Vertrag zur Auftragsverarbeitung gemäß Art. 28 Datenschutz-Grundverordnung (DS-GVO) zwischen

als Auftragsverarbeiter im Sinne der DS-GVO,
nachfolgend „**Auftragnehmer**“ genannt

und dem Universitätsklinikum Carl Gustav Carus Dresden an der Technischen Universität Dresden, AÖR
als Verantwortlicher im Sinne der DS-GVO,
nachfolgend „**Auftraggeber**“ genannt

Auftragnehmer und Auftraggeber haben einen Vertrag über …… (im Folgenden „Hauptvertrag“ genannt) geschlossen. Im Rahmen der vertraglich zu erbringenden Leistungen ist der Zugriff auf personenbezogene Datenbestände (z.B. Patienten-Behandlungsdaten und / oder Mitarbeiterdaten) nicht auszuschließen.

Dieser Vertrag konkretisiert die datenschutzrechtlichen Verpflichtungen, die sich aus der im Hauptvertrag beschriebenen Arbeitsaufgabe ergeben.
Zur Einhaltung der Datenschutzbestimmungen und der ärztlichen Schweigepflicht werden ausgehend von in dem Hauptvertrag bereits getroffenen Festlegungen folgende Maßnahmen zwischen dem Auftragnehmer und dem Auftraggeber vereinbart:

§ 1 Allgemeine Regelungen

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz, insbesondere der EU Datenschutz-Grundverordnung, des Bundesdatenschutzgesetzes, der landesgesetzlichen Bestimmungen sowie der auf Grundlage dieser Gesetze ergangenen untergesetzlichen Normen und Verwaltungsvorschriften zu beachten und gewährleistet, dass er die aus dem Bereich des Auftraggebers erlangten Informationen, insbesondere Patienten- und Beschäftigtendaten, Informationen über Datensicherheitsmaßnahmen und alle sonstigen vertraulichen Daten
   - streng vertraulich behandelt und
   - Dritten nicht zugänglich werden, insbesondere auch nicht an mit dem Auftragnehmer verbundene Unternehmen.

(2) Die Verwendung von vertraulichen Informationen ist ausschließlich im Rