

Auftragsverarbeitungsvertrag gem. Art. 28 DSGVO - medflex

zwischen

medflex GmbH
Reichenaustraße 39a
78467 Konstanz
Deutschland

- im Folgenden: „medflex“ -

und

Firma

Str

PLZ Ort

Deutschland

- im Folgenden: „Kunde“ -

§ 1 Definitionen und zuständige Aufsichtsbehörden

- (1) Es gelten die Begriffsbestimmungen der DSGVO (Art. 4 DSGVO). Verantwortlicher ist der Kunde, Auftragsverarbeiter ist medflex.
- (2) Zuständige Aufsichtsbehörde für medflex ist der Landesbeauftragte für den Datenschutz in Baden-Württemberg.
- (3) Die Zuständigkeit der jeweiligen Aufsichtsbehörden für die Vertragsparteien richtet sich nach den gesetzlichen Vorgaben.
- (4) medflex und der Kunde arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

§ 2 Vertragsgegenstand

- (1) medflex erbringt für den Kunden IT-Dienstleistungen gemäß den in Anlage 1 beschriebenen Zwecken und Leistungen. Im Rahmen dieser Tätigkeit verarbeitet medflex personenbezogene Daten ausschließlich im Auftrag und gemäß den Weisungen des Kunden. Dabei gelten ergänzend die AGB von medflex.
- (2) Die Bestimmungen dieses Vertrages gelten für alle Tätigkeiten, bei denen medflex personenbezogene Daten im Auftrag des Kunden verarbeitet oder auf solche Daten Zugriff erhält.
- (3) Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Hauptvertrags zwischen den Parteien, sofern ein solcher besteht. Unabhängig davon bleibt dieser AVV gültig, solange medflex personenbezogene Daten im Auftrag des Kunden verarbeitet oder über solche Daten verfügt, und endet erst mit Abschluss aller vereinbarten Lösch- und Rückgabepflichten.

§ 3 Datenverarbeitung

- (1) Art und Umfang der Datenverarbeitung ergeben sich aus Anlage 1.
- (2) medflex darf personenbezogene Daten nur zu folgenden Zwecken verarbeiten:
 - In Übereinstimmung mit diesem Vertrag und zum Zweck der Auftragsverarbeitung für den Kunden
 - Zur Ausführung von Aktionen, die von autorisierten Nutzern initiiert werden
 - Zur Befolgung angemessener Weisungen des Kunden (z.B. per E-Mail oder Support-Tickets)
- (3) medflex verwendet die Daten nicht für eigene Zwecke.
- (4) Die Verarbeitung personenbezogener Daten in einem Drittland ist nur zulässig, wenn:
 - Ein Angemessenheitsbeschluss der EU-Kommission gemäß Art. 45 DSGVO vorliegt, oder
 - Geeignete Garantien gemäß Art. 46 DSGVO vereinbart wurden (z.B. Standardvertragsklauseln)
- (5) Ist medflex der Ansicht, dass der Kunde gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Kunden unverzüglich darauf hinzuweisen. medflex ist berechtigt, die Durchführung einer Verarbeitung so lange auszusetzen, bis die erfolgreiche Veränderung durch den Kunden bestätigt oder geändert wird. medflex darf die Durchführung einer offensichtlich rechtswidrigen Nutzung ablehnen.
- (6) Für Videosprechstunden im Sinne der Anlage 31b zum BMV-Ä erfolgt die Verarbeitung ausschließlich in der EU/des EWR oder in Staaten mit gültigem Angemessenheitsbeschluss gemäß Art. 45 DSGVO.
- (7) medflex verpflichtet sich gem. Art. 28 Abs. 3 lit. a DSGVO, den Kunden unverzüglich zu informieren, sollten gesetzliche Bestimmungen medflex zu einer Verarbeitung personenbezogener Daten entgegen den Weisungen des Kunden verpflichten, es sei denn, das betreffende Recht verbietet eine solche Mitteilung aus wichtigen Gründen des öffentlichen Interesses.

§ 4 Pflichten von medflex

- (1) medflex verpflichtet sich zur Einhaltung aller datenschutzrechtlichen Bestimmungen und zum vertraulichen Umgang mit allen erhaltenen Informationen.
- (2) medflex implementiert und unterhält angemessene technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO, wie in Anlage 3 beschrieben, und passt diese regelmäßig an den Stand der Technik an.
- (3) medflex hat einen Datenschutzbeauftragten bestellt und verpflichtet alle mit der Verarbeitung personenbezogener Daten betrauten Mitarbeiter zur Vertraulichkeit gemäß Art. 28 Abs. 3 lit. b

DSGVO sowie zur Wahrung der gesetzlichen Verschwiegenheitspflichten, insbesondere nach § 203 StGB, § 3 TDDDG und § 206 StGB sowie § 35 SGB I, soweit diese jeweils anwendbar sind.

