Auftragsspezifische Vereinbarungen

1. Gegenstand und Dauer der Auftragsdatenverarbeitung

Bezüglich Gegenstand und Dauer der Auftragsdatenverarbeitung wird auf den zwischen den Parteien bestehenden Hauptvertrag verwiesen.

2. Umfang, Art und Zweck der Datenverarbeitung, Art der Daten und Kreis der Betroffenen

Umfang, Art und Zweck der Datenverarbeitung: Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Umfang, Art und Zweck der Aufgaben des Aufragnehmers ergibt sich aus dem Rahmenvertrag SciTIM Dienstleistung on Demand. Die Auftragsdatenverarbeitung erfolgt nur innerhalb Deutschland.

Kreis der Betroffenen (Kategorien):
-Ärzte
-Patienten
-Mitarbeiter
-Lieferanten
-Dienstleister
-Ansprechpartner

Art der Daten (Kategorien):
-Blutdruckwerte
-Patienteninformationen
-Geräteinformationen
-weitere Vitaldaten wie Gewicht usw.

3. Weisungsberechtigte Personen des Auftraggebers

[Auftraggeber]

4. Weisungsberechtigte Personen des Auftragnehmers

Tino Römer

TIM Telemonitoring Interventions in Medicine UG (haftungsbeschränkt)

Gartenstrasse 22a, D-82049 Pullach im Isartal

Tel. +49 (0)89 / 69 39 55 90 Fax +49 (0)89 / 69 39 55 91

E-Mail: roemer@tim-med.de

Unterauftragsverhältnisse

Als Unterauftragnehmer werden derzeit seitens des Auftragnehmers folgende Unternehmen (Firma, Anschrift, im Rahmen der Auftragsdatenverarbeitung wahrgenommene Tätigkeit) oder freien Mitarbeiter (Name, Anschrift, im Rahmen der Auftragsdatenverarbeitung wahrgenommene Tätigkeit) eingesetzt:

eddyson GmbH
Anschrift: Groner Landstr. 23/25
37079 Göttingen
Deutschland
Kontakt: +49 (0) 551 / 77077600
37081 Göttingen
info@eddyson.de
https://www.eddyson.de

IT-Programmierung, Entwicklung und Betreuung

OEDIV Oetker Daten- und Informationsverarbeitung KG
Anschrift: Bechterdisser Str, 10
33719 Bielefeld
Deutschland
Kontakt: +49 (0) 521 / 260500
kontakt@oediv.de
https://www.oediv.de

Datenbankhosting , Rechenzentrumsbetrieb und Application Hosting

Technische und organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

Der Auftragnehmer verhindert, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen haben.

Der Auftragnehmer hat folgende Maßnahmen zur Zutrittskontrolle ergriffen:

☒ Zutrittskontrollsystem, Ausweisleser (Magnet-/Chipkarte)

☒ Türsicherungen (elektrische Türöffner, Zahlenschloss, etc.)

☒ Sicherheitstüren / -fenster

☐ Gitter vor Fenstern/Türen

☒ Zaunanlagen

☒ Schlüsselverwaltung/Dokumentation der Schlüsselvergabe

☒ Werkschutz, Pförtner

☒ Alarmanlage

☒ Videoüberwachung

☒ Spezielle Schutzvorkehrungen des Serverraums

☒ Spezielle Schutzvorkehrungen für die Aufbewahrung von Back-Ups und/oder sonstigen Datenträgern

☒ Nicht-reversible Vernichtung von Datenträgern

☒ Mitarbeiter- und Berechtigungsausweise

☐ Sperrbereiche

☒ Besucherregelung (Bspw. Abholung am Empfang, Dokumentation von Besuchszeiten, Besucherausweis, Begleitung nach dem Besuch bis zum Ausgang)

☐ sonstiges: [Bitte ausführen]

Zugangskontrolle

Der Auftragnehmer stellt sicher, dass Unbefugte keinen Zugang zu den Datenverarbeitungssystemen haben.

