Auftragsverarbeitungsvertrag gem. Art. 28 DSGVO - medflex

zwischen

medflex GmbH
Reichenaustraße 39a
78467 Konstanz
Deutschland

- im Folgenden: „medflex“ -

und

_____

_____

_____

_____

- 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 stellt einen betrieblichen Datenschutzbeauftragten und verpflichtet alle Mitarbeiter zur Wahrung der Schweigepflicht gem. § 203 StGB, der Vertraulichkeit nach Art. 28 Abs. 3 lit. b DSGVO,

§ 23 GeschGehG sowie § 3 TDDDG i. V. m. § 206 StGB, zur Einhaltung des Sozialgeheimnisses gem. § 35 SGB I und zur Wahrung des Datengeheimnisses gem. § 53 BDSG.

(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 unterstützt den Kunden bei der Erfüllung seiner Pflichten nach Art. 12-22, 32, 35 und 36 DSGVO, soweit dies technisch und wirtschaftlich zumutbar ist. Dies umfasst insbesondere die Unterstützung bei der Durchführung von Datenschutz-Folgenabschätzungen gemäß Art. 35 DSGVO sowie bei der vorherigen Konsultation der Aufsichtsbehörde gemäß Art. 36 DSGVO, wenn eine Datenschutz-Folgenabschätzung ergibt, dass die Verarbeitung ein hohes Risiko zur Folge hätte.

(7) Anfragen von betroffenen Personen leitet medflex unverzüglich an den Kunden weiter und setzt dessen Weisungen zur Umsetzung von Betroffenenrechten um.

§ 5 Subunternehmer

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung gelten Dienstleistungen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht darunter fallen Nebenleistungen, wie beispielsweise Telekommunikationsleistungen, Post- und Transportdienste, Wartungs- und Benutzerservices oder die Entsorgung von Datenträgern, sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit von Datenverarbeitungsanlagen und -systemen. medflex stellt sicher, dass bei solchen Nebenleistungen die Anforderungen an den Datenschutz und die Datensicherheit ebenfalls eingehalten werden.

(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 über Änderungen bei Subunternehmern durch Veröffentlichung auf seiner Website und per E-Mail-Benachrichtigung.

(4) Der Kunde kann innerhalb von 30 Tagen nach Benachrichtigung begründete Einwände gegen neue Subunternehmer erheben. Erfolgen keine Einwände, gilt die Zustimmung als erteilt.

(5) medflex dokumentiert alle eingesetzten Subunternehmer und deren Datenschutzmaßnahmen.

(6) medflex beauftragt Subunternehmer mit Sitz innerhalb der Europäischen Union. Der Einsatz erfolgt unter Abschluss eines den Anforderungen des Art. 28 DSGVO entsprechenden Auftragsverarbeitungsvertrags (AVV). Eine Datenverarbeitung durch Dienstleister außerhalb der EU oder des EWRs findet derzeit nicht statt. Sollte in Ausnahmefällen eine Drittlandverarbeitung erforderlich werden, erfolgt dies ausschließlich unter Verwendung geeigneter Garantien gemäß Kapitel V DSGVO (z. B. Standardvertragsklauseln oder Binding Corporate Rules) - und nur nach vorheriger Information der Kunden mit Möglichkeit zum Widerspruch gem. den vertraglichen Vereinbarungen.

§ 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) Die Kosten für Kontrollen trägt der Kunde, soweit sie über das übliche Maß hinausgehen. Dies gilt nicht, wenn durch eine Kontrolle ein Datenschutzverstoß 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 AVVs, 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.

(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

Die Verarbeitung erfolgt ausschließlich auf Weisung des Kunden und dient der Unterstützung seiner medizinischen Leistungserbringung.

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
- Aufzeichnung, Transkription und Kategorisierung von Telefonanrufen beim Telefonassistenten
- Authentifizierung und Identifikation von Nutzern
- 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

Dauer der Verarbeitung

- Sämtliche Kommunikationsinhalte (Nachrichten, Sprachaufzeichnungen, Transkriptionen) werden automatisch nach 105 Tagen gelöscht; diese Frist ergibt sich aus den quartalsweisen Abrechnungsanforderungen medizinischer Einrichtungen, um erbrachte Leistungen für die Abrechnung nachvollziehen zu können.
- 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
- Identifikationsdaten: Name, Vorname
- Kontaktdaten: E-Mail-Adresse, Telefonnummer (optional)
- 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.

