Vereinbarung zum Datenschutz und zur Datensicherheit in Auftragsverhältnissen gem. Art. 28 DSGVO (Auftragsverarbeitung)

zwischen dem Auftraggeber:

⌜ ⌝

(nachstehend „Kunde“ genannt)

und

MediCOM Praxismanagement
Peter Gesang
Über der Nonnenwiese 7
99428 Weimar-Tröbsdorf

(nachstehend „MediCOM“ genannt)

Präambel

Der Kunde hat MediCOM vertraglich zur Erbringung definierter Leistungen beauftragt. Darüber liegen gesonderte Leistungsverträge vor. Im Rahmen der Leistungserbringung kann MediCOM ggf. Zugriff auf vom Kunden gespeicherte oder anders gegenüber der Kunde zur Verfügung gestellte personenbezogene Daten erhalten. Soweit MediCOM solche personenbezogenen Daten im Auftrag des Kunden verarbeitet, handelt es sich um Auftragsverarbeitung im Sinne von Art. 28 der Datenschutz-Grundverordnung („DSGVO"). MediCOM ist in dieser Konstellation Auftragsverarbeiter und der Kunde datenschutzrechtlicher Verantwortlicher. Diese im Auftrag des Kunden verarbeiteten personenbezogenen Daten werden im Folgenden auch als „Kunden - Daten" bezeichnet. Zur Regelung der Verarbeitung personenbezogener Daten durch die MediCOM im Auftrag des Kunden treffen die Vertragspartner diese Vereinbarung zum Datenschutz und zur Datensicherheit in Auftragsverhältnissen gem. Art. 28 DSGVO („Auftragsverarbeitungsvertrag").

§ 1 Datenschutz, Auftragsverarbeitung

1.1 MediCOM beachtet das jeweils geltende Datenschutzrecht und trifft alle notwendigen organisatorischen Maßnahmen, um die Einhaltung des Datenschutzrechts zu gewährleisten.

1.2 Der Kunde ist für die Rechtmäßigkeit der Verarbeitung der Kunden-Daten sowie für die Wahrung der Rechte der betroffenen Personen im Verhältnis der Vertragspartner zueinander allein verantwortlich.

1.3 MediCOM verarbeitet im Auftrag des Kunden möglicherweise auch Daten, die in den Anwendungsbereich von § 203 Strafgesetzbuch („StGB") fallen (im Folgenden „Geheimnisschutzdaten") und wirkt insoweit an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mit. MediCOM verpflichtet sich, über Geheimnisschutzdaten Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben unbedingt erforderlich ist.

1.4 MediCOM wird zur Verarbeitung personenbezogener Daten im Auftrag des Kunden nur solche Mitarbeiter einsetzen, die er vorab auf das Datengeheimnis sowie, falls einschlägig, auf die Vertraulichkeit der Kommunikation sowie das Fernmeldegeheimnis gem. § 3 des Telekommunikation-Telemedien-Datenschutz-Gesetzes („TTDSG") und/oder das Sozialgeheimnis gem. § 35 des ersten Buchs des Sozialgesetzbuchs („SGB I") verpflichtet hat. MediCOM hat die Mitarbeiter über einschlägige Strafbestimmungen, insbesondere § 203 StGB, belehrt und soweit erforderlich zur Geheimhaltung verpflichtet.

1.5 Zeugnisverweigerungsrecht der mitwirkenden Personen nach § 53a der Strafprozessordnung („StPO") und Beschlagnahmeverbot: Im Falle einer Befragung zu Geheimnisschutzdaten wird MediCOM unter Hinweis auf § 53a StPO unverzüglich den Kunden informieren und die Kunden-Daten nicht ohne das Einverständnis desselben (Berufsgeheimnisträger) an deutsche Strafverfolgungsbehörden herausgegeben. MediCOM ist bekannt, dass die sich in seinem Gewahrsam befindenden Geheimnisschutzdaten dem Beschlagnahmeverbot gemäß § 97 Abs. 2 StPO unterliegen. Im Falle einer Beschlagnahme durch deutsche oder ausländische Strafverfolgungsbehörden wird MediCOM unverzüglich den Kunden informieren.

