Auftragsverarbeitung gemäß Art. 28 DSGVO

Vereinbarung zwischen

Kunde

- Verantwortlicher - nachstehend Auftraggeber genannt -

und der

STARC medical GmbH, Jathostrasse 9, 30916 Isernhagen

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen zum Datenschutz. Sie findet Anwendung auf alle Tätigkeiten, bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

1. Gegenstand und Dauer des Auftrags

(1) **Gegenstand**
Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Alle anfallenden Arbeiten und Dienstleistungen im Rahmen des bestehenden Softwarewartungs- und Supportvertrages.

(2) **Dauer**
Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2. Konkretisierung des Auftragsinhalts

(1) **Art und Zweck der vorgesehenen Verarbeitung von Daten**
Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:
Der Auftragsverarbeiter stellt dem Auftraggeber eine Archivlösung (STARC-PACS oder STARC-easySTORE) zur Verfügung. Die Lieferung der Software erfolgt ohne jeglichen Patientenbezug. Der Auftragsverarbeiter könnte aber evtl. bei einer Programmfrage oder einer Softwarestörung vom Auftraggeber zu einer Fernwartungssitzung aufgefordert werden, die in der Regel an einem Testpatienten durchgeführt wird.
Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(2) **Art der Daten**
Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- ☒ Personenstammdaten
- ☒ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☒ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☒ Kundenhistorie
- ☒ Vertragsabrechnungs- und Zahlungsdaten
- ☒ Gesundheitsdaten
- ☒ Sozialdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben von Dritten (z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

(3) Kategorien betroffener Personen
Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☒ Kunden
- ☒ Patienten und / oder Kunden des Kunden
- ☒ Mitarbeiter

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a)

☒ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.
☐ Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.
Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
☒ Als Datenschutzbeauftragter ist beim Auftragnehmer Herr Simon Herzog, QUASI, Analyse, Beratung, Lösung, Tel. 09391/6094645, E-Mail: datenschutz@starc-medical.de bestellt.
Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
☒ Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b)

Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c)

Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in Anlage 1] sicherzustellen.

d)

Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e)

Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f)

Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g)

Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h)

Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a)

☐ Eine Unterbeauftragung ist unzulässig.

b)

☒ Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

Firma Unterauftragnehmer	Anschrift/Land	Leistung
Trimamed GmbH & Co. KG	Borsigstraße 19 30916 Isernhagen	Support-Leistungen gemäß Softwarewartungs- und Supportvertag
TeamViewer GmbH	Jahnstraße 30 73037 Göppingen	Support-Leistungen gemäß Softwarewartungs- und Supportvertag

c)

☒ Die Auslagerung auf Unterauftragnehmer oder

☒ der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Der Auftragnehmer wird etwaige Unterauftragnehmer sorgfältig auswählen und diese, soweit sie im Rahmen ihrer Tätigkeit Kenntnis von fremden Geheimnissen im Sinne dieser Vereinbarung erlangen könnten, zum Stillschweigen verpflichten. Der Auftragnehmer wird ferner etwaige Unterauftragnehmer dazu verpflichten, sämtliche von diesen eingesetzte Personen und etwaige weitere Unterauftragnehmer, die bestimmungsgemäß mit Geheimnisschutzdaten in Berührung kommen oder bei denen nicht auszuschließen ist, nach den zuvor genannten Grundsätzen zur Verschwiegenheit zu verpflichten und über die Folgen einer Pflichtverletzung zu belehren.

Des weiteren werden Subunternehmer über das bestehende Schweigerecht gemäß §53a StPO sowie den Beschlagnahmeschutz gemäß §97 StPO informiert; dies beinhaltet auch den Hinweis auf das Recht zu entscheiden und die damit verbundene Pflicht, unverzüglich den Auftraggeber bzgl. der Wahrnehmung dieser Rechte zu kontaktieren.
Diese Verpflichtung gilt für sämtliche weitere Unterbeauftragungen.

Eine weitere Auslagerung durch den Unterauftragnehmer
☐ ist nicht gestattet;
☐ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);
☒ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);
sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch (optional durch den Auftragnehmer zu belegen):
☐ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
☒ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
☒ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a)
die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b)
die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c)
die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

d)
die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e)
die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Informationspflichten, Schriftformklausel

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den Daten beim Auftraggeber liegt.