- (4) medflex informiert den Kunden unverzüglich, spätestens jedoch innerhalb von 48 Stunden, bei:
 - Schwerwiegenden Störungen oder Verdacht auf Datenschutzverletzungen
 - Verletzungen vertraglicher Verpflichtungen
 - Sicherheitsrelevanten Vorfällen
 - Prüfungen durch die Datenschutz-Aufsichtsbehörde
 - Gefährdung der Daten des Kunden durch Dritte
- (5) medflex trifft unverzüglich erforderliche Maßnahmen zur Sicherung der Daten und zur Schadensminimierung.
- (6) medflex stellt dem Kunden die zur Bewertung der Erforderlichkeit einer Datenschutz-Folgenabschätzung erforderlichen Informationen über die standardmäßige Funktionsweise des Dienstes, die verarbeiteten Datenkategorien und die technischen und organisatorischen Maßnahmen zur Verfügung. Die Bewertung der konkreten Einsatzbedingungen und die Entscheidung über die Durchführung oder Aktualisierung einer Datenschutz-Folgenabschätzung obliegen dem Kunden als Verantwortlichem.

medflex unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und der medflex zur Verfügung stehenden Informationen im nach Art. 28 Abs. 3 lit. f DSGVO erforderlichen Umfang bei der Erfüllung seiner Pflichten nach Art. 32 bis 36 DSGVO. medflex informiert den Kunden über wesentliche Änderungen der vereinbarten Verarbeitung, soweit diese die datenschutzrechtliche Risikobewertung des Kunden erkennbar beeinflussen können.
- (7) Anfragen von betroffenen Personen leitet medflex unverzüglich an den Kunden weiter und setzt dessen Weisungen zur Umsetzung von Betroffenenrechten um.

§ 5 Subunternehmer

- (1) Unterauftragsverarbeiter sind Dienstleister, die im Auftrag von medflex personenbezogene Kundendaten zur Erbringung der vereinbarten Leistungen verarbeiten. Die Einordnung richtet sich nach der tatsächlich ausgeübten Tätigkeit; insbesondere können auch Wartungs-, Support- und sonstige Nebenleistungen eine Unterauftragsverarbeitung darstellen. Reine Nebenleistungen ohne Verarbeitung personenbezogener Kundendaten im Auftrag von medflex fallen nicht unter diese Regelung. medflex gewährleistet auch bei solchen Nebenleistungen einen angemessenen Schutz der Daten.
- (2) Der Kunde erteilt medflex die allgemeine Genehmigung, Subunternehmer gemäß Art. 28 Abs. 2-4 DSGVO einzusetzen. Die aktuell eingesetzten Subunternehmer sind in Anlage 2 aufgeführt.
- (3) medflex informiert den Kunden mindestens 30 Tage vor dem vorgesehenen Einsatz eines neuen oder der Ersetzung eines bestehenden Unterauftragnehmers in Textform, insbesondere per E-Mail an den vom Kunden benannten Ansprechpartner. Ergänzend kann medflex die jeweils aktuelle Liste der Unterauftragnehmer auf seiner Website veröffentlichen.
- (4) Der Kunde kann innerhalb von 30 Tagen nach Zugang der Mitteilung aus sachlich gerechtfertigten datenschutzrechtlichen Gründen Einwände gegen den Einsatz eines neuen oder die Ersetzung eines bestehenden Unterauftragnehmers erheben. medflex wird den Einwand prüfen und sich bemühen, eine für beide Parteien zumutbare Lösung zu finden. Kann der Einwand nicht ausgeräumt werden und ist der Einsatz des betreffenden Unterauftragnehmers für die Erbringung einer Leistung erforderlich, ist der Kunde berechtigt, die hiervon betroffene Leistung zum Zeitpunkt des vorgesehenen Einsatzes des Unterauftragnehmers außerordentlich zu kündigen. Erfolgt innerhalb der genannten Frist kein Einwand, gilt die Änderung als genehmigt.
- (5) medflex dokumentiert alle eingesetzten Subunternehmer und deren Datenschutzmaßnahmen.
- (6) medflex setzt vorrangig Unterauftragsverarbeiter mit Verarbeitung in der EU bzw. im EWR ein. Mit Unterauftragsverarbeitern werden, soweit erforderlich, Vereinbarungen nach Art. 28 DSGVO geschlossen. Soweit im Einzelfall eine Drittlandübermittlung oder ein Drittlandzugriff erfolgt, gewährleistet medflex die Einhaltung der Anforderungen des Kapitels V DSGVO sowie gegebenenfalls anwendbarer sektorspezifischer Vorgaben. Über den vorgesehenen Einsatz oder Wechsel von Unterauftragsverarbeitern wird der Kunde nach Maßgabe der Absätze 3 und 4 informiert.