§ 2 Definitionen und Festlegungen

2.1 Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung ergeben sich aus dem in der Präambel genannten Vertrag bzw. den genannten Verträgen. Soweit MediCOM personenbezogene Daten zur Erbringung der vom Kunden geschuldeten Leistungen verarbeitet, erfolgt dies im Auftrag und auf Weisung des Kunden. Für den Fall, dass der Kunden andere Fremdunternehmen mit der Arbeit an seinen Daten beauftragt, schließt der Kunden einen eigenen Vertrag mit diesen Unternehmen ab. Die vorliegende Vereinbarung bezieht sich ausschließlich auf Leistungen von MediCOM.

2.2 Soweit MediCOM Zugriff auf personenbezogene Daten hat, oder der Kunde auf anderen Wegen MediCOM zur Verfügung stellt und die MediCOM zur Erbringung der von MediCOM geschuldeten Leistungen verarbeitet oder nutzt (diese Daten werden im Folgenden die „Nutzerdaten" genannt), erfolgt dies im Auftrag und auf Weisung vom Kunden gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO).

2.3 Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44

ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

2.4 Die Kategorien betroffener Kundendaten und betroffener Personen sind in Anlage 1 genannt.

§ 3 Weisungsgebundenheit; Erhebung, Nutzung und Verarbeitung der Daten durch MediCOM

3.1 MediCOM wird die Kunden-Daten nur im Rahmen der dokumentierten Weisungen desselben erheben, nutzen oder sonst verarbeiten, sofern der Kunden nicht durch das Recht der Union oder der Mitgliedsstaaten, dem MediCOM unterliegt, zur Verarbeitung verpflichtet ist; in einem solchen Fall teilt die MediCOM dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Kunde wird mündliche Weisungen unverzüglich schriftlich bestätigen (E-Mail an info@medicom-weimar.de genügt). Der Kunden darf der MediCOM Weisungen im Rahmen der Auftragsverarbeitungen erteilen. Datenverarbeitungen außerhalb des Auftragsverhältnisses sind davon ausgenommen**.**

3.2 MediCOM wird die Kunden-Daten nur in dem Maße nutzen und sonst verarbeiten, wie es für die Erfüllung der von MediCOM nach dem in der Präambel genannten Vertrag bzw. den Verträgen geschuldeten Leistungen bzw. zur Erfüllung relevanter rechtlicher Verpflichtungen aus dem Recht der Union oder der Mitgliedsstaaten erforderlich ist. MediCOM darf die Verarbeitung im Auftrag auch im Wege von Home-Office und mobilem Arbeiten durch der MediCOM unterstellte Personen erbringen.

§ 4 Technische und organisatorische Maßnahmen

4.1 MediCOM wird alle technischen und organisatorischen Maßnahmen treffen, die erforderlich und geeignet sind, um die im Rahmen der Verarbeitung der Kunden-Daten anwendbaren Vorschriften der DSGVO zu erfüllen, insb. die in Art. 32 DSGVO genannten Anforderungen. MediCOM wird gemäß Art. 32 DSGVO erforderliche, geeignete technische und organisatorische Maßnahmen ergreifen, die unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Kunden-Daten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die verarbeiteten Daten zu gewährleisten. Die konkreten Maßnahmen ergeben sich aus dem Dokument „Technische und organisatorische Maßnahmen“, welches dieser Vereinbarung als Anlage 2 beigefügt ist. Dies gilt auch für Home-Office und bei mobilem Arbeiten**.**

4.2 MediCOM ist es gestattet, technische und organisatorische Maßnahmen während der Laufzeit des Vertrages zu ändern oder anzupassen, solange der sich aus den konkret vereinbarten Maßnahmen gemäß Anlage 2 ergebende Standard nicht unterschritten wird.