(2) Es gelten ausschließlich diese Bedingungen; Nebenabreden, Änderungen oder Ergänzungen dieser Bedingungen bedürfen für Ihre Wirksamkeit der Schriftform. Dieses gilt auch für die Abbedingung der Schriftformklausel.

12. Verpflichtung zur Geheimhaltung von Berufsgeheimnissen (§ 203 StGB)

(1) Im Rahmen dieses Auftrages werden auch Daten verarbeitet, die unter ein Berufsgeheimnis (im Sinne von 203 StGB) fallen.

Der Auftragnehmer verpflichtet sich, über Berufsgeheimnisse Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben erforderlich ist.
Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich Personen, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken und unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist, strafbar machen nach § 203 Abs. 4 S. 1 StGB.
Zudem macht sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde.

(2) Der Auftragnehmer stellt sicher, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des Auftraggebers befassten Beschäftigten und andere für den Auftragnehmer tätigen Personen (z.B. Subunternehmer), die damit befasst sind, sich in Textform dazu verpflichtet haben, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren und sie über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB belehrt wurden. Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar macht, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und die mitwirkende Person nicht dafür Sorge getragen hat, dass die weitere Mitwirkende Person zur Geheimhaltung verpflichtet wurde.

(3) Der Auftragnehmer wird darauf hingewiesen, dass Daten, die er im Auftrag eines Berufsgeheimnisträgers verarbeitet u.U. dem Zeugnisverweigerungsrechts von sogenannten mitwirkenden Personen unterliegt (§ 53a Strafprozessordnung (StPO)). Entsprechend § 53a StPO entscheidet jedoch der Berufsgeheimnisträger über die Ausübung des Schweigerechts. Im Falle einer Befragung wird der Auftragnehmer unter Hinweis auf § 53a StPO dieser widersprechen und unverzüglich den Auftraggeber informieren, der daraufhin bzgl. der Wahrnehmung des Schweigerechts entscheidet.

(4) Der Auftragnehmer wird darauf hingewiesen, dass die sich in seinem Gewahrsam befindenden Geheimnisschutzdaten dem Beschlagnahmeverbot gemäß § 97 Abs. 2 StPO unterliegen. Die Daten dürfen nicht ohne das Einverständnis des Auftraggebers (Berufsgeheimnisträger) herausgegeben werden. Im Falle einer Beschlagnahme wird der Auftragnehmer dieser widersprechen und unverzüglich den Auftraggeber informieren.

13. Haftung

Die Haftung richtet sich nach den allgemeinen Gesetzen insbesondere nach Artikel 82 DSGVO.

14. Salvatorische Klausel

Sollten einzelne Bestimmungen dieses Vertrages ganz oder teilweise unwirksam oder unanwendbar sein oder werden, oder sollte sich in dem Vertrag eine Lücke befinden, so soll hierdurch die Gültigkeit der übrigen Bestimmungen nicht berührt werden. Anstelle der unwirksamen oder unanwendbaren Bestimmung oder zur Ausfüllung der Lücke soll eine angemessene Regelung treten, die, soweit rechtlich möglich, dem am nächsten kommt, was die Vertragsparteien gewollt haben oder nach dem Sinn und Zweck dieses Vertrages gewollt haben würden, wenn sie den Punkt bedacht hätten.

15. Rechtswahl, Gerichtsstand

Soweit der Kunde Vollkaufmann ist, ist für etwaige Streitigkeiten aus den Verträgen oder damit im Zusammenhang stehenden Rechtsbeziehungen Hannover als Gerichtsstand vereinbart. Die STARC medical GmbH ist auch berechtigt, am Sitz des Kunden zu klagen. Es gilt deutsches Recht als vereinbart.

Anlage 1: Technisch-organisatorische Maßnahmen (TOM)
Diese stellt der Auftragnehmer dem Auftraggeber in freier Form zur Prüfung zur Verfügung.

Anlage 1

STARC medical
Mehr Zeit für Medizin.

