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

zwischen dem Auftraggeber:

⌜ ⌝

⌞ ⌟

(nachstehend „**AG**“ genannt)

und

medatixx GmbH & Co. KG
Im Kappelhof 1
65343 Eltville/Rhein

(nachstehend „**AN**“ genannt)

(nachstehend werden AG und AN auch gemeinsam „**Vertragspartner**“ genannt)

Präambel

Der AG hat den AN vertraglich zur Erbringung definierter Leistungen (lt. Softwarepflegevertrag) beauftragt. Darüber liegen gesonderte Leistungsverträge vor. Im Rahmen der Leistungserbringung kann der AN ggf. Zugriff auf von dem AG gespeicherte oder von dem AG anders gegenüber dem AN zur Verfügung gestellte personenbezogene Daten erhalten. Soweit der AN solche personenbezogenen Daten im Auftrag des AG verarbeitet, handelt es sich um Auftragsverarbeitung im Sinne von Art. 28 der Datenschutz-Grundverordnung („**DSGVO**"). Der AN ist in dieser Konstellation Auftragsverarbeiter und der AG datenschutzrechtlicher Verantwortlicher. Diese im Auftrag des AG verarbeiteten personenbezogenen Daten werden im Folgenden auch als „**AG-Daten**" bezeichnet. Zur Regelung der Verarbeitung personenbezogener Daten durch den AN im Auftrag des AG treffen die Vertragspartner diese Vereinbarung zum Datenschutz und zur Datensicherheit in Auftragsverhältnissen gem. Art. 28 DSGVO („**Auftragsverarbeitungsvertrag**"). Die Anlagen 1, 2 und 3a sind Teil des Vertrages.

§ 1 Datenschutz, Vertraulichkeit

1.1 Der AN beachtet das jeweils geltende Datenschutzrecht und trifft alle notwendigen organisatorischen Maßnahmen, um die Einhaltung des Datenschutzrechts bei der Verarbeitung der AG-Daten im Auftrag des AG zu gewährleisten.

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

1.3 Der AN verarbeitet im Auftrag des AG 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. Der AN 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 Der AN wird zur Verarbeitung personenbezogener Daten im Auftrag des AG 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-Digitale-Dienste-Datenschutz-Gesetz („**TDDDG**") und/oder das Sozialgeheimnis gem. § 35 des ersten Buchs des Sozialgesetzbuchs („**SGB I**") verpflichtet hat. Der AN 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 der AN unter Hinweis auf § 53a StPO unverzüglich den AG informieren und die AG-Daten nicht ohne das Einverständnis des AG (Berufsgeheimnisträger) an deutsche Strafverfolgungsbehörden herausgegeben. Dem AN 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 der AN unverzüglich den AG informieren.

1.6 Der AN wird anwendbare Regelungen aus dem evangelischen und katholischen Kirchendatenschutzgesetz („**KDG**") umsetzen.

§ 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 der AN personenbezogene Daten zur Erbringung der von AN geschuldeten Leistungen verarbeitet, erfolgt dies im Auftrag und auf Weisung des AG. Für den Fall, dass der AG zur Betreuung seiner Praxissoftwarelösung regionale Servicepartner des AN oder andere Fremdunternehmen mit der Arbeit an seinen Daten beauftragt, schließt der AG einen eigenen Vertrag mit diesen Unternehmen ab. Die vorliegende Vereinbarung bezieht sich ausschließlich auf Leistungen des AN.

2.2 Die Kategorien betroffener AG-Daten und Kategorien betroffener Personen sind in Anlage 1 genannt.

2.3 Die vertraglich geschuldeten Leistungen werden ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Leistungen oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des AG und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, EU-Standardvertragsklauseln (SCC), genehmigte Verhaltensregeln).