§ 5 Unterauftragsverarbeiter

5.1 MediCOM ist berechtigt, für die Verarbeitung von Kunden-Daten gemäß dieses Auftragsverarbeitungs-vertrages Unterauftragsverarbeiter einzusetzen. MediCOM wird dem Kunden immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Unterauftragsverarbeiter informieren, wodurch der Kunden die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Widerspricht der Kunden einer solchen Änderung aufgrund vernünftiger Einwände (zum Beispiel in Fällen, wenn ein Unterauftragsnehmer, der beauftragt werden soll, als unzuverlässig im Hinblick auf die Einhaltung gesetzlicher/vertraglicher Datenschutzpflichten bekannt ist oder ein Wettbewerber des Kunden ist), wird die MediCOM vernünftigerweise zu erwartenden Anstrengungen unternehmen, die Änderung zu vermeiden. Sollte sich die Änderung nicht vermeiden lassen, sind die Vertragspartner jeweils berechtigt den in der Präambel genannten Vertrag bzw. die Verträge und diesen Auftragsverarbeitungsvertrag zu kündigen, soweit die darunter erbrachten Dienste von der Änderung betroffen sind. Eine Liste der gegenwärtig beauftragten und vom Kunden mit Unterzeichnung genehmigten Unterauftragsverarbeiter ist diesem Auftragsverarbeitungsvertrag als Anlage 3 beigefügt.

5.2 Soweit MediCOM von der Berechtigung in § 5.1 Gebrauch macht, wird MediCOM dem Unterauftragsverarbeiter die Datenschutzpflichten auferlegen, welche für den Kunden in diesem Auftragsverarbeitungsvertrag festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt

werden, dass die Verarbeitung der Kunden-Daten durch den Unterauftragsverarbeiter entsprechend den Anforderungen der DSGVO erfolgt.

§ 6 Rechte der betroffenen Personen

6.1 MediCOM wird dem Kunden auf schriftliches Verlangen (E-Mail an info@medicom-weimar.de genügt) angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, der Pflicht Kunden zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person nachzukommen. Zusammen mit dem schriftlichen Verlangen wird der Kunden den Antrag an MediCOM übermitteln, unter Angabe der entsprechenden Gesetzesnorm mitteilen, um welches Recht bzw. welche Rechte der betroffenen Person es sich handelt und bestätigen, dass der Antrag berechtigt ist.

§ 7 Unterstützungspflichten des Kunden zu Art. 32-36 DSGVO

7.1 Der Kunde wird MediCOM unter Berücksichtigung der Art der Verarbeitung und dem Kunden zur Verfügung stehenden Informationen unterstützen bei der Einhaltung der in den Art. 32, 35, 36 DSGVO genannten Pflichten des Kunden (Sicherheit der Verarbeitung; ggf. Datenschutz-Folgenabschätzung auch ggf. mit vorheriger Konsultation der Datenschutzbehörde), soweit der Kunden gegenüber MediCOM nachweist, dass für den Kunden im konkreten Einzelfall, für den Kunden Unterstützung verlangt, in Bezug auf die von MediCOM geschuldeten Leistungen derartigen Pflichten bestehen. MediCOM wird den Kunden bei der Erfüllung von Melde- und Benachrichtigungspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen unterstützen, soweit den Kunden eine gesetzliche Melde- oder Benachrichtigungspflicht wegen einer Verletzung des Schutzes von Kunden-Daten nach Art. 33, 34 DSGVO trifft.

§ 8 Pflichten bei Vertragsbeendigung

4.1 Spätestens einen (1) Monat nach Beendigung des Vertrags wird MediCOM von dem Kunden übergebene Datenträger, die Kunden-Daten enthalten, an den Kunden zurückgeben und die bei MediCOM gespeicherten Kunden-Daten nach Wahl des Kunden entweder löschen oder zurückgeben. Dies gilt nicht, soweit MediCOM aufgrund Unionsrecht oder dem Recht der Mitgliedstaaten der EU zur Speicherung der personenbezogenen Daten verpflichtet ist. Im Falle einer solchen längeren gesetzlichen Aufbewahrungs- bzw. Speicherungspflicht wird MediCOM die betreffenden Datenträger zurückgeben und die Kunden-Daten löschen, sobald das Gesetz dies zulässt.