Der Auftragnehmer hat folgende Maßnahmen zur Zugangskontrolle ergriffen:

☒ Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk

☒ Autorisierungsprozess für Zugangsberechtigungen

☒ Begrenzung der befugten Benutzer

☒ Single Sign-On

☐ BIOS-Passwörter

☒ Kennwortverfahren (Angabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsintervall)

☒ Elektronische Dokumentation von Passwörtern und Schutz dieser Dokumentation vor unbefugtem Zugriff

☒ Personalisierte Chipkarten, Token, PIN-/TAN, etc.

☒ Protokollierung des Zugangs

☒ Zusätzlicher System-Log-In für bestimmte Anwendungen

☒ Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung)

☒ Firewall

☐ sonstige: [Bitte ausführen]

Zugriffskontrolle

Der Auftragnehmer stellt sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben.

Der Auftragnehmer hat folgende Maßnahmen zur Zugriffskontrolle ergriffen:

☒ Verwaltung und Dokumentation von differenzierten Berechtigungen

☒ Sorgfältige Auswahl des Personals für die externe Pflege, Wartung und Reparatur von Datenverarbeitungsanlagen

☒ Auswertungen/Protokollierungen von Datenverarbeitungen

☒ Autorisierungsprozess für Berechtigungen

☒ Genehmigungsroutinen

☒ Profile/Rollen

☐ Verschlüsselung von CD/DVD- ROM, externen Festplatten und/oder Laptops (etwa per Betriebssystem, TrueCrypt, Safe Guard Easy, WinZip, PGP)

☒ Maßnahmen zur Verhinderung unbefugten Überspielens von Daten auf extern verwendbare Datenträger (z.B. Kopierschutz, Sperrung von USB-Ports, „Data Loss Prevention (DLP)-System“)

☐ „Mobile Device Management-System“

☒ Vier-Augen-Prinzip

☒ Funktionstrennung „Segregation of Duties“

☒ Fachkundige Akten- und Datenträgervernichtung gemäß DIN 66399

☒ Nicht-reversible Löschung von Datenträgern

☐ Sichtschutzfolien für mobile Datenverarbeitungssysteme

☒ sonstige: Prüfung / Auditierung (etwa im Rahmen von ISO-Zertifizierung, SOX-Compliance)

Trennungskontrolle

Der Auftragnehmer stellt sicher, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden.

Der Auftragnehmer hat folgende Maßnahmen zur Trennungskontrolle ergriffen:

☒ Speicherung der Datensätze in physikalisch getrennten Datenbanken

☒ Getrennte Systeme (logische Trennung)

☒ Zugriffsberechtigungen nach funktioneller Zuständigkeit

☒ Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen

☒ Mandantenfähigkeit von IT-Systemen

☒ Pseudonymisierung von Daten

☒ Verwendung von Testdaten

☒ Trennung von Entwicklungs- und Produktionsumgebung

☐ Sonstiges: [Bitte ausführen]

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

Der Auftragnehmer stellt sicher, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben.

Der Auftragnehmer hat folgende Maßnahmen zur Weitergabekontrolle ergriffen:

☐ Verschlüsselung von Email bzw.- Email-Anhängen (z.B. WinZip)

☒ Verschlüsselung des Speichermediums von Laptops

☒ Gesicherter File Transfer (z.B. sftp)

☒ Gesicherter Datentransport (z.B. SSL, ftp, ftps, TLS)

☐ Verschlüsselung von CD/DVD- ROM, externen Festplatten oder USB-Sticks (z.B. True Crypt, Safe Guard Easy, PGP)

☒ Physikalische Transportsicherung

☒ Verpackungs- und Versandvorschriften

☐ Elektronische Signatur

☒ Gesichertes WLAN

☒ Fernwartungskonzept (z.B. Verschlüsselung, Ereignisauslösung durch Auftraggeber, Challenge-Response, Rückrufautomatik, Einmal-Passwort)

☐ „Mobile Device Management-System“

☒ „Data Loss Prevention (DLP)-System“

☒ Regelung zum Umgang mit mobilen Speichermedien (z.B. Laptop, USB-Stick, Mobiltelefon)