§ 3 Weisungsgebundenheit, Verarbeitung der AG-Daten durch den AN

3.1 Der AN wird die AG-Daten nur im Rahmen der dokumentierten Weisungen des AG erheben, nutzen oder sonst verarbeiten (auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation), sofern der AN nicht durch das Recht der Union oder der Mitgliedsstaaten, dem der AN unterliegt, zur Verarbeitung verpflichtet ist; in einem solchen Fall teilt der AN dem AG diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der AG wird mündliche Weisungen unverzüglich schriftlich bestätigen (E-Mail an datenschutz@medatixx.de genügt). Der AG darf dem AN Weisungen im Rahmen der Auftragsverarbeitungen erteilen. Datenverarbeitungen außerhalb des Auftragsverhältnisses sind davon ausgenommen.

3.2 Der AN wird die AG-Daten nur in dem Maße nutzen und sonst verarbeiten, wie es für die Erfüllung der von dem AN 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. Der AN darf die Verarbeitung im Auftrag auch im Wege von Home-Office und mobilem Arbeiten durch dem AN unterstellte Personen erbringen.

§ 4 Technische und organisatorische Maßnahmen

4.1 Der AN wird alle technischen und organisatorischen Maßnahmen treffen, die erforderlich und geeignet sind, um die im Rahmen der Verarbeitung der AG-Daten anwendbaren Vorschriften der DSGVO zu erfüllen, insb. die in Art. 32 DSGVO genannten Anforderungen. Der AN 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 AG-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 Dem AN 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. Der AN wird die konkreten

Maßnahmen, welche sich aus Anlage 2 dieser Vereinbarung ergeben, anpassen, soweit dies erforderlich ist, um den in Art. 32 DSGVO genannten Anforderungen zu genügen.

§ 5 Unterauftragsverarbeiter

5.1 Der AN ist berechtigt, für die Verarbeitung von AG-Daten gemäß dieses Auftragsverarbeitungsvertrages Unterauftragsverarbeiter einzusetzen. Der AN wird dem AG immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Unterauftragsverarbeiter informieren, wodurch der AG die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Widerspricht der AG 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 AG ist), wird der AN vernünftigerweise zu erwartende 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 von dem AG mit Unterzeichnung genehmigten Unterauftragsverarbeiter ist diesem Auftragsverarbeitungsvertrag als Anlage 3a und in der Zusatzvereinbarung für Klinikkunden beigefügt.

5.2 Soweit der AN von der Berechtigung in § 5.1 Gebrauch macht, wird der AN dem Unterauftragsverarbeiter die Datenschutzpflichten auferlegen, welche für den AN 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 AG-Daten durch den Unterauftragsverarbeiter entsprechend den Anforderungen der DSGVO erfolgt. Der AN schließt hierüber einen schriftlichen Vertrag mit dem Unterauftragsverarbeiter.

§ 6 Rechte der betroffenen Personen

Der AN wird dem AG auf schriftliches Verlangen (E-Mail an datenschutz@medatixx.de genügt) angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, der Pflicht des AG 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 AG den Antrag an den AN 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 AN zu Art. 32 bis 36 DSGVO

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

§ 8 Pflichten bei Vertragsbeendigung

Nach Abschluss der Erbringung der Verarbeitungsleistungen durch AN nach Maßgabe dieses Auftragsverarbeitungsvertrags, spätestens einen (1) Monat nach Beendigung des Vertrags, wird der AN von dem AG übergebene Datenträger, die AG-Daten enthalten, an den AG zurückgeben und die beim AN gespeicherten AG-Daten nach Wahl des AG entweder löschen oder zurückgeben. Dies gilt nicht, soweit der AN 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 der AN die betreffenden Datenträger zurückgeben und die AG-Daten löschen, sobald das Gesetz dies zulässt.

§ 9 Kontrollrechte

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

9.2 Der AG hat das Recht, im Benehmen mit dem AN Überprüfungen durchzuführen oder durch einen zu benennenden Prüfer durchführen zu lassen:

- Der AG 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 des AN in dessen Geschäftsbetrieb im Rahmen der üblichen Geschäftszeiten (montags bis freitags von 10 bis 18 Uhr) ohne übermäßige Beeinträchtigung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des AG zu überzeugen. In begründeten Fällen höchster Dringlichkeit ist auch eine unverzügliche Überprüfung möglich, in Fällen, in welchen eine Voranmeldung den Zweck der Überprüfung gefährden würde, ist eine solche entbehrlich.

- Der AG darf im Regelfall eine solche Überprüfung einmal pro Kalenderjahr durchführen; weitere Überprüfungen erfolgen nur in begründeten Fällen und nach Abstimmung mit dem AN, es sei denn, eine solche Abstimmung würde den Zweck der Überprüfung gefährden.

- Der AN ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des AG, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des AN sind oder wenn der AN durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der AG ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des AN, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des AN, die nicht unmittelbar relevant für die vereinbarten Überprüfungszwecke sind, zu erhalten.

- Beauftragt der AG einen Dritten mit der Durchführung der Überprüfung, hat der AG den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des AN hat der AG ihm die Verschwiegenheitsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der AG darf keinen unmittelbaren Wettbewerber des AN mit der Kontrolle beauftragen.

- Der AN wird im erforderlichen Umfang zur Überprüfung durch den AG nach Maßgabe dieses § 9.1 beitragen.

- Für die Ermöglichung von und den Beitrag zu Kontrollen durch den AG kann der AN einen - dem tatsächlichen Aufwand entsprechenden - Vergütungsanspruch geltend machen, es sei denn die Kontrolle(n) wurde(n) wegen eines Gesetzes- oder Vertragsverstoß durch den AN erforderlich.

9.3 Der AN wird dem AG auf Anforderung des AG alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO beschriebenen Pflichten des AN zur Verfügung stellen, wenn der AG konkret unter Zitat der entsprechenden gesetzlichen Formulierung benennt, für welche Pflicht des AN gem. Art 28 DSGVO der AG die Informationen benötigt.

§ 10 Hinweispflichten, Pflichten bei Vertragsbeendigung

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

10.2 Die Kontaktdaten des aktuell bestellten Datenschutzbeauftragten teilt der AN unter https://medatixx.de/datenschutz mit.

10.3 Der AG hat den AN unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt. Die Information muss schriftlich an datenschutz@medatixx.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 medatixx GmbH & Co. KG

Anlage 1 Kategorien betroffener Personen und AG-Daten

Der AN erhält Zugriff auf die nachfolgend genannten AG-Daten:

- Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DSGVO):
  - Patienten des AG
  - Mitarbeiter des AG
  - Dienstleister des AG

- Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1 DSGVO), die der AG 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 AG in den jeweiligen eingesetzten Praxissoftwarelösungen und deren Zusatzprodukten verarbeitet
  - Allgemeine Personendaten (Beruf, Arbeitgeberdaten usw.)
  - Kennnummern (Kundennummer, Nummer bei den Krankenkassen, sonstige Versicherungsnummer, Arztnummer)
  - Bankdaten
  - Administrative Daten (Betriebsstättenbezogene 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 auf das Datengeheimnis, sowie ggf. § 3 TDDDG, § 35 SGB I und zum § 203 StGB und entsprechende Verpflichtung zur Geheimhaltung. Soweit erforderlich gilt das auch für das evangelische und katholische Kirchendatenschutzgesetz („**KDG**“).
- 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.
- Housing eigener Hardware in den Rechenzentren noris network AG, Equinix und ecotel communication ag.
- 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.
- Die internen Systeme, sowie die angebotenen Praxissoftwarelösungen werden regelmäßig durch externe Anbieter Penetrationstests unterzogen und dadurch gehärtet.

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

1. 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 des AN 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.
- Zusätzlich werden außerhalb der Bürozeiten einbruch- und feuerhemmende Sicherheitstüren verschlossen.
- Ausgabe und Rückgabe von Transpondern und Schlüsseln ist geregelt, mit Systemdokumentation.

