Vertrag zur Auftragsverarbeitung (AVV)

1. Parteien und Gegenstand

1.1 Dieser Vertrag zur Auftragsverarbeitung (AVV) regelt die datenschutzrechtlichen Beziehungen in Bezug auf die Überlassung und die Zurverfügungstellung der Webanwendung QuickBEM zwischen der Medisoft GmbH (nachfolgend Medisoft) und dem Kunden. Medisoft ist nur unter der Bedingung bereit, dem Kunden eine Nutzungslizenz einzuräumen, dass der Kunde sämtliche Bestimmungen dieses Vertrages uneingeschränkt akzeptiert.

1.2 Im Sinne dieses AVV ist Medisoft der Auftragnehmer und der Kunde der Auftraggeber.

1.3 Der Auftragnehmer verarbeitet im Rahmen der Webanwendung QuickBEM für den Auftraggeber personenbezogene Daten im Rahmen einer Auftragsverarbeitung gemäß Art. 28 DSGVO. Gegenstand, Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind in Anlage 1 näher definiert.

1.4 Die vom Auftrag betroffenen Personen und die damit verbundenen Zugriffe auf deren Daten sind in Anlage 2 aufgeführt.

1.5 Änderungen des Verarbeitungsgegenstandes, Verarbeitungsumfanges sowie Verfahrensänderungen sind schriftlich zu vereinbaren.

1.6 Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, 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 bis 49 DSGVO erfüllt sind.

2. Pflichten des Auftragnehmers

2.1 Der Auftragnehmer führt die Leistungen ausschließlich im Rahmen der getroffenen Vereinbarung und nach Weisung des Auftraggebers durch. Der Auftraggeber ist verpflichtet, die Weisungen schriftlich zu erteilen. Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen geltendes Recht verstößt.

2.2 Der Auftragnehmer verwendet Daten, die ihm im Rahmen der Erfüllung dieses Vertrags bekannt geworden sind, nur für die vereinbarten Vertragszwecke. Eine Verarbeitung oder Nutzung ohne Kenntnis des Auftraggebers oder zu eigenen Zwecken des Auftragnehmers ist nicht erlaubt. Kopien oder Duplikate 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.

2.3 Der Auftragnehmer sichert in seinem Verantwortungsbereich die Umsetzung und Einhaltung der vereinbarten allgemeinen und technischen und organisatorischen Maßnahmen entsprechend Art. 32 DSGVO zu. Die konkreten Vorgaben sind durch Anlage 3 geregelt. Der Auftragnehmer hat die Umsetzung der Maßnahmen zu dokumentieren und dem Auftraggeber auf Anfrage zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Bestandteil des Vertrags.

2.4 Sofern ein betrieblicher Datenschutzbeauftragter (freiwillig oder verpflichtend) bestellt wurde, wird der Auftragnehmer diesen in Anlage 4 entsprechend benennen. Bei der Bestellung werden die gesetzlichen Anforderungen der Art. 37 bis 39 DSGVO sowie der nationalen Regelungen entsprechend berücksichtigt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

2.5 Der Auftragnehmer verpflichtet sich, soweit rechtlich und tatsächlich möglich, den Verantwortlichen auch mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen zu unterstützen, die Betroffene zur Ausübung ihrer Rechte nach Art. 12-22 DSGVO stellen. Dies betrifft insbesondere das Auskunftsrecht der Betroffenen (Art. 15 DSGVO), das Recht auf Berichtigung unrichtiger personenbezogener Daten, das Recht der Betroffenen auf Löschung ihrer personenbezogenen Daten (Art. 17 DSGVO) sowie das Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO). Der Auftragnehmer darf Daten nur auf dokumentierte Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Er wird ferner keinerlei Auskunft über personenbezogene Daten an Dritte, aber auch nicht an den Betroffenen selbst erteilen. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

2.6 Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit schriftlich verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

2.7 Der Auftragnehmer unterrichtet den Auftraggeber umgehend bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder andere Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers sowie in Fällen eines Verstoßes gegen die in diesem Auftrag getroffenen Festlegungen. Ebenso informiert er den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde oder anderer öffentlicher Stellen.

2.8 Darüber hinaus unterstützt der Auftragnehmer den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei seinen Verpflichtungen aus Art. 33 DSGVO (Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde) sowie aus Art. 34 DSGVO (Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person). Ebenso unterstützt er den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Durchführung der Datenschutz-Folgenabschätzung, einer ggf. erforderlichen Konsultation der Aufsichtsbehörde (Art. 35, 36 DSGVO) sowie sonstigen behördlichen Anfragen und Kontrollen.