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 ein vortrainiertes Large Language Model (LLM) ein, das ohne externe Verbindungen in einer isolierten Enterprise European Data Residency Daten verarbeitet.
- Die Eingaben und Ergebnisse werden nicht zur Verbesserung oder zum Training des Modells verwendet und nicht gespeichert.
- Die Datenverarbeitung erfolgt ausschließlich in europäischen Rechenzentren und unterliegt europäischen Datenschutzstandards.
- 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).

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.

Anlage 2 - Subunternehmer

Hosting

Name	Anschrift	Funktion	Ort der Verarbeitung
OVHcloud	OVH GmbH St. Johanner Str. 41-43 66111 Saarbrücken, Deutschland	Rechenzentrum	EU

Telefonassistent Classic[1] / interaktive Gesprächsführung[2]

Name	Anschrift	Funktion	Ort der Verarbeitung
Microsoft[1,2]	Microsoft Deutschland GmbH Walter-Gropius-Straße 5, 80807 München Deutschland	Terminbuchung Transkription vortrainiertes isoliertes LLM auf Azure	EU
Twilio[1,2]	Twilio Germany GmbH Unter den Linden 10, 10117 Berlin Deutschland	Telefonanlage des 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	Zustimmungs-verwaltung	EU

Benachrichtungsdienste

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

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

Verantwortlicher: medflex GmbH
Rechtsgrundlage: Art. 32 DSGVO - Sicherheit der Verarbeitung

1 Datenschutzorganisation

1.1 Datenschutz-Managementsystem

- Etablierung eines Datenschutz-Managementsystems (DSMS) 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 (DSB)
- Regelmäßige Audits zur Wirksamkeit der TOM
- Auftragskontrolle durch den DSB, inkl. Überprüfung von Dienstleistern
- Durchführung regelmäßiger Datenschutzschulungen für Mitarbeitende
- Verpflichtung aller Mitarbeiter zur Wahrung der Schweigepflicht gem. § 203 StGB, der Vertraulichkeit nach Art. 28 Abs. 3 lit. b DSGVO, § 23 GeschGehG sowie § 3 TDDDG i. V. m. § 206 StGB, zur Einhaltung des Sozialgeheimnisses gem. § 35 SGB I und zur Wahrung des Datengeheimnisses gem. § 53 BDSG

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

2.1 Zutrittskontrolle

Schutz vor unbefugtem physischen Zugang zu Datenverarbeitungsanlagen

- Zentraler Empfang für Besucher und Dienstleister
- Besuchermanagement inkl. Begleitung
- Elektronische Schließsysteme mit Zugangs-Batches und Protokollierung
- Serverraum mit separatem Schließbereich
- Zutrittskontrollsysteme: Ausweisleser, Magnet-/Chipkarten
- Alarmsicherung, Türsicherungen, Gebäudesicherung

2.2 Zugangskontrolle

Schutz vor unbefugter Nutzung von IT-Systemen

- Zentrale Serververwaltung im gesicherten Bereich
- VPN-Zugang mit Zwei-Faktor-Authentifizierung für Telearbeitsplätze
- Passwortmanagement (Mindestlänge, Komplexität, regelmäßiger Wechsel)
- Login-Sperrung nach Fehlversuchen
- Gezielte Rechtevergabe pro Benutzer
- Verschlüsselung von Datenträgern
- Software- und Hardware-Firewall
- 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

- Grundsatz: Keine Weitergabe an Dritte, außer gesetzlich/vertraglich notwendig
- Verschlüsselung bei Übertragungen (VPN, https, E-Mail)
- Protokollierung des Datenverkehrs (ein- und ausgehend)
- 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

- Tägliche, wöchentliche und monatliche Datensicherungen (inkrementell/vollständig)
- Archivierung gemäß gesetzlicher Aufbewahrungsfristen

- Betrieb zentraler Serversysteme in gesicherter Umgebung
- Räumlich getrennte Sicherungsspeicher
- Redundanzsysteme und USV (unterbrechungsfreie Stromversorgung)
- Peripheriesysteme zur Brandfrüherkennung, Klimatisierung
- Online- und Offline-Backup-Strategien
- 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
- Einfache Löschung und randomisiertes Überschreiben von Datensätzen
- 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.