§ 9 Kontrollrechte

9.1 MediCOM stellt sicher, dass der Datenschutzbeauftragte des Kunden, und die für den Kunden im Bereich Datenschutzrecht zuständigen Aufsichtsbehörden ihre gesetzlichen Aufsichts- und Kontrollrechte wahrnehmen können.

9.2 Der Kunden hat das Recht, im Benehmen mit MediCOM Überprüfungen durchzuführen oder durch im Einzelfall zu benennenden Prüfer durchführen zu lassen:

Der Kunden hat das Recht, sich durch Kontrollen, die rechtzeitig, jedoch mindestens drei (3) Wochen vorher anzumelden sind, von der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten der MediCOM in dessen Geschäftsbetrieb im Rahmen der üblichen Geschäftszeiten (montags bis freitags von 10 bis 16 Uhr) ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen der MediCOM zu überzeugen.
In begründeten Fällen höchster Dringlichkeit ist auch eine unverzügliche Überprüfung möglich. Der Kunden darf im Regelfall eine solche Überprüfung einmal pro Kalenderjahr durchführen; weitere Überprüfungen erfolgen nur in begründeten Fällen und nach Abstimmung mit der MediCOM. MediCOM ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen Kunden, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte von MediCOM sind oder wenn der Kunden durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Kunde ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden von MediCOM, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten, die nicht unmittelbar relevant für die vereinbarten Überprüfungszwecke sind, zu erhalten.

Beauftragt der Kunde einen Dritten mit der Durchführung der Überprüfung, hat der Kunde den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen von MediCOM hat der Kunde ihm die Verschwiegenheitsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Kunde darf keinen Wettbewerber der MediCOM mit der Kontrolle beauftragen. Für die Ermöglichung von Kontrollen durch den Kunden kann die MediCOM einen - dem tatsächlichen Aufwand entsprechenden - Vergütungsanspruch geltend machen.

4.1 Die MediCOM wird dem Kunden auf dessen Anforderung alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO beschriebenen Pflichten zur Verfügung stellen, wenn der Kunde konkret unter Zitat der entsprechenden gesetzlichen Formulierung benennt, für welche Pflicht der MediCOM gem. Art 28 DSGVO der Kunde die Informationen benötigt wird.

§ 10 Hinweispflichten, Pflichten bei Vertragsbeendigung

10.1 MediCOM wird dem Kunden unverzüglich darauf hinweisen, wenn MediCOM der Ansicht ist, dass eine Weisung des Kunden gegen geltendes Datenschutzrecht verstößt. Ist MediCOM der Ansicht, dass eine Weisung des Kunden gegen diesen Auftragsverarbeitungsvertrag oder das geltende Datenschutzrecht verstößt, ist MediCOM nach einer entsprechenden Mitteilung an den Kunden berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Kunden auszusetzen.

10.2 Der Kunden hat MediCOM unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt. Die Information muss schriftlich an info@medicom-weimar.de erfolgen.

§ 11 Schlussbestimmungen

11.1 Änderungen dieses Auftragsverarbeitungsvertrages müssen schriftlich erfolgen, die elektronische Form ist hierfür ausreichend.

11.2 Sollten Bestimmungen dieses Auftragsverarbeitungsvertrages rechtsunwirksam sein oder werden, so bleiben die übrigen Bestimmungen hiervon unberührt. Die rechtsunwirksamen Bestimmungen sind von den Vertragspartnern unverzüglich durch solche Bestimmungen zu ersetzen, die dem wirtschaftlich gewollten Zweck der Vertragspartner entsprechen und dabei den Anforderungen des Art. 28 DSGVO genügen. Das gilt entsprechend für Lücken im Auftragsverarbeitungsvertrag.

11.3 Im Falle von Widersprüchen zwischen diesem Auftragsverarbeitungsvertrag und sonstigen Vereinbarungen zwischen den Vertragspartnern gehen die Regelungen dieses Auftragsverarbeitungsvertrages vor.

11.4 Es gilt deutsches Recht. Gerichtsstand ist der Sitz des Auftragnehmers.

Ort, Datum	Unterschrift Auftraggeber Stempel Auftraggeber
	Vor- und Nachname in Druckbuchstaben
Ort, Datum	Unterschrift Auftragnehmer Geschäftsführung MediCOM

Anlage 1 Kategorien betroffener Personen und Kunden-Daten

MediCOM erhält Zugriff auf die nachfolgend genannten Kunden-Daten:

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DSGVO):

- Patienten des Kunden
- Mitarbeiter des Kunden
- Dienstleister des Kunden

Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1 DSGVO), die der Kunden im Rahmen der Auftragsverarbeitung offenbart:

- Identifikationsdaten (Name, Vorname)
- Kommunikations- und Adressdaten (Anschrift, Telefon, Fax, E-Mail-Adresse usw.)
- Sozialversicherungsrelevante Daten (Familienstand, Steuerklasse, Krankenkasse usw.)
- Gesundheitsdaten (Daten nach Art. 9 DSGVO), die der Kunden in den jeweiligen eingesetzten Praxissoftwarelösungen und deren Zusatzprodukten verarbeitet
- Allgemeine Personendaten (Beruf, Arbeitgeberdaten usw.)
- Kennnummern (Kundennummer, Nummer bei den Krankenkassen, sonstige Versicherungs-nummer, Arztnummer)
- Bankdaten
- Administrative Daten (Betriebsstätten bezogene Daten)
- IT-Nutzungsdaten (Protokolldaten, Hard- und Softwareinformationen usw.)

Anlage 2 Technische und organisatorische Maßnahmen

Generelle Beschreibung

- Vorhandensein von internem IT-Sicherheitskonzept und IT-Sicherheitsrichtlinien.
- Datenverarbeitung ist in Arbeits- und Prozessbeschreibungen schriftlich geregelt.
- Fremdfirmen haben keinen Zugriff auf Datenverarbeitung.
- Vertretungsregelung für IT-Verantwortlichen bei Urlaub oder Krankheit.
- Schriftliche Bestellung eines Datenschutzbeauftragten.
- Verpflichtung aller Mitarbeiter nachweislich auf das Datengeheimnis sowie ggf. § 88 TKG, § 35 SGB I, KDG und DSG-EKD; Belehrung über den § 203 StGB.
- Regelmäßige Kontrolle bzgl. Einhaltung von Datenschutz- und Datensicherheitsmaßnahmen.
- Vorhandensein von Verzeichnissen von Verarbeitungstätigkeiten gem. Art. 30 Abs. 2 DSGVO, soweit eine Verpflichtung gem. Art. 30 Abs. 5 DSGVO besteht.
- Namentliche Nennung der Ansprechpartner (IT/DV-Verantwortlicher und externer Datenschutzbeauftragter) zur Klärung fachlicher, technischer und organisatorischer Fragen.
- Pseudonymisierung der Daten, soweit dies unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen in Anbetracht der Verarbeitungszwecke möglich ist.
- Verschlüsselung der Daten, soweit dies unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen in Anbetracht der Verarbeitungszwecke möglich ist.

In den folgenden Abschnitten sind einige technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO konkret beschrieben:

Zugangskontrolle

Die Zugangskontrolle umfasst Maßnahmen, die geeignet sind, Unbefugten den Zutritt (physikalische Sicherheit) zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Maßnahmen von MediCOM im Einzelnen:

- Aufgrund der Lage der Geschäftsräume sind Einwirkversuche von außen über die Fenster ausreichend verhindert. Die Geschäftsräume sind nur durch Personal mit entsprechenden Transpondern oder Schlüsseln zu betreten.
- Ausgabe und Rückgabe von Transpondern und Schlüsseln ist geregelt, mit Schlüsselbuch bzw. durch Systemdokumentation.
- Betriebsfremde Besucher haben keinen Zutritt zu den Büroräumen
- MediCOM verpflichtet auch Auftragnehmer, die keinen Kontakt zur Datenverarbeitung haben (beispielsweise den Gebäudereiniger), die eigenen Mitarbeiter über den Datenschutz aufzuklären und diese aufzufordern, sich vorsichtig zu verhalten, insbesondere Schlüssel sorgfältig zu verwahren.
- Der gesamte Bereich der Büroräume ist alarmgesichert.