- Betriebsfremde Besucher werden am Empfang begrüßt, stets von Mitarbeitern des AN im Büro begleitet und können sich nicht unkontrolliert im Bürobereich aufhalten.
- Der AN 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 Zutritt zu den Serverräumen ist durch eine separate digitale Schließanlage abgesichert. Die Zutrittserlaubnis ist auf das unbedingt notwendige Personal (Systemadministratoren) beschränkt. Personen, die nicht für die Wartung und den Betrieb der Server zuständig sind, erhalten keinen Zutritt zu den Serverräumen.

2. Datenträgerkontrolle

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

Maßnahmen des AN im Einzelnen:

- Externer Zugriff von AN-Mitarbeitern auf AN-Server ist nur via VPN und Zwei-Faktor-Authentifizierung am AN-LAN möglich.
- Trennung Gast-WLAN vom Firmennetzwerk.
- AN-WLAN wird mit WPA2 betrieben.
- 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 AG auf dem Notebook zu speichern (sondern möglichst nur innerhalb der zentralen Server des AN).
- Wenn ein Mitarbeiter ausscheidet, gibt er die ihm zur Verfügung gestellten Geräte an den AN zurück.

3. 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 des AN im Einzelnen:

- Zugriffe auf die Server des AN 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 AG ist durch die von AN eingesetzten Fernwartungssoftware sichergestellt, dass berechtigte Mitarbeiter des AN 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 des AN sind mit Datenverschlüsselung versehen und werden auf dem jeweils aktuellen technischen Stand gehalten.
- Aufgrund der aufgeführten Maßnahmen ist es Unbefugten nicht möglich, Daten aus dem Bereich des AG zu lesen, zu kopieren, zu ändern oder zu entfernen.
- Wenn der AN die Daten aus dem Bereich des AG 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. Siehe im Übrigen Datenträgerkontrolle und Zugriffskontrolle.

4. Benutzerkontrolle

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

Maßnahmen des AN im Einzelnen:

- Siehe Datenträgerkontrolle und Zugriffskontrolle.

5. Zugriffskontrolle

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

Maßnahmen des AN 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 des AN 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.
- Zugangsprotokollierung.
- Sperrung nach mehrmaligen fehlerhaften Anmeldeversuchen.
- Löschung und Zwischenlagerung defekter Datenträger bis zur datenschutzkonformen Vernichtung.
- Ausgedruckte Daten werden von einem Entsorgungsbetrieb datenschutzkonform vernichtet, dazu hält der AN verschlossene Datenentsorgungsbehälter des jeweiligen Anbieters vor.

- Umgang mit Datenträgern sowie Verwendung von USB-Sticks, externen Festplatten, Tablets und Smartphones und anderer externer Geräte durch Arbeitsanweisung schriftlich geregelt.

6. Übertragungskontrolle

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

Maßnahmen des AN im Einzelnen:

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

7. 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 des AN im Einzelnen:

- Regelungen zur Dateneingabe sind vorhanden.
- Erstellung und Änderung von Daten wird protokolliert.
- Es ist nicht vorgesehen, dass der AN personenbezogene Daten aus dem Bereich des AG in die Software eingibt.
- Werden personenbezogene Daten aus dem Bereich des AG zum Zwecke der Fehlersuche an den AN 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 AG dies vorher ausdrücklich schriftlich beauftragt hat.
- Nur auf Anweisung des AG werden Mitarbeiter des AN, Daten in den operativen Systemen des AG eingeben, ändern oder entfernen.

8. 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 des AN im Einzelnen:

- Firewall.
- Versendung personenbezogener Daten mit verschlüsselter elektronischer Verbindung.
- Statistiken mit personenbezogenen Inhalten werden nur im Auftrag des AG und nur an berechtigte Personen beim AG übermittelt.

9. Wiederherstellbarkeit

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

Maßnahmen des AN im Einzelnen:

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

10. Zuverlässigkeit

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

Maßnahmen des AN im Einzelnen:

- Siehe Verfügbarkeitskontrolle.

11. Datenintegrität

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

Maßnahmen des AN im Einzelnen:

- Siehe Verfügbarkeitskontrolle.

12. Auftragskontrolle

Die Auftragskontrolle umfasst Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen verarbeitet werden können.