☒ Protokollierung von Datenübertragung oder Datentransport

☒ Protokollierung von lesenden Zugriffen

☒ Protokollierung des Kopierens, Veränderns oder Entfernens von Daten

☒ Getunnelte Datenfernverbindungen (VPN = Virtuelles Privates Netzwerk)

☒ sonstige: Exklusive WAN-Verbindungen mit Zugriffskontrollen

Eingabekontrolle

Der Auftragnehmer stellt sicher, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat. Der Auftragnehmer hat folgende Maßnahmen zur Eingabekontrolle ergriffen:

☒ Zugriffsrechte

☒ Systemseitige Protokollierungen

☒ Dokumenten Management System (DMS) mit Änderungshistorie

☒ Sicherheits-/Protokollierungssoftware

☒ Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten

☒ Mehraugenprinzip

☒ „Data Loss Prevention (DLP)-System“

☐ sonstige: [Bitte ausführen]

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeits- und Wiedererstellungskontrolle

Der Auftragnehmer stellt sicher, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind.

Der Auftragnehmer hat folgende Maßnahmen zur Verfügbarkeitskontrolle ergriffen:

- ☒ Sicherheitskonzept für Software- und IT-Anwendungen
- ☒ Back-Up Verfahren
- ☒ Aufbewahrungsprozess für Back-Ups (brandgeschützter Safe, getrennter Brandabschnitt, etc.)
- ☒ Gewährleistung der Datenspeicherung im gesicherten Netzwerk
- ☒ Bedarfsgerechtes Einspielen von Sicherheits-Updates
- ☒ Spiegeln von Festplatten
- ☒ Einrichtung einer unterbrechungsfreien Stromversorgung (USV)
- ☒ Geeignete Archivierungsräumlichkeiten für Papierdokumente
- ☒ Brand- und/oder Löschwasserschutz des Serverraums
- ☒ Brand- und/oder Löschwasserschutz der Archivierungsräumlichkeiten
- ☒ Klimatisierter Serverraum
- ☒ Virenschutz
- ☒ Firewall
- ☒ Notfallplan
- ☐ Erfolgreiche Notfallübungen
- ☒ Redundante, örtlich getrennte Datenaufbewahrung (Offsite Storage)
- ☒ sonstige: Alarmanlage

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. b DSGVO; Art. 25 Abs. 1 und 2 DSGVO)

Auftragskontrolle

Der Auftragnehmer stellt sicher, dass personenbezogene Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Der Auftragnehmer hat folgende Maßnahmen zur Auftragskontrolle ergriffen:

- ☒ Schriftlicher Vertrag zur Auftragsdatenverarbeitung gem. Art. 32 Abs. 1 lit. b DSGVO; Art. 25 Abs. 1 und 2 DSGVO mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers
- ☒ Prozess zur Erteilung und/oder Befolgung von Weisungen
- ☒ Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
- ☒ Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung
- ☒ Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragnehmer
- ☐ Unabhängige Auditierung der Weisungsgebundenheit
- ☒ Verpflichtung der Mitarbeiter auf das Datengeheimnis gem. § 5 BDSG
- ☒ Vereinbarung von Konventionalstrafen für Verstöße gegen Weisungen
- ☒ sonstige: Regelmäßige Datenschutzaudits des betrieblichen Datenschutzbeauftragten
- ☒ sonstige: Bestimmung von Ansprechpartnern und verantwortlichen Projektmanagern für den konkreten Auftrag

Incident Management

- ☒ 24/7 Incident Aufnahme
- ☒ Incident Management Prozess
- ☒ Protokollierung

Datenschutz

Technisch-organisatorische Maßnahmen zur Umsetzung datenschutzrechtlicher Vorgaben, d.h. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen. Data Privacy by Design and by Default.

- ☒ Beschränkung bzgl. der Menge der erhobenen Daten
- ☒ Beschränkung des Umfangs der Verarbeitung der erhobenen Daten
- ☒ Beschränkung der Speicherfrist
- ☒ Beschränkung der Zugänglichkeit

Datenschutzrelevante Zertifizierungen

- ☒ Zertifizierung nach ISO 27001
- ☐ Zertifizierung nach ISO 27018
- ☐ sonstige: [Bitte ausführen]