Datenträgerkontrolle

Die Datenträgerkontrolle umfasst Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen (logische Sicherheit) durch Unbefugte verhindert wird.

Maßnahmen von MediCOM im Einzelnen:

- Externer Zugriff von MediCOM-Mitarbeitern auf MediCOM-Server ist nur via VPN und Authentifizierung am MediCOM-LAN möglich.
- Trennung WLAN vom Firmennetzwerk.
- Anti-Viren-Software auf allen eingesetzten IT/DV-Anlagen.
- Akten unter Verschluss. Zugang nur für berechtigte Personen.
- Der Zugang zu den IT-Systemen ist durch Zugangsberechtigungen geregelt. Eine Firewall verhindert ungewollte Zugriffe von außen.
- Werden Passwörter mehrfach fehlerhaft eingegeben, erfolgt eine Sperrung. Diese kann nur durch einen Administrator rückgängig gemacht werden.
- Die Mitarbeiter sind gehalten, Notebooks vor unberechtigtem Zugriff zu schützen und so wenig Daten wie möglich aus dem Bereich des Auftraggebers auf dem Notebook zu speichern (sondern möglichst nur innerhalb der zentralen Server von MediCOM).
- Wenn ein Mitarbeiter ausscheidet, gibt er die ihm zur Verfügung gestellten Geräte an die MediCOM zurück.

Speicherkontrolle

Die Speicherkontrolle umfasst Maßnahmen, mit denen die unbefugte Eingabe von personenbezogenen Daten sowie die unbefugte Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten verhindert wird.

Maßnahmen von MediCOM im Einzelnen:

- Zugriffe auf den Server von MediCOM erfolgen durch Authentifizierung (Benutzername/Passwort) mit entsprechenden Zugriffsberechtigungen.
- Über Zugriffsberechtigungen wird außerdem sichergestellt, dass die Mitarbeiter nur auf die Datenbanken, Anwendungen und Daten zugreifen können, die sie für ihre Aufgabenerfüllung benötigen.
- Bei Zugriff auf Daten beim Auftraggeber ist durch die von MediCOM eingesetzten Fernwartungssoftware sichergestellt, dass berechtigte Mitarbeiter von MediCOM ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass alle Zugriffe in der Kundendokumentation festgehalten werden.
- Wenn ein Mitarbeiter ausscheidet, werden ihm die Zugriffsrechte entzogen.
- Die Datenfernübertragungssysteme von MediCOM sind mit Datenverschlüsselung versehen und werden auf dem jeweils aktuellen technischen Stand gehalten.
- Aufgrund der aufgeführten Maßnahmen sollte der Zugriff Unbefugter verhindert werden, z.B. Daten aus dem Auftraggeberbereich zu lesen, zu kopieren, zu ändern oder zu entfernen.
- Wenn MediCOM die Daten aus dem Auftraggeberbereich nicht mehr benötigt, werden die Datenträger nach DIN-Norm 66399 und gemäß den Bestimmungen des Datenschutzes vernichtet. Eventuell angefertigte Kopien der Daten, die zum Zweck der Aufgabenerfüllung erstellt wurden, werden gelöscht. s. im Übrigen Datenträgerkontrolle und Zugriffskontrolle.
- siehe im Übrigen Datenträgerkontrolle und Zugriffskontrolle.

Benutzerkontrolle

Die Benutzerkontrolle umfasst Maßnahmen, mit denen die Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte verhindert wird.

Maßnahmen von MediCOM im Einzelnen:

- siehe Datenträgerkontrolle und Zugriffskontrolle.