Maßnahmen des AN im Einzelnen:

- Alle AN-Mitarbeiter sind angewiesen, nur nach den vereinbarten Vertragsinhalten zu arbeiten.
- Alle vom AG bereitgestellten Daten verbleiben ausschließlich in der Verfügungsmacht des AN.
- Weitergabe personenbezogener Daten erfolgt nur nach schriftlicher Einwilligung des AG bzw. soweit der AN durch das Recht der Union oder der Mitgliedsstaaten, dem der AN unterliegt, dazu verpflichtet ist.

- Dienstleister des AN unterliegen Überprüfungen (Lieferantenaudits).
- Der AN führt Arbeiten, bei denen er Kontakt zu personenbezogenen Daten aus dem Bereich des AG bekommen kann oder bekommen soll, nur durch, wenn dieser diese im Einzelfall anfordert. Dies ist beispielsweise dann der Fall, wenn der AG an den AN einen Fehler oder ein Problem meldet. Die Mitarbeiter des AN sind angewiesen, solche Maßnahmen vorsorglich mit dem AG abzustimmen.
- Alle Mitarbeiter des AN, die mit personenbezogenen Daten aus dem Bereich des AG 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 AG durchführen dürfen.

13. Verfügbarkeitskontrolle

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

Maßnahmen des AN im Einzelnen:

- Tägliche Datensicherung.
- Feuerlöscher in ausreichender Anzahl im Gebäude.
- Brandschutztüren.
- Vorgaben des Brandschutzes werden eingehalten und regelmäßig durch externe Prüfungen verifiziert.
- Rauchverbot im Serverraum.
- Serverraum mit unterbrechungsfreier Stromversorgung, Überspannungsschutz.
- Back-Up-Verfahren für Server und Arbeitsplatz-PCs.
- Alle betroffenen Server verfügen über RAID-Systeme, welche das Verlustrisiko minimieren.
- Von dem AG übergebene Datenträger werden unter Verschluss verwahrt.
- Sicherungskopien außerhalb des Gebäudes.
- Gespiegelte Server-Festplatten.
- Virenschutzprogramme auf allen Computersystemen.
- Intrusion Detection System.
- Der AN 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 Scannerprogramme auf Schadsoftware, Malware 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 des AN zu überspielen.
- Schriftlicher Notfallplan.
- MS Enterprise E5 Lizenzen (ATP, Appblocker).
- MS Exchange (Sandboxverfahren für Mail-Anhänge, Safelink, Attachment scanning).
- Active Directory nach dem Microsoft Tier Administrative Model (https://docs.microsoft.com/de-de/security/compass/privileged-access-access-model).
- Least privilege Prinzip.
- Stringente Netzwerksegmentierung im Client und Serverbereich durch Firewalls mit IPS/IDS
- Nutzung von Privileged Access Workstations für Administrationstätigkeiten.
- Umfassende Systemprotokollierung.

- Stringente Rechteeinschränkung der Benutzer
  - Keine lokalen Adminrechte
  - Installation und Ausführung nur von zugelassenen Programmen und Apps
  - Zugriff nur über zugelassene Geräte – Devicemanagement über Microsoft (Endpoint-Manager)
  - Die VPN-Verbindung ist per Zwei-Faktor-Authentifizierung abgesichert - Benutzer; Passwort und FortiToken per Hardware oder App.

14. Trennbarkeit

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

Maßnahmen des AN im Einzelnen:

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

Anlage 3a Unterauftragnehmer

Allgemein

DRACOON GmbH	**Galgenbergstraße 2a, 935053 Regensburg**
Datentransfer von und zur medatixx	
I-Motion GmbH Gesellschaft für Kommunikation und Service	**Nordring 23, 90765 Fürth**
Kommunikationsdienstleister	
Microsoft Deutschland GmbH	**Walter Gropius Straße 5, 80807 München**
M365	
Stiftung Gesundheit	**Behringstraße 28a, 22765 Hamburg**
Datenschnittstelle	

Ggf. zusätzlich für Kunden der nachstehend aufgeführten Produkte und Dienstleistungen

AG Data GmbH	**Braunstraße 14, 04347 Leipzig**	Alle
Konvertierungen		
Amedtec Medizintechnik Aue GmbH	**Schneebergerstraße 5, 08280 Aue**	Alle
Wartung und Service für Hard- und Software für Medizingeräte		
Amian & Witzel GmbH	**Krefelder Straße 225, 52070 Aachen**	Kunden der NL West
Technische Installationen		
bytesatwork GmbH	**Bellenbruchstraße 6, 32683 Barntrup**	Kunden der Niederlassungen
Manage4All		
Dr. Hans-Jochen Müller	**Auf den Ebenbergen 5, 01445 Radebeul**	x.concept, x.concept Edition Ambulanz
Entwicklung und Pflege von Software und Datenbanken		
edudip GmbH	**Jülicher Strasse 306, 52070 Aachen**	Kunden der medatixx akademie
Webinar-Software		
ELOVADE Deutschland GmbH	**Garbenheimer Str. 36, 35578 Wetzlar**	Kunden der Niederlassungen
Cloud-Backup		
foxpert GmbH	**Badstraße 5, 92318 Neumarkt i. d. Opf.**	x.concept, x.comfort
Entwicklung, Pflege von Software und Unterstützung Secondlevelsupport		
Freiblick GmbH	**Kindelsbergstraße 2, 57223 Kreuztal**	x.vianova, x.comdoxx
Unterstützung bei Fernwartung, Installation und Entwicklung		
Hetzner Online GmbH	**Industriestraße 25, 91710 Gunzenhausen**	x.comdoxx
Virtuelle Server		
Hogrefe Verlag GmbH und Co. KG	**Merkelstraße 3, 37085 Göttingen**	psyx
Schnittstelle psychodiagnostische Testverfahren		
Imilia Interactive Mobile Applications GmbH	**Wichmannsstraße 7, 10787 Berlin**	x.vianova, x.concept Edition Ambulanz
Onlineterminvereinbarung		
indevis IT-Consulting and Solution GmbH	**Irschenhauser Straße 10, 81379 München**	x.webtermin, Terminfunktionen in medatixx / psyx
Mailfilter, Mobil Iron (MDM)		
Krämer IT Solutions GmbH	**Koßmannstraße 7, 66571 Eppelborn**	Kunden der Niederlassungen
Monitoring bei IT-Service-Veträgen ServerEye		
mediDOK Software Entwicklungsgesellschaft mbH	**Handschuhsheimer Landstraße 1, 69221 Dossenheim**	mediDOK
Unterstützung im Secondlevelsupport bei mediDOK		
Meier Computersysteme GmbH	**Ortsstraße 33, 92364 Deining**	Kunden der NL Süd
Technischer Support, Installationen TI		
Microsoft Deutschland GmbH	**Walter Gropius Straße 5, 80807 München**	medatixx mobil
Microsoft Deutschland GmbH		medatixx-Lizenzserver
Microsoft Deutschland GmbH		x.webtermin
Microsoft Deutschland GmbH		Verordnungsmodul (VOM)

MT-Computer ME	**Rua Ouro Branco 92, CEP 52, 111-150 Recife**	Kunden der NL Nord
Fernwartungen und Installationen		
retarus GmbH	**Aschauer Straße 30, 81549 München**	x.webtermin
Cloud-Services		
Schmidt Unternehmungsberatungs GmbH	**Gerhardt-Hauptmann-Straße 6, 99096 Erfurt**	medatixx / psyx
Unterstützung bei der Entwicklung und Weiterentwicklung		
Syntax GmbH	**Donnerschweer Straße 54, 15566 Schöneiche bei Berlin**	Kunden der NL Nord
Technischer Support, Installationen TI		
WKB-Systempartner GmbH	**Robert-Leicht-Straße 139 a, 70569 München**	x.impfen
Software-Entwicklung		
Wortmann AG	**Bredenhop 20, 32609 Hüllhorst**	Kunden der Niederlassungen
Cloud-Backup		