§ 6 Rechte des Kunden

- (1) Der Kunde hat das Recht, die Einhaltung der Datenschutzvorschriften und vertraglichen Vereinbarungen durch medflex zu überprüfen. medflex stellt auf Anfrage geeignete Nachweise bereit (z.B. Auditberichte, Zertifizierungen).
- (2) Vor-Ort-Kontrollen sind in begründeten Ausnahmefällen zulässig und grundsätzlich mit angemessener Frist, in der Regel 14 Kalendertage im Voraus, anzukündigen. Sie dürfen den Betriebsablauf nicht unangemessen stören. Abweichend hiervon sind Kontrollen auch ohne Vorankündigung zulässig, sofern konkrete Anhaltspunkte für einen erheblichen Verstoß gegen datenschutzrechtliche Pflichten oder die vertraglichen Vereinbarungen bestehen oder eine vorherige Ankündigung den Zweck der Kontrolle gefährden würde. medflex ist in diesem Fall unverzüglich bei Durchführung der Kontrolle zu unterrichten. Der Kunde hat bei der Durchführung der Kontrolle die Vertraulichkeitsinteressen von medflex sowie die Sicherheit anderer Kunden- und Systemumgebungen angemessen zu berücksichtigen.
- (3) medflex stellt dem Kunden die zur Erfüllung der gesetzlichen Nachweispflichten erforderlichen Informationen ohne gesonderte Berechnung zur Verfügung. Verlangt der Kunde darüber hinaus eine Vor-Ort-Kontrolle oder entsteht medflex durch eine vom Kunden veranlasste Prüfung ein außergewöhnlicher und nicht nur unerheblicher Aufwand, trägt der Kunde die hierdurch entstehenden angemessenen und vorab abgestimmten Kosten. Dies gilt nicht, soweit die Kontrolle aufgrund konkreter Anhaltspunkte für einen Datenschutzverstoß veranlasst war und ein solcher Verstoß festgestellt wird.
- (4) medflex ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Kunden gem. Art. 58 DSGVO die erforderlichen Auskünfte zu erteilen und Kontrollen der Behörde zu ermöglichen, sofern dies gesetzlich vorgeschrieben ist. medflex informiert den Kunden unverzüglich über geplante Maßnahmen, die ihn betreffen, und unterstützt ihn angemessen bei der Erfüllung seiner gesetzlichen Pflichten.

§ 7 Haftung

- (1) Die Haftung der Parteien gegenüber betroffenen Personen richtet sich nach den zwingenden gesetzlichen Vorschriften, insbesondere nach Art. 82 DSGVO.
- (2) Die nachfolgenden Regelungen betreffen ausschließlich das Innenverhältnis zwischen den Parteien und lassen Ansprüche betroffener Personen sowie Befugnisse von Aufsichtsbehörden unberührt.
- (3) Im Innenverhältnis haften die Parteien einander nach den gesetzlichen Vorschriften und entsprechend dem jeweiligen Verursachungs- und Verantwortungsbeitrag.
- (4) Zwingende gesetzliche Haftungsvorschriften bleiben unberührt.

§ 8 Beendigung des Vertrags

- (1) Der Kunde kann den Vertrag fristlos kündigen, wenn medflex seinen Pflichten nicht nachkommt, die DSGVO vorsätzlich oder grob fahrlässig verletzt oder Weisungen nicht ausführen kann oder will. Bei einfachen Verstößen ist eine angemessene Nachfrist zu setzen.
- (2) medflex ist verpflichtet, auch über das Ende des Vertragsverhältnisses hinaus alle im Rahmen der Auftragsverarbeitung bekannt gewordenen personenbezogenen Daten vertraulich zu behandeln. Der vorliegende Vertrag bleibt auch nach Beendigung des Hauptvertrags, sofern ein solcher besteht, ansonsten nach Beendigung dieses AVs, solange medflex noch über personenbezogene Daten verfügt, die ihm vom Kunden übermittelt wurden oder die er für diesen erhoben hat.
- (3) Nach Beendigung des Vertrags hat medflex alle verarbeiteten Daten gemäß Weisung des Kunden zurückzugeben oder zu löschen, sofern keine gesetzliche Aufbewahrungspflicht besteht. Die Löschung von Datenkopien in technisch notwendigen Sicherungen erfolgt nach den hierfür festgelegten Löszyklen; bis dahin werden diese Kopien gegen eine reguläre weitere Nutzung geschützt.
- (4) medflex ist berechtigt, Daten oder Unterlagen, die unter gesetzliche Aufbewahrungspflichten fallen, bis zum Ablauf der entsprechenden Frist aufzubewahren. In diesen Fällen erfolgt eine Löschung unverzüglich nach Ablauf der Aufbewahrungsfrist.

- (5) Erteilt der Kunde innerhalb von 30 Tagen nach Vertragsende keine Weisung, werden die Daten von medflex nach Ablauf dieser Frist datenschutzkonform gelöscht, sofern keine gesetzlichen Aufbewahrungspflichten dem entgegenstehen.

§ 9 Schlussbestimmungen

- (1) Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform.
- (2) Sollten einzelne Bestimmungen unwirksam sein, bleibt der Vertrag im Übrigen wirksam.
- (3) Es gilt deutsches Recht. Ausschließlicher Gerichtsstand ist Konstanz.