2.9 Der Auftragnehmer führt ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten, die den Anforderungen des Art. 30 Abs. 2 DSGVO genügt. Hinsichtlich des Verzeichnisses von Verarbeitungstätigkeiten des Auftraggebers hat der Auftragnehmer den Auftraggeber auf Anforderung in dem ihm möglichen Umfang zu unterstützen.

2.10 Der Auftragnehmer verpflichtet sich, dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten zur Verfügung zu stellen. Er erteilt auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte, die zur Durchführung einer umfassenden Kontrolle erforderlich sind.

2.11 Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind.

3. Pflichten des Auftraggebers

3.1 Der Auftraggeber ist für die Einhaltung der jeweils einschlägigen Datenschutzgesetze sowie die Wahrung der Betroffenenrechte verantwortlich. Betroffenenrechte sind gegenüber dem Auftraggeber geltend zu machen.

3.2 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

4. Rechte des Auftraggebers (Kontrollen)

4.1 Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Ablauf der Datenverarbeitung zu erteilen. Gleiches gilt für die Festlegung bzw. Fortschreibung der Datensicherungsmaßnahmen.

4.2 Der Auftraggeber oder ein Beauftragter des Auftraggebers kann sich nach rechtzeitiger Anmeldung zu Prüfzwecken in den Betriebsstätten zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsverarbeitung einschlägigen Datenschutzgesetze überzeugen. Der Auftragnehmer hat die entsprechenden Kontrollen zu dulden und wird den Auftraggeber bei deren Durchführung unterstützen.

4.3 Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer umfassenden Kontrolle erforderlich sind.

5. Subunternehmer

5.1 Aufträge an Subunternehmer durch den Auftragnehmer dürfen nur mit schriftlicher Genehmigung des Auftraggebers vergeben werden. Dies und die nachfolgenden Regelungen gelten auch für den Subunternehmer.

5.2 Der Auftragnehmer hat den Auftraggeber ohne gesonderte Aufforderung über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Subunternehmer zu informieren. Gegen solche Änderungen steht dem Auftraggeber ein Widerspruchsrecht zu.

5.3 Der Auftragnehmer hat den Subunternehmer sorgfältig auszuwählen. Er hat sich vor Beginn der Datenverarbeitung durch den Subunternehmer und sodann regelmäßig von der Einhaltung der beim Subunternehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen und die Ergebnisse zu dokumentieren. Dem Auftraggeber ist auf Verlangen die Prüfdokumentation zur Verfügung zu stellen.

5.4 Die Auftragsvergabe an Subunternehmer muss mittels eines schriftlichen Vertrages erfolgen. Die vertraglichen Vereinbarungen sind so zu gestalten, dass sie den Anforderungen dieser Vereinbarung entsprechen, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt.

5.5 Dem Auftraggeber sind unmittelbare Kontroll- und Überprüfungsrechte entsprechend Ziffer 4 dieser Vereinbarung auch gegenüber dem Subunternehmer einzuräumen. Ebenso ist der Auftraggeber berechtigt, auf schriftliche Anforderung vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragsnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

5.6 Sofern der Subunternehmer außerhalb eines in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum stammt oder die Datenverarbeitung dort stattfindet, ist durch den Auftragnehmer darüber hinaus sicherzustellen, dass die Voraussetzungen der Art. 44 bis

49 DSGVO erfüllt sind. Dies ist dem Auftraggeber gegenüber schriftlich vor Aufnahme der Tätigkeiten des Subunternehmers nachzuweisen.

5.7 Die Genehmigung zur Einschaltung der Dienstleister in Anlage 5 gilt als erteilt, sofern die vorstehenden Anforderungen erfüllt sind.

5.8 Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten eines jeden Subunternehmers.

6. Vertraulichkeit

6.1 Die Parteien verpflichten sich, die ihnen während der Durchführung dieses Vertrages zur Kenntnis gelangten Informationen und Unterlagen, insbesondere Geschäfts- und Betriebsgeheimnisse des Vertragspartners streng vertraulich zu behandeln. Ebenso vertraulich zu behandeln sind der Gegenstand und Inhalt des Vertrages. Die Parteien sind verpflichtet, die zur Verfügung gestellten oder im Rahmen des Auftrages zur Kenntnis genommenen Daten und Informationen des Vertragspartners ausschließlich im Rahmen des Vertragszwecks zu verarbeiten und zu nutzen. Eine Verarbeitung oder Nutzung für eigene Zwecke sowie eine Weitergabe an Dritte ist nur nach schriftlicher Zustimmung des Vertragspartners zulässig.