Zugriffskontrolle

Die Zugriffskontrolle umfasst Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

Maßnahmen von MediCOM im Einzelnen:

- Vorhandensein eines Berechtigungskonzepts.
- Datenträgerverwaltung, Datensicherung, Aufbewahrung außerhalb des Gebäudes, Verschlüsselung.
- Zugriff zu den Festplatten mit Datensicherung nur für bestimmte Personen.
- Dokumentation von Datenträgerwechseln und Aufbewahrungsorten.
- Verbot der Nutzung privater Datenträger.
- Zugriff auf Notebooks, PC und Server von MediCOM nur mit Username und Passwort möglich.
- Passwörter unterliegen definierten Passwortrichtlinien (hohen Anforderungen).
- Administratoren sind für Vergabe und regelmäßige Änderung von Passwörtern verantwortlich.
- Betrieb von Arbeitsplatz-PC und Servern nur nach Anmeldung mit Benutzername und Passwort.
- Automatische Bildschirmsperre mit Passwort-Aktivierung.
- Sperrung nach mehrmaligen fehlerhaften Anmeldeversuchen.
- Löschung und Zwischenlagerung defekter Datenträger bis zur datenschutzkonformen Vernichtung.
- Vernichtung ausgedruckter Daten im Aktenvernichter bzw. durch zugelassene Fachunternehmen.
- Umgang mit Datenträgern sowie Verwendung von USB-Sticks, PDAs, externen Festplatten, Tablets und Smartphones und anderer externer Geräte durch Arbeitsanweisung schriftlich geregelt.

Übertragungskontrolle

Die Übertragungskontrolle umfasst Maßnahmen, die gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

Maßnahmen von MediCOM im Einzelnen:

- Regelungen zur Datenübertragung sind vorhanden.
- Übermittlung und Zur-Verfügung-Stellen von Daten wird protokolliert.
- Die MediCOM bearbeitet die Daten nur im Rahmen der Weisungen des Auftraggebers.
- Die Speicherung von Daten aus dem Auftraggeberbereich erfolgt nur während der Arbeiten zur Mängelbeseitigung oder zur Unterstützung des Einsatzes der von MediCOM gelieferten Systeme bzw. von Systemen, für die MediCOM Serviceleistungen erbringt. Daten aus dem Bereich des Auftraggebers werden an einen Dritten nur weitergegeben, sofern der Auftraggeber das im Einzelfall schriftlich wünscht.
- Der Auftraggeber kann MediCOM die Daten entweder verschlüsselt über eine gesicherte Fernwartungsverbindung auf einen Server von MediCOM übertragen oder als Datenbank auf einem Datenträger zur Verfügung stellen.

Eingabekontrolle

Die Eingabekontrolle umfasst Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder aus diesen entfernt worden sind.

Maßnahmen von MediCOM im Einzelnen:

- Regelungen zur Dateneingabe sind vorhanden.
- Erstellung und Änderung von Daten wird protokolliert.
- Werden personenbezogene Daten aus dem Bereich des Auftraggebers zum Zwecke der Fehlersuche an MediCOM übertragen, werden diese Daten nach Beendigung der Fehlersuche gelöscht. Eine Veränderung oder Entfernung im Sinne des Datenschutzrechts findet nicht statt, es sei denn, dass der Auftraggeber dies vorher ausdrücklich schriftlich beauftragt hat.

Transportkontrolle

Die Transportkontrolle umfasst Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Maßnahmen von MediCOM im Einzelnen:

- Firewall.
- Versendung personenbezogener Daten mit verschlüsselter elektronischer Verbindung.
- Statistiken mit personenbezogenen Inhalten werden nur im AuftrKunde von AuftrKundegeber und nur an berechtigte Personen bei Auftraggeber übermittelt.

Wiederherstellbarkeit

Die Wiederherstellbarkeit umfasst Maßnahmen, die gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Maßnahmen von MediCOM im Einzelnen:

- Zugriff zu den Festplatten mit Datensicherung nur für bestimmte Personen.
- Datenträgerverwaltung, Datensicherung, Aufbewahrung gesichert.
- Dokumentation von Datenträgerwechseln und Aufbewahrungsorten.

Zuverlässigkeit

Die Zuverlässigkeit umfasst Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

Maßnahmen von MediCOM im Einzelnen:

- siehe Verfügbarkeitskontrolle.

Datenintegrität

Die Datenintegrität umfasst Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

Maßnahmen von MediCOM im Einzelnen:

- siehe Verfügbarkeitskontrolle.