Unterschrift (medflex)
Felix Rademacher
Geschäftsführer medflex GmbH

Unterschrift (Kunde)

Datum

Name Ansprechpartner Kunde

E-Mail Ansprechpartner Kunde

Kontaktinformation medflex:

E-Mail: service@medflex.de
Tel.: +49 7531 363 9390

Senden Sie bitte Ihre unterzeichnete Kopie an:

daten.schutz@medflex.de

Anlagen:

- Anlage 1 - Beschreibung und Zweck der Daten/Datenkategorien
- Anlage 2 - Subunternehmer
- Anlage 3 - Technische und organisatorische Maßnahmen

Anlage 1 - Beschreibung und Zweck

Gegenstand der Verarbeitung

medflex stellt eine sichere Kommunikationslösung bereit, die speziell für den Gesundheitssektor entwickelt wurde. Die Verarbeitung umfasst:

- Bereitstellung einer sicheren Messenger-Plattform für die Kommunikation zwischen medizinischem Fachpersonal und Patienten
- Durchführung von Videosprechstunden gemäß den Anforderungen der KBV (Kassenärztliche Bundesvereinigung)
- Automatisierte Annahme und Transkription eingehender Anrufe durch den Telefonassistenten
- Verwaltung von Terminanfragen und sonstigen patientenbezogenen Anfragen
- Sichere Speicherung und Übermittlung von Dokumenten und Nachrichten
- Anbindung des beim Kunden eingesetzten Praxisverwaltungssystems x.isynet über die hierfür verfügbare bzw. zwischen den Parteien vereinbarte Schnittstelle, einschließlich des Abrufs, der Zuordnung, des Abgleichs und, soweit technisch vorgesehen, der Übermittlung patientenbezogener Daten zwischen x.isynet und medflex.

Die Verarbeitung erfolgt ausschließlich auf Weisung des Kunden und dient der Unterstützung seiner medizinischen Leistungserbringung. Die in dieser Anlage beschriebenen einzelnen Produktfunktionen und insbesondere die PVS-Anbindung mit x.isynet kommen nur zur Anwendung, soweit der Kunde die jeweilige Funktion tatsächlich nutzt bzw. mit medflex vereinbart hat.

Art der Verarbeitung

Die Verarbeitung durch medflex umfasst folgende Vorgänge:

- Erhebung und Speicherung von Nutzerdaten
- Übermittlung von Nachrichten und Dokumenten
- Durchführung und technische Absicherung von Videogesprächen
- Entgegennahme, gegebenenfalls vorübergehende Aufzeichnung, Transkription und Kategorisierung von Telefonanrufen beim Telefonassistenten
- Authentifizierung und Identifikation von Nutzern
- Abruf und Abgleich patientenbezogener Daten aus dem beim Kunden eingesetzten Praxisverwaltungssystem x.isynet zur Zuordnung von Patienten bzw. Kontakten in medflex (Patient-Matching). Hierfür können insbesondere Name, Geburtsdatum, Kontaktdaten und die PVS-Patienten-ID verarbeitet werden.
- Ergibt das Patient-Matching mehrere mögliche Treffer, erfolgt keine abschließende automatische Zuordnung durch medflex. Die Auswahl und Bestätigung des zutreffenden Kontakts erfolgt durch einen hierzu autorisierten Nutzer des Kunden.
- Soweit x.isynet die entsprechende Funktion unterstützt, kann ein Patient aus medflex heraus im PVS angelegt werden. Ist dies technisch nicht vorgesehen, kann der betreffende Kontakt ausschließlich im Zusammenhang mit der jeweiligen Anfrage in medflex verarbeitet bzw. durch einen autorisierten Nutzer des Kunden als dauerhafter Kontakt angelegt werden.
- Automatisierte Löschung nach definierten Fristen
- Backup zur Datensicherung

Zweck der Verarbeitung

Die Verarbeitung dient folgenden Zwecken:

- Ermöglichung einer sicheren und datenschutzkonformen Kommunikation zwischen Ärzten und Patienten
- Vereinfachung der Praxisorganisation und Entlastung des Praxispersonals
- Verbesserung der Erreichbarkeit medizinischer Einrichtungen
- Sicherstellung der Einhaltung berufsrechtlicher Vorgaben bei der digitalen Kommunikation im Gesundheitswesen
- Bereitstellung von Funktionen zur Erfüllung der ärztlichen Dokumentationspflicht
- Anbindung des Praxisverwaltungssystems x.isynet sowie Zuordnung von Kommunikationsvorgängen, Anfragen und Kontakten zu den zutreffenden Patienten zur Unterstützung der Arbeitsabläufe des Kunden.

Dauer der Verarbeitung

- Nachrichten und Anhänge sowie die in der medflex-App bereitgestellten aufbereiteten Anliegen und Gesprächszusammenfassungen werden spätestens nach 105 Tagen gelöscht, soweit nicht für einzelne Datenarten abweichende, in dieser Anlage genannte Fristen gelten. Die 105-Tage-Frist dient insbesondere der Nachvollziehbarkeit von Kommunikations- und Abrechnungsvorgängen und wird mit Abschluss dieses AVV als dokumentierte Weisung des Kunden vereinbart. Eine kundenspezifische Anpassung dieser Standardfrist ist nicht vorgesehen.