Technische und organisatorische Maßnahmen (TOM) der STARC medical GmbH zu den Themen Datenschutz und Datensicherheit (i.S.d. Art. 32 DSGVO)

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die o. g. Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Folgende Maßnahmen zur Absicherung des Gebäudes wurden getroffen:

Gebäudeüberwachung durch:

» Zentrale Alarmanlage mit Aufschaltung auf einen Sicherheitsdienst

Schließsystem des Gebäudes inkl. Eingangstür/en

» Das Öffnen der Haupt-Eingangstür ist nur mittels speziellem elektronischen Schlüssel möglich, diese Tür ist permanent verschlossen.
» Die Eingangstüre zu den Büros der STARC medical GmbH ist ebenfalls über die elektronischen Schlüssel möglich, auch diese Eingangstüren sind permanent verschlossen.
» Besucher müssen an der Haupteingangstür klingeln, erst nach Nennung des Namens wird diese Tür über die Telefonanlage geöffnet.
» Die Besucher werden an der Bürotür von einem Mitarbeiter der STARC medical GmbH abgeholt, mit einem Besucherausweis versehen und dann zum jeweiligen Ansprechpartner begleitet.

Zutrittsberechtigungen (Organisatorisch)

Welcher Mitarbeiter zu welchen Räumlichkeiten Zutritt hat, wird in der Stellenbeschreibung geregelt.

Zutrittsmittel (Verwaltung)

Es existiert ein Schlüsselverzeichnis, aus dem die Schlüsselvergabe ersichtlich ist, alle Mitarbeiter unterschreiben den Erhalt und die Rückgabe der jeweiligen Schlüssel. Eine organisatorische Regelung regelt den Verlust eines Schlüssels.

Geschäftsräume (Reinigung)

Ein externes Dienstleistungsunternehmen reinigt die Büroräume der STARC medical GmbH. Der Serverraum kann von diesem Unternehmen nicht gereinigt werden, da keine Zutrittsberechtigung besteht.

Serverraum (Zugang)

Der Serverraum ist permanent verschlossen und kann nur über ein angebrachtes Codeschloss geöffnet werden, den Code hierfür haben nur berechtigte Personen.

1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten" Passworts).

Arbeitsplätze (Gestaltung)

Die Arbeitsplätze, welche für Besucher einsehbar wären sind so gestaltet, dass kein Einblick auf Bildschirme (Blickschutzfilter), Drucker und Faxe möglich ist und somit keine personenbezogenen Daten eingesehen werden können.

Benutzer (Authentifizieren und Identifizieren)

Beides erfolgt mittels Benutzernamen und Passwort am Client, sowie mittels Benutzername und Passwort am CRM-System. Ein Bildschirmschoner mit Passwortschutz ist eingerichtet und greift nach 15Min.

Passwort (Richtlinie)

Eine Dienstanweisung regelt die Anforderung an die Passwortlänge und Komplexität von Passwörtern. Einstellungen der Domäne erzwingen diese Dienstanweisung.

Remotezugriff (Mitarbeiter)

Jeder Heimarbeitsplatz hat einen aktuellen Virenscanner und einen VPN-Client als einziges Zugangssystem zu den Servern in der Firma. Die Genehmigung der VPN-Zugangserlaubnis erteilt die Geschäftsleitung.

Wartungen (und Reparaturen)

Alle Wartungs- und Reparaturarbeiten werden von internen Mitarbeitern durchgeführt.

Ein Wartungsplan regelt die permanente Pflege der vorhandenen EDV.

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Systemadministration

Die Systemadministration wird ausschließlich von Mitarbeitern der STARC medical GmbH durchgeführt, zur Administration der Anlagen wird ein spezieller Admin-Account verwendet, die Berechtigung zur Verwendung des Accounts legt die Geschäftsleitung fest.

Aktenvernichtung

Täglich anfallende Dokumente werden durch Schredder der Schutzklasse P4 vernichtet. Die Vernichtung der kompletten Aktenordner wird durch einen externen, zertifizierten Dienstleister durchgeführt.

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Daten, welche zu unterschiedlichen Zwecken erhoben wurden, werden getrennt verarbeitet.

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

2.1 Weitergabekontrolle

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. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Maßnahmen:

- Einsatz von VPN-Technologie
- Funktionierendes Backup- und Recovery-Konzept, Datenträger sind verschlüsselt und werden in einem geeigneten Safe aufbewahrt.
- Konzept zur rechtskonformen Vernichtung von Datenträgern vorhanden (Verwendung von zertifizierter Löschsoftware inkl. Entsorgungsnachweis)
- Entsorgungskonzept für die Papierentsorgung vorhanden (Schredder mit Schutzklasse P4)

2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

STARC medical GmbH nutzt zur Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten ein Berechtigungskonzept (Domäne) und ein eigenes Berechtigungskonzept für das eingesetzte ERP-System.

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

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

Betriebssicherheit

Eigenes Personal ist von 8-18 Uhr (Mo-Fr) vor Ort, am Wochenende besteht Rufbereitschaft für einen Techniker, der bei Alarmierung vor Ort kommt.

Datensicherung

» Tägliches Backup aller Maschinen
» Tägliche Replikation aller Maschinen auf einen Backupserver
» Kontrolle der Backups und Replikationen mittels E-Mail-Benachrichtigung
» Geplante Rücksicherungen einzelner Backups auf dem Replikationsserver inkl. Dokumentation

Schutz vor Ausfall der Systeme (Elektrisch)

» Alle Systemrelevanten Server werden durch ein mehrstufiges Sicherheitskonzept geschützt.
» Spezielle Steckdosenleisten schützen die nachgelagerten Systeme vor Überspannung
» 2 redundante Unterbrechungsfreie Stromversorgungen (USV)
» Beide Unterbrechungsfreie Stromversorgungen werden von jeweils 2 getrennten Stromkreisen versorgt

Schutz vor Brand- und Wasserschäden:

» Im Serverraum sind Feuerlöscher vorhanden
» Ein Sensor überwacht sowohl die Raumtemperatur, als auch die Feuchtigkeit

Schutz vor Überhitzung:

» Klimaanlage
» Regelmäßige Wartung der Klimaanlage
» Optimale Positionierung der Anlage

3.2 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

a. Datenschutz-Management

Dokumentation:
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz
mit Zugriffsmöglichkeit für Mitarbeiter.

Schulung/Sensibilisierung:
Alle Mitarbeiter wurden bzgl. Datenschutz/Datensicherheit geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet.
Eine Mitarbeitersensibilisierung wird jährlich durchgeführt, alle Mitarbeiter müssen dafür unterschreiben.

Wirksamkeit der getroffenen Maßnahmen:
Alle getroffenen Maßnahmen werden durch den Datenschutzbeauftragten regelmäßig überprüft.

Datenschutzbeauftragter:
Zur Einhaltung bestehender Gesetze, zur Sensibilisierung der Mitarbeiter und als Ansprechpartner für die Kunden der STARC medical GmbH wurde ein Datenschutzbeauftragter bestellt und der zuständigen Landesbehörde gemeldet:

Kontaktdaten:
QUASI, Analyse, Beratung, Lösung, Herr Simon Herzog
Michelriether Str. 26
97828 Marktheidenfeld
Telefon: 09391/6094645, E-Mail: datenschutz@starc-medical.de

Weitere getroffene Maßnahmen:
Ein formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener wurde etabliert und im Team vorgestellt.

b. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen
STARC medical setzt Firewall-Technologien nach aktuellem Stand der Technik ein, diese sind unter anderem:

» Intrusion Detection System (IDS)
» Intrusion Prevention System (IPS)
» Virenscanner mit mehrmals täglicher Aktualisierung und geplanten Scans der kompletten Systeme

Außerdem wurden folgende Organisatorische Maßnahmen getroffen:

» Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
» Der Datenschutzbeauftragte wird in Sicherheitsvorfälle und Datenpannen eingebunden

STARC medical ist zertifiziert nach PN-EN ISO 13485:2012

c. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

Privacy by Design / Privacy by default

Es gibt ein einheitliches Konzept zu datenschutzfreundlichen Voreinstellungen und
Standards innerhalb der IT basierend auf der internen Richtlinie. Hierunter fallen:
Einstellung des Betriebssystems für Client PCs und der automatischen Bereitstellung und Verteilung von Software-Applikationen
Einstellung des Betriebssystems für aus Vorlagen bereitgestellten virtuellen Servern
Festplattenverschlüsselung für Client Endgeräte (Notbooks, PCs)

d. Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Alle Auftragnehmer der STARC medical GmbH werden nach strengen Sorgfaltsgesichtspunkten bzgl. Datenschutz und Datensicherheit ausgewählt. Mit allen Auftragsnehmern werden die benötigten Vereinbarungen zur Auftragsverarbeitung geschlossen und alle Mitarbeiter wurden auf das Datengeheimnis verpflichtet.