fehlenden Bestimmungen treten die jeweiligen gesetzlichen Regelungen.