- Beim KI-Telefonassistenten werden Audio-Rohdaten und Rohtranskripte grundsätzlich nur für die unmittelbare Gesprächsverarbeitung verwendet und anschließend gelöscht, soweit nicht für eine ausdrücklich vereinbarte Produktfunktion eine abweichende Speicherung vorgesehen ist.
- Technische Betriebs-, Verbindungs- und Sicherheitsprotokolle unterliegen gesonderten, zweckbezogenen Speicher- und Löschrufen. Konkrete Fristen richten sich nach der jeweils eingesetzten und dokumentierten Produkt- bzw. Dienstkonfiguration.
- Patienten- bzw. Kontaktdatenätze, die ausschließlich in medflex angelegt werden und nicht aus x.isynet stammen, bleiben gespeichert, bis sie durch einen hierzu berechtigten Nutzer des Kunden gelöscht werden oder die Löschung aufgrund der Beendigung des Vertragsverhältnisses nach den Regelungen dieses AVV erfolgt. Die für bestimmte Kommunikationsinhalte vorgesehene Löschrufen von 105 Tagen führt nicht automatisch zur Löschung eines solchen Patienten- bzw. Kontaktdatenatzes.
- Bestandsdaten aktiver Nutzer werden für die Dauer der Nutzung des Dienstes gespeichert
- Nach Beendigung des Vertragsverhältnisses werden sämtliche Daten gemäß Vereinbarung dieses Vertrags gelöscht oder zurückgegeben
- Daten, die gesetzlichen Aufbewahrungspflichten unterliegen (z.B. Rechnungsdaten), werden für die Dauer der gesetzlich vorgeschriebenen Frist aufbewahrt und anschließend gelöscht

Kategorien betroffener Personen

Die Verarbeitung betrifft folgende Personengruppen:

- Ärzte, Zahnärzte, Psychotherapeuten, Gutachter und andere medizinische Fachkräfte
- Mitarbeiter der medizinischen Einrichtungen
- Patienten der medizinischen Einrichtungen
- Anfragende Personen (potentielle Patienten)
- Anrufer bei Verwendung des Telefonassistenten

Kategorien personenbezogener Daten

Bestandsdaten der Fachkräfte und ihrer Mitarbeiter

- Identifikationsdaten: Name, Vorname, Fachgebiet
- Kontaktdaten: E-Mail-Adresse, Telefonnummer (optional), Postleitzahl
- Zugangsdaten: Passwort (gespeichert als Hash)

Bestandsdaten der Patienten

- Identifikations- und Zuordnungsdaten: Name, Vorname, Geburtsdatum, PVS-Patienten-ID
- Kontaktdaten: E-Mail-Adresse, Telefonnummer (optional)
- Daten aus dem angebundenen Praxisverwaltungssystem x.isynet: je nach eingesetzter Funktion insbesondere Termini, administrative Marker am Patienten sowie BMP-Daten und Dokumente
- Zugangsdaten: Passwort (gespeichert als Hash) bei registrierten Patienten

Kommunikationsdaten

- Chat-Nachrichten und -Anhänge
- Kommunikationshistorie (Metadaten wie Zeitstempel, Teilnehmer, Art der Kommunikation)
- Verbindungsdaten bei Videosprechstunden (technische Metadaten zur Verbindungsqualität)
- Sprachaufzeichnungen und Transkriptionen bei Verwendung des Telefonassistenten
- Anfrageninhalte aus verschiedenen Kommunikationskanälen

Dokumente

- Durch den Kunden erstellte und übermittelte Dokumente (z.B. Anamnesebögen, Einwilligungserklärungen)
- Unterschriften der Patienten bei digitalen Formularen

Verarbeitung besonderer Kategorien personenbezogener Daten

Bei folgenden Datenkategorien können besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO enthalten sein:

- Chat-Nachrichten zwischen Ärzten und Patienten
- Anfrageninhalte und Kommunikationshistorien
- Sprachaufzeichnungen und deren Transkriptionen
- Übermittelte medizinische Dokumente (z.B. Anamnesebögen, Befunde). Diese Daten können besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO enthalten. Ihre Verarbeitung erfolgt gemäß Art. 9 Abs. 2 DSGVO und unter Anwendung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO.

- Daten aus dem angebundenen Praxisverwaltungssystem x.isynet, soweit diese im jeweiligen Anwendungsfall Gesundheitsdaten oder sonstige besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO enthalten, insbesondere BMP-Daten und medizinische Dokumente.

Die Verarbeitung dieser Daten erfolgt gemäß Art. 9 Abs. 2 lit. h DSGVO (Gesundheitsversorgung und Behandlung im Gesundheitsbereich) in Verbindung mit § 22 Abs. 1 Nr. 1 lit. b BDSG bzw. den entsprechenden landesrechtlichen Regelungen. Bei der Verarbeitung werden angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen gemäß Art. 32 DSGVO angewandt, wie in Anlage 3 detailliert beschrieben.

KI-Modell für den Telefonassistenten

medflex setzt für den interaktiven Telefonassistenten KI-gestützte Sprach- und Textverarbeitung ein. Hierzu werden entsprechend konfigurierte Cloud-Dienstleistungen mit europäischer Datenresidenz eingesetzt.