Auftragskontrolle

Die Datenintegrität umfasst Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

Maßnahmen von MediCOM im Einzelnen:

- Alle MediCOM-Mitarbeiter sind angewiesen, nur nach den vereinbarten Vertragsinhalten zu arbeiten.
- Alle vom Auftraggeber bereit gestellten Daten verbleiben ausschließlich in der Verfügungsmacht von MediCOM.
- Weitergabe personenbezogener Daten erfolgt nur nach schriftlicher Einwilligung vom Auftraggeber.
- Dienstleister von MediCOM unterliegen Überprüfungen (Lieferantenaudits).
- Die MediCOM führt Arbeiten, bei denen sie Kontakt zu personenbezogenen Daten aus dem Bereich des Auftraggebers bekommen kann oder bekommen soll, nur durch, wenn dieser diese im Einzelfall anfordert. Dies ist beispielsweise dann der Fall, wenn der Auftraggeber an die MediCOM einen Fehler oder ein Problem meldet. Die Mitarbeiter von MediCOM sind angewiesen, solche Maßnahmen vorsorglich mit dem Auftraggeber abzustimmen.
- Alle Mitarbeiter von MediCOM, die mit personenbezogenen Daten aus dem Bereich des Auftraggebers in Kontakt kommen können, sind schriftlich auf die Einhaltung des Datenschutzes verpflichtet. Sie sind entsprechend belehrt und angewiesen, dass sie Arbeiten gemäß dem vorstehenden Absatz nur auf Anforderung des Auftraggebers durchführen dürfen.

Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle umfasst Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Maßnahmen von MediCOM im Einzelnen:

- Tägliche Datensicherung.
- Feuerlöscher in ausreichender Anzahl im Gebäude.
- Vorgaben des Brandschutzes werden eingehalten und regelmäßig durch externe Prüfungen verifiziert.
- Rauchverbot
- Serverraum mit unterbrechungsfreier Stromversorgung, Überspannungsschutz.
- Back-Up-Verfahren für Server und Arbeitsplatz-PCs.
- Alle betroffenen Server sowie NAS verfügen über RAID-Systeme, welche das Verlustrisiko minimieren.
- Von einem Auftraggeber übergebene Datenträger werden unter Verschluss verwahrt.
- Sicherungskopien außerhalb des Gebäudes.
- Virenschutzprogramme auf allen Computersystemen.
- Intrusion Detection System.
- MediCOM setzt eine Firewall und aktuelle Virenscanner zur Absicherung sowohl des zentralen Datenbankservers als auch des E-Mail-Servers ein. Die Virensignaturen des verwendeten Virenscanners werden täglich mehrmals aktualisiert.
- Arbeitsplatzrechner werden laufend durch aktuelle Scanner Programme auf schadhafte Software überprüft. E-Mail-Anhänge werden auf Infizierung überwacht.
- Die Mitarbeiter sind verpflichtet, personenbezogene Daten, die sie auf ihren Notebooks gespeichert haben, möglichst bald auf ein zentrales System von MediCOM zu überspielen und vom Notebook zu löschen.
- Schriftlicher Notfallplan.

Trennbarkeit

Das Trennungsgebot umfasst Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Maßnahmen von MediCOM im Einzelnen:

- Wenn Daten aus dem Bereich des Auftraggebers zum Zwecke der Fehlersuche oder deren Wiederherstellung übertragen werden, werden diese gesondert von Daten anderer Auftraggeber gespeichert.

Anlage 3 Unterauftragnehmer

Allgemein

medatixx GmbH & Co. KG	Im Kappelhof 1, 65343 Eltville/Rhein
Unterstützung im Secondlevelsupport	
I-Motion GmbH	Nordring 23, 90765 Fürth
Kommunikationsdienstleister	
mediDOK Software Entwicklungsgesellschaft mbH	Handschuhsheimer Landstr. 1, 69221 Dossenheim
Unterstützung im Secondlevelsupport	
AMEDTEC Medizintechnik Aue GmbH	Schneeberger Straße 5, 08280 Aue
Unterstützung im Secondlevelsupport	