6.2 Sofern zur Abwicklung des Auftrages die Einschaltung Dritter erforderlich ist, wird dafür Sorge getragen, dass die getroffenen Datenschutz- und Geheimhaltungsvereinbarungen von diesen Dritten ebenfalls strikt eingehalten werden. Die Einschaltung von Dritten erfordert das ausdrückliche Einverständnis des Vertragspartners.

6.3 Die vorstehenden Rechte und Pflichten gelten über die Dauer des Vertrages fort.

7. Vertragslaufzeit und Kündigung

7.1 Der Auftrag ist unbefristet erteilt und kann mit einer Frist von 4 Wochen zum Monatsende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt. Die Verpflichtungen zur Einhaltung des Datengeheimnisses und der Vertraulichkeit bestehen auch nach Beendigung dieser Vereinbarung fort.

7.2 Nach Beendigung des Vertrages oder früher nach Aufforderung durch den Auftraggeber hat der Auftragnehmer sämtliche in seinem Besitz befindlichen Unterlagen, Datenträger oder sonstigen Ergebnisse auf Wunsch des Auftraggebers physisch zu löschen bzw. diesem restlos mit der Erklärung zurückzugeben, dass sich keine weiteren Kopien beim Auftragnehmer oder bei Unterauftragnehmern befinden. Beim Auftragnehmer gespeicherte Daten sind physisch zu löschen. Die Löschung ist zu dokumentieren. Test- und Ausschussmaterial ist unverzüglich datenschutzkonform zu vernichten bzw. zu löschen.

7.3 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.

7.4 Der Auftraggeber ist berechtigt, die Einhaltung der vorstehenden Verpflichtungen, ggf. auch vor Ort, zu kontrollieren.

8. Verschiedenes

8.1 Ausschließlicher Gerichtsstand für alle Streitigkeiten aus diesem Vertragsverhältnis ist der Geschäftssitz von Medisoft.

8.2 Sämtliche Rechtsbeziehungen im Zusammenhang mit dieser Vereinbarung richten sich ausschließlich nach dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN-

Kaufrechtsübereinkommens (CISG) und der Weiterverweisungsregeln des deutschen internationalen Privatrechts.

8.3 Der Kunde darf die ihm aus dem Vertrag obliegenden Rechte und Pflichten nicht ohne vorherige schriftliche Zustimmung von Medisoft ganz oder teilweise abtreten, welche nicht ohne wichtigen Grund verwehrt werden soll.

8.4 Änderungen, Ergänzungen oder eine Aufhebung dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für die Aufhebung des Schriftformerfordernisses. Mündliche Nebenabreden sind nicht getroffen.

8.5 Vertragssprache ist deutsch. Werden von dieser Vereinbarung Übersetzungen angefertigt, so bleibt alleine die deutsche Fassung maßgeblich.

8.6 Sollte eine Bestimmung dieser Vereinbarung unwirksam, undurchführbar oder lückenhaft sein oder werden, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. Anstelle der unwirksamen, undurchführbaren oder fehlenden Bestimmungen gilt diejenige Bestimmung als vereinbart, welche die Parteien vernünftigerweise vereinbart hätten, wenn ihnen die Unwirksamkeit, Undurchführbarkeit oder Lückenhaftigkeit bewusst gewesen wäre.

Anlage 1
Leistungsbeschreibung

Die Tätigkeiten des Auftragnehmers für den Auftraggeber im Rahmen der Auftragsverarbeitung sind wie folgt festgelegt (Mehrfachnennungen sind möglich):

☒ **IT-Dienstleistungen**

- ☒ Pflege und Wartung der folgenden Software-Produkte: **Webanwendung QuickBEM**
- ☒ Betrieb des folgenden Software-Produkts (SaaS): **Webanwendung QuickBEM**
- ☒ Bereitstellung von Rechenzentrums-Leistungen: ScaleUp Technologies GmbH & Co. KG

Anlage 2
Betroffene Personen und Datenkategorien

Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber. Diese werden im Folgenden spezifiziert. Bedingt durch den technologischen Wandel und organisatorischen Veränderungen kann sich die Zusammensetzung der Daten auch verändern.

1. Betroffene Personengruppen

☒ Beschäftigte

☒ Bewerber

☒ Auszubildende

☒ Ggf. Fremdpersonal (Leiharbeitskräfte, Freiberufler etc.)

2. Zugriffsberechtigte (Nutzergruppen)

☒ Mitarbeiter des Auftraggebers (Admin-Rechte)

☒ Mitarbeiter des Auftraggebers (eingeschränkter Zugriff auf jeweiligen Bereich)

☒ Mitarbeiter Medisoft (Lieferant) Admin-Rechte für Wartung und Systempflege

3. Datenkategorien

☒ Personenstammdaten (z.B. Name, Vorname, Kontaktdaten)

☒ Kommunikationsstammdaten (eMail, Telefon, Mobiltelefon)

☒ Personenidentifikationsdaten

☒ Anschrift von Dritten

☒ Ärztliche Dokumentationsdaten (Befunde, Untersuchungsergebnisse, Terminplanungen)

☒ Systemdaten zur Sicherstellung des Systembetriebs (Systemprotokolldaten)

☒ **Besondere Daten der betroffenen Personen (gemäß Artikel 9 DSGVO)**

☒ Gesundheitsdaten (vgl. Artikel 4 Nr. 15 DSGVO)

Anlage 3
Technische und organisatorische Schutzmaßnahmen

Bei der Verarbeitung personenbezogener Daten sind technische und organisatorische Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des Datenschutzes zu gewährleisten:

„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.“

[Artikel 32 DSGVO]

Es sind insbesondere – aber nicht abschließend – die nachfolgenden Vorgaben zu beachten:

Diese technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es der datenempfangenden Gesellschaft gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber anzuzeigen.

Die Zugangsberechtigungen sind auf die für die Aufgabenerfüllung notwendigen Rechte zu beschränken (Minimalprinzip). Nach Erfüllung der Aufgabe sind die Berechtigungen zu löschen oder zu sperren. Die Rechtebeantragung unterliegt der Pflichtentrennung. Die Vergabe ist zu dokumentieren.

Sofern ein Zugriff auf das System des Auftraggebers stattfindet, sind diese Zugangsrechte für Mitarbeiter des Auftragnehmers beim Auftraggeber per E-Mail unter Nennung der Gründe und des Umfangs der Rechte zu beantragen bzw. der Auftraggeber ist rechtzeitig vorher zu informieren. Sollte der Zugriff auf personenbezogene Daten nicht zwingend erforderlich sein, so ist hierauf zu verzichten. Die Rechte sind in

Lese- und Schreibrechte zu unterscheiden. Der Zugriff über externe Netze ist entsprechend zu schützen (Verschlüsselung, Authentifizierung etc.: siehe oben).

Die Zugangsprotokolle umfassen erfolgreiche / erfolglose Logins und vom Benutzer bzw. dem System initiierte Logins. Systemsicherheitsrelevante Aktivitäten (alle Aktivitäten im Administrator-Modus) sind stets zu protokollieren. Die Protokolldaten sind manipulationssicher, zeitnah verfügbar und gemäß den gesetzlichen Anforderungen aufzubewahren. Der Zugriff auf Protokolldaten ist nur autorisierten Benutzern zu gestatten. Die Protokolldaten sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

Es sind sichere Kennwortverfahren nach dem aktuellen Stand der Technik (beispielsweise gemäß Empfehlungen des BSI) eingerichtet. Datenverarbeitungssysteme werden gesperrt, wenn diese unbeaufsichtigt sind. Es sind Maßnahmen der Zwei-Faktor-Authentifizierung zu prüfen.

Wenn Daten / Unterlagen nicht unter Aufsicht / Kontrolle der zuständigen Mitarbeiter sind, sind sie unter Verschluss aufzubewahren und beim Transport entsprechend des Schutzbedarfs sicher zu transportieren; hierzu sollten mobile Datenträger verschlüsselt werden.

Die Daten sind entsprechend zu ihren Zwecken getrennt zu verarbeiten. So sind die vorgegebenen Systeme zu nutzen und keine Datenexporte vorzunehmen, um Daten unterschiedlicher Systeme / Zweckbestimmungen zusammenzuführen (z. B. in Excel).

Auch ist Unbefugten der Zutritt zu den Räumlichkeiten zu verwehren. Hierunter fallen neben dem Serverraum auch die weiteren Räume, in denen sich Datenverarbeitungsanlagen befinden, die einen Zugang zu den Systemen ermöglichen. Zutritt ist nur für bestimmte, berechtigte Zwecke erlaubt. Hierbei sind auch Personen von Dienstleistern entsprechend zu berücksichtigen. Zur Zutrittskontrolle gehören ferner u. a. folgende Maßnahmen:

- Zutrittskontrollsystem
- Türsicherung (elektrische Türöffner usw.)
- Werkschutz, Pförtner, Besucherregelung
- Überwachungseinrichtung
- Alarmanlage

Die Übertragung von personenbezogenen Daten ist zu schützen. Die Klassifikationsstufe der jeweiligen Informationen ist bei der Form des Datenaustauschs entsprechend zu berücksichtigen. Sollten im Rahmen des gleichen Datenaustauschs Informationen mit unterschiedlichen Klassifikationsstufen an einen Kommunikationspartner übermittelt werden, dann ist für den gesamten Datenaustausch das Schutzniveau der höchsten Klassifikationsstufe zu nutzen. Die Übertragung sensibler / vertraulicher Daten ist ausschließlich in verschlüsselter Form zulässig.

Sofern eine direkte Personenbeziehbarkeit nicht erforderlich ist, ist von den Möglichkeiten der Pseudonymisierung Gebrauch zu machen, wenn dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht (Datensparsamkeit).

Nicht mehr benötigte Daten sind zeitnah und sicher zu vernichten, z. B. wenn eine gesetzliche Vorschrift existiert, die die Löschung zwingend vorschreibt oder eine gesetzliche und / oder die betriebliche Aufbewahrungsnotwendigkeit entfällt.

Datenträger, die schützenswerte Daten enthalten und nicht mehr gebraucht werden oder aufgrund eines Defektes ausgesondert werden sollen, sind so zu entsorgen, dass keine Rückschlüsse auf vorher gespeicherte Daten möglich sind; bis zur Vernichtung sind diese sicher zu verwahren, dass Unbefugte auf die Unterlagen nicht zugreifen können. Analoges gilt für Belege und Druckausgaben.

Es sind angemessene Maßnahmen zu ergreifen, die die Unversehrtheit der Daten und der Programme vor Fälschung, Vernichtung und Änderung sicherstellen. Auch sind Maßnahmen einzuführen, die fehlerhafte Daten als solche erkennen. So sind u. a. eingehende Daten (z. B. E-Mails oder Datenträger) auf Viren zu prüfen und die Mitarbeiter entsprechend zu sensibilisieren). Die Firewall ist so zu konfigurieren und zu administrieren, dass sie einen effektiven Schutz darstellt und Manipulationen verhindert werden.

Um Sicherheitslücken in den IT-Systemen zu schließen, sind zeitnah Sicherheits-Updates und -Patches einzuspielen. Hierbei sind mobile Geräte bzw. nicht dauerhaft mit dem internen IT-Netzwerk verbundene Geräte ebenfalls zu berücksichtigen.

Dateneingaben, -veränderungen und -löschungen sind zu protokollieren. Diese sind regelmäßig auf unbefugte Datenverarbeitungsvorgänge zu prüfen.

Um das Risiko eines Datenverlusts zu reduzieren, sind regelmäßige Datensicherungen durchzuführen. Ferner sind die Datenverarbeitungssysteme entsprechend zu warten und zu aktualisieren. Ferner gehören zur Verfügbarkeitskontrolle u. a. folgende Maßnahmen:

- Backup-Verfahren
- Spiegeln von Festplatten
- Unterbrechungsfreie Stromversorgung (USV)
- Getrennte (räumliche) Aufbewahrung der Datensicherungen
- Virenschutz / Firewall

Alle sicherheitsrelevanten Ereignisse (wie z. B. unerklärliches Systemverhalten, Verlust oder Veränderung von Daten und Programmen, Verfügbarkeit nicht explizit freigegebener Dienste, Verdacht auf Missbrauch der eigenen Benutzerkennung, usw.) sind sofort zu melden. Es sind Maßnahmen für Notfall-, Katastrophen- und Wiederanlaufplanung zu erstellen.

Es hat eine regelmäßige Überprüfung hinsichtlich der Wirksamkeit der getroffenen Maßnahmen stattzufinden. So sollte in regelmäßigen Abständen eine Analyse durchgeführt werden, die die derzeitigen Schwächen und Schwachstellen aufdeckt. Darauf aufbauend sind Maßnahmen zur Beseitigung zu erarbeiten. Darüber hinaus ist eine Risikoanalyse durchzuführen, um die Risiken hinsichtlich des Geschäfts aufzudecken und bei den IT-Sicherheitsmaßnahmen zu berücksichtigen.

Es ist sicherzustellen, dass die Einhaltung der Datenschutzgrundsätze nachgewiesen werden kann (Rechenschaftspflicht). Es sind geeignete technische und organisatorische Maßnahmen umzusetzen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß den datenschutzrechtlichen Vorschriften erfolgt. Dies bedeutet, dass beweissicher dokumentiert werden muss, was zur Einhaltung der datenschutzrechtlichen Vorgaben unternommen wird.

Die Umsetzung der vorangestellten Anforderungen seitens des Auftragnehmers wird mittels folgender Dokumente nachgewiesen:

☒ Eigenerklärung / DS-Kontrolldokumentation zu den Technischen und Organisatorischen Maßnahmen beim Auftragnehmer

☒ Zertifikat (ISO 27001/ISO 27002/BSI) des Subunternehmers (RZ-Betrieb)

☒ Prüfvermerke unabhängiger Dritter (Revisions-/Audit-Reports)

Anlage 4
Betrieblicher Datenschutzbeauftragter

Datenschutzbeauftragter des Auftragnehmers:

Name:	Claas Rudolph
	Medisoft GmbH | Zertifizierter Datenschutzbeauftragter (TÜV)
Anschrift:	Haferweg 38
	22769 Hamburg
Tel.-Nr.:	+49 40 8888 00 7-0
E-Mail:	datenschutz@medisoft.de

Der betriebliche Datenschutzbeauftragte ist der zuständigen Aufsichtsbehörde (Hamburger Beauftragte für Datenschutz und Informationsfreiheit) gem. Art. 37 (7) DSGVO ordnungsgemäß gemeldet.

Anlage 5
Unterauftragnehmer gemäß Ziffer 5 des Vertrags

Es besteht ein Unterauftragsverhältnis zu dem nachfolgend aufgeführten Rechenzentrum.

Name des Dienstleisters:	ScaleUp Technologies GmbH & Co. KG
Anschrift:	Süderstr. 198
	20537 Hamburg
Art der Dienstleistung / Verarbeitung:	Rechenzentrum
Tel.-Nr.:	+49 40 59380 500
E-Mail:	support@scaleuptech.com
Bestellter Datenschutzbeauftragter	Tobias Mauß (Mauß Datenschutz)
Tel.-Nr.:	+49 40 999 99 52-0
E-Mail:	datenschutz@datenschutzbeauftragter-hamburg.de

Das Rechenzentrum, in dem die Systeme der Medisoft GmbH untergebracht sind, ist ISO 27001-zertifiziert und befindet sich am oben angegebenen Standort. Der Zutritt des Rechenzentrums ist rund um die Uhr möglich. Das Rechenzentrum selbst ist videoüberwacht. Zudem verfügt das Rechenzentrum über eine automatische Brandlöschanlage (Argon-Flutung).

1. **Infrastruktur**

- Mehrstufige Firewall
- Schaffung einer Demilitarisierten Zone (DMZ)
- Die Datenbank und der Active-Directory-Server erhalten private IP-Adressen (NAT)
- Segmentierung der Netze
- Aufteilen der Terminal-Server (ein Server pro Mandant)
- Trennung der Mandanten über gekapselte virtuelle Maschinen
- IPSEC-VPN
- Zutritt via Handscanner und RFID-Card

Bei einem Ausfall der Datenbank wird ein Backup zurückgesichert. Die Benutzer haben keine Möglichkeit, Änderungen an der Datenbankstruktur vorzunehmen.

2. **Zusätzliche Sicherheitsmaßnahmen**

- Fremd- und Reinigungspersonal darf das Rechenzentrum nur unter Aufsicht betreten.
- Das Rechenzentrum wird per Kamera überwacht und die Racks sind abgeschlossen.
- Die Möglichkeit, unbemerkt Zugriff auf die IT-Systeme im Rechenzentrum zu erhalten, kann mit an Sicherheit grenzender Wahrscheinlichkeit ausgeschlossen werden.
- Die Datenbank ist über das Netz für den Benutzer nicht direkt erreichbar.
- Eine Fernwartung ist nur über den VPN-Tunnel und für Geräte mit bekannten MAC-Adressen möglich.
- Der Zugang erfolgt verschlüsselt mit komplexen Kennwörtern.

Durch die Summe an Sicherheitsmaßnahmen kann eine missbräuchliche IT-Nutzung hinreichend zuverlässig ausgeschlossen werden.