- Die für den Telefonassistenten verarbeiteten Daten werden nicht zum Training oder zur Verbesserung der eingesetzten KI-Modelle verwendet. Eine dauerhafte Speicherung personenbezogener Daten im KI-Modell erfolgt nicht. Die Speicherung aufbereiteter Gesprächsinformationen in der medflex-App richtet sich nach den vorstehenden Löschregelungen.
- Die reguläre Datenverarbeitung erfolgt an europäischen Verarbeitungsstandorten. Etwaige Drittlandzugriffe unterliegen den in § 5 Abs. 6 geregelten Anforderungen.
- Es werden keine personenbezogenen Daten im Modell gespeichert oder persistiert.
- Zugriffskontrolle, Verschlüsselung sowie weitere organisatorische und technische Maßnahmen sind nach Stand der Technik umgesetzt (z. B. TLS, Verschlüsselung im Ruhezustand, rollenbasierte Kontrollen).

Information der betroffenen Personen und Transparenzpflichten

Der Kunde ist als Verantwortlicher für die Erfüllung der datenschutzrechtlichen Informationspflichten gegenüber den betroffenen Personen, insbesondere nach Art. 13 DSGVO, verantwortlich. Dies umfasst auch die Festlegung der Form, des Inhalts und des Zeitpunkts der Information der betroffenen Personen.

medflex stellt dem Kunden die technische Möglichkeit zur Verfügung, den Ansagetext des Telefonassistenten selbst zu konfigurieren. Der Kunde entscheidet eigenverantwortlich, welche Informationen er in den Ansagetext aufnimmt und welche ergänzenden Informationen er über seine Website oder andere Informationskanäle bereitstellt. Die datenschutzrechtliche Bewertung und Ausgestaltung der vom Kunden verwendeten Ansagetexte und Datenschutzhinweise verbleiben beim Kunden.

medflex stellt dem Kunden die technische Möglichkeit bereit, Anrufende über die Interaktion mit einem KI-System zu informieren. Der Kunde sorgt im Rahmen seiner datenschutzrechtlichen Verantwortlichkeit für die ordnungsgemäße Verwendung und Ausgestaltung der entsprechenden Ansage und ergänzender Datenschutzhinweise. Etwaige eigenständige gesetzliche Pflichten von medflex als Anbieter des KI-Systems bleiben hiervon unberührt.

Hinweise zur Systemnutzung

Der Umfang, Inhalt und die Art der verarbeiteten Daten hängen maßgeblich von den Eingaben der jeweiligen Nutzer (Behandler, Mitarbeiter, Patienten) ab. medflex stellt lediglich die technische Infrastruktur zur Verfügung und hat keinen Einfluss auf die Art, den Inhalt und Umfang der durch die Nutzer eingegebenen Daten.

Die Videochat-Funktion entspricht den Anforderungen der KBV gemäß Anlage 31b zum BMV-Ä und ist entsprechend zertifiziert. Für die inhaltliche Kommunikation sind die Nutzer selbst verantwortlich; medflex übernimmt die technische Bereitstellung und bietet keine medizinischen oder therapeutischen Leistungen an.

Bei der Anbindung von x.isynet sind die über das PVS bereitgestellten Patientendaten ausschließlich für hierzu autorisierte Nutzer auf Seiten des Kunden zugänglich. Patienten sehen ausschließlich die ihnen zugeordneten eigenen Anfragen. Sofern das Patient-Matching mehrere mögliche Treffer ergibt, werden diese möglichen Zuordnungen dem Patienten nicht angezeigt; die abschließende Zuordnung erfolgt durch einen autorisierten Nutzer des Kunden.

Anlage 2 - Subunternehmer

Hosting

Name	Anschrift	Funktion	Ort der Verarbeitung
OVHcloud	OVH GmbH, St. Johanner Str. 41-43, 66111 Saarbrücken, Deutschland	Rechenzentrum	EU
MongoDB	MongoDB Ltd., Shelbourne Rd, Ballsbridge, Dublin D04 Y3X9, Irland	Datenhaltung/Suchfunktion	EU

Telefonassistent Classic¹ / interaktive Gesprächsführung²

Name	Anschrift	Funktion	Ort der Verarbeitung
Microsoft ^{1,2}	Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park, Dublin D18 P521, Irland	Nachbearbeitung, z.B. Zusammenfassung von Patientenfragen	EU
Twilio ^{1,2}	Twilio Germany GmbH, Unter den Linden 10, 10117 Berlin, Deutschland	Anruf-Routing für den Telefonassistenten	EU
Elevenlabs ²	ElevenLabs Poland LLC, Lipska 27/22, 03-907 Warschau, Polen	Kommunikationsagent	EU

Kommunikationsdienste

Name	Anschrift	Funktion	Ort der Verarbeitung
Arztkonsultation ³	arztkonsultation ak GmbH, Schusterstr. 3, 19055 Schwerin, Deutschland	Video Kommunikation API	EU

Zustimmungsverwaltung

Name	Anschrift	Funktion	Ort der Verarbeitung
CCM19	Papoo Software & Media GmbH, Auguststr. 4, 53229 Bonn, Deutschland	Zustimmungsverwaltung	EU

Benachrichtigungsdienste

Name	Anschrift	Funktion	Ort der Verarbeitung
Cleverpush	CleverPush GmbH, Brauhausstr. 15A, 22041 Hamburg, Deutschland	Benachrichtigungen	EU
Brevo	Sendinblue GmbH, Köpenicker Str. 126, 10179 Berlin, Deutschland	Benachrichtigungen	EU
smsmode	Calade Technologies SARL, 4 rue Duverger, 13002 Marseille, Frankreich	Benachrichtigungen	EU

Technische Integrationspartner, optional vom Kunden beauftragt.

Keine Subunternehmer von medflex.

Die nachfolgend genannten Unternehmen sind keine Unterauftragnehmer von medflex im Sinne des Art. 28 Abs. 2 DSGVO. Sie können vom Kunden optional und unmittelbar mit der technischen Einrichtung oder Betreuung der PVS-Anbindung beauftragt werden. Das entsprechende Vertrags- und datenschutzrechtliche Verhältnis besteht in diesem Fall unmittelbar zwischen dem Kunden und dem jeweiligen Integrationspartner. Erforderliche Vereinbarungen, insbesondere ein gegebenenfalls erforderlicher Auftragsverarbeitungsvertrag, werden unmittelbar zwischen dem Kunden und dem jeweiligen Integrationspartner abgeschlossen.

Name	Anschrift	Funktion	Ort der Verarbeitung
CTL	CTL GmbH, Im Hart 18, 89558 Böhmenkirch, Deutschland	Optionale technische PVS-/GDT-/BDT-Anbindung	EU
xSolve	xSolve GmbH, Kreutzerweg 4, 77654 Offenburg, Deutschland	Optionale technische PVS-/GDT-/BDT-Anbindung	EU

¹ Betrifft den Telefonassistent Classic

² Betrifft den Telefonassistent interaktive Gesprächsführung

³ Betrifft den Video-Messenger

Anlage 3 - Technische und organisatorische Maßnahmen

Auftragsverarbeiter: medflex GmbH

Rechtsgrundlage: Art. 32 DSGVO - Sicherheit der Verarbeitung

1 Datenschutzorganisation

1.1 Datenschutz-Managementsystem

- Etablierung eines Datenschutz-Managementsystems zur Kontrolle und Überwachung der Einhaltung datenschutzrechtlicher Anforderungen
- Regelmäßige Überprüfung der Maßnahmen auf Aktualität und Wirksamkeit
- Regelungen zur sicheren Datenvernichtung nach Beendigung von Verarbeitungstätigkeiten
- Datenschutzrichtlinie als Handlungsrahmen für alle Mitarbeitenden

1.2 Zuständigkeiten & Rollen

- Bestellter Datenschutzbeauftragter
- Regelmäßige Audits zur Wirksamkeit der TOM
- Datenschutzrechtliche Begleitung der Dienstleisterkontrolle durch den DSB und zuständige Fachbereiche
- Durchführung regelmäßiger Datenschutz- und KI-Schulungen für Mitarbeiter
- Verpflichtung aller mit der Verarbeitung personenbezogener Daten betrauten Mitarbeiter zur Vertraulichkeit gemäß Art. 28 Abs. 3 lit. b DSGVO sowie zur Wahrung der gesetzlichen Verschwiegenheitspflichten, insbesondere nach § 203 StGB, § 3 TDDDG und § 206 StGB sowie § 35 SGB I, soweit diese jeweils anwendbar sind.

2. Maßnahmen zur Gewährleistung der Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Zutrittskontrolle

Schutz vor unbefugtem physischen Zugang zu Datenverarbeitungsanlagen

- Kontrollierte physische Zutrittsverfahren in den Rechenzentren der eingesetzten Hosting-Dienstleister
- Besuchermanagement inkl. Begleitung
- Elektronische Zutrittskontrollen und Dokumentation bei den eingesetzten Rechenzentrumsbetreibern
- Gesicherte Rechenzentrums- und Serverbereiche bei den beauftragten Hosting-Dienstleistern
- Zutrittskontrollsysteme: Ausweisleser, Magnet-/Chipkarten
- Alarmsicherung, Türsicherungen, Gebäudesicherung

2.2 Zugangskontrolle

Schutz vor unbefugter Nutzung von IT-Systemen

- Gesicherte administrative Verwaltung der eingesetzten Cloud- und Serversysteme
- VPN-Zugang mit Zwei-Faktor-Authentifizierung für Telearbeitsplätze
- Passwortmanagement (Mindestlänge, Komplexität, sichere Vergabe und anlassbezogener Wechsel)
- Login-Sperrung nach Fehlversuchen
- Gezielte Rechtevergabe pro Benutzer
- Verschlüsselung von Datenträgern
- Netzwerk- und Anwendungsschutz einschließlich geeigneter Firewall-Funktionen
- Mobile Device Management (Fernlöschung/-sperrung)
- Schutzmaßnahmen für BYOD-Endgeräte

2.3 Zugriffskontrolle

Schutz vor unbefugtem Zugriff innerhalb von Systemen

- Persönliche Benutzerkonten und differenzierte Berechtigungen
- Berechtigungskonzepte mit Rollenzuweisung
- Zugriffsbeschränkungen auf Datei-/Verzeichnisebene

- Kryptographische Maßnahmen (VPN, Verschlüsselung)
- Protokollierung von Zugriffen in Logs
- Regelmäßige System-Updates
- Klassische Rollenverteilung: Lesen, Schreiben, Löschen

2.4 Trennungskontrolle

Getrennte Verarbeitung von Daten zu unterschiedlichen Zwecken

- Projektbezogene Ordnerstrukturen
- Mandantentrennung (logisch)
- Trennung von Produktiv- und Testsystemen
- Separierung von Datenbanken und Tabellen
- Zweckbindung gemäß Auftraggeberweisung
- Funktionstrennung für Test/Produktiv/Sandbox

3. Maßnahmen zur Sicherstellung der Integrität (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Weitergabekontrolle

Schutz vor unbefugter Offenlegung bei Übertragung

- Keine Offenlegung gegenüber unberechtigten Dritten; Weitergabe nur soweit gesetzlich oder vertraglich vorgesehen
- Transportverschlüsselung geeigneter Kommunikationskanäle, insbesondere mittels HTTPS/TLS oder VPN
- Datensparsame Protokollierung sicherheitsrelevanter Netzwerk- und Systemereignisse
- Versand von Datenträgern nur verschlüsselt, durch autorisierte Personen oder Kurier
- Zerstörung physischer Medien vor Entsorgung (Papier, CD/DVD)
- Datenschutzgerechte Entsorgung durch zertifizierte Dienstleister
- Organisatorische Regeln für Wartung, Reparatur und Außerdienststellung

3.2 Eingabekontrolle

Nachvollziehbarkeit, ob und von wem personenbezogene Daten eingegeben, verändert oder gelöscht wurden

- Organisatorische Festlegung von Zuständigkeiten
- Zugriffsteuerung auf Serverebene
- Eingabekontrolle auf Feldebene nur begrenzt möglich – wird durch organisatorische Verfahren ersetzt
- Sicherung von Protokolldaten gegen Veränderung und Verlust

4. Maßnahmen zur Sicherstellung der Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b, c DSGVO)

4.1 Verfügbarkeitskontrolle

Schutz gegen zufälligen oder mutwilligen Verlust/Schaden

- Regelmäßige, bedarfsgerechte Datensicherungen nach dokumentiertem Backup-Konzept
- Archivierung gemäß gesetzlicher Aufbewahrungsfristen
- Betrieb zentraler Serversysteme in gesicherter Umgebung
- Räumlich getrennte Sicherungsspeicher
- Redundanzsysteme und USV (unterbrechungsfreie Stromversorgung)
- Peripheriesysteme zur Brandfrüherkennung, Klimatisierung
- Gesicherte, vom Produktivsystem getrennte Datensicherungen nach dem jeweiligen Backup-Konzept
- Überspannungsschutz, Diebstahlschutz, Virenschutz

4.2 Wiederherstellbarkeit

Wiederherstellung von Daten bei technischen oder physischen Zwischenfällen

- Notfallmanagement inkl. Notfallplänen
- Testverfahren zur Überprüfung der Wiederherstellung
- Dokumentierte Handlungsanleitungen zur Notfallbewältigung

5. Maßnahmen zur Umsetzung des Rechts auf Löschung (Art. 17 DSGVO)

- Implementierung von Fernlöschfunktionen auf mobilen Endgeräten
- Anwendungsbezogene Löschung personenbezogener Datensätze und sichere Verfahren zur Löschung von Datenträgern
- Automatische Löschung nach Ablauf definierter Fristen
- Protokollierung von Löschvorgängen
- Mechanische Vernichtung von Datenträgern (Schreddern, physikalische Zerstörung)
- Auswahl zertifizierter Entsorgungsdienstleister

6. Maßnahmen zur kontinuierlichen Kontrolle und Evaluierung (Art. 32 Abs. 1 lit. d, Art. 25 Abs. 1 DSGVO)

- Regelmäßige Überprüfung und Evaluierung der TOM
- Datenschutzaudits zur Wirksamkeitskontrolle
- Datenschutzfreundliche Voreinstellungen (Privacy by Design & Default)
- Klare vertragliche Regelungen bei Auftragsverarbeitung (AV-Verträge)
- Nachkontrollen bei Dienstleistern
- Trennung von Datenschutzmaßnahmen für verschiedene Unternehmensbereiche

7. Gesamteinschätzung gem. Art. 32 Abs. 1 DSGVO

Die dokumentierten Maßnahmen entsprechen dem Stand der Technik, dem wirtschaftlich vertretbaren Aufwand sowie Art, Umfang und Zweck der Datenverarbeitung. Sie sind geeignet, ein dem Risiko angemessenes Schutzniveau zu gewährleisten und die Rechte und Freiheiten betroffener Personen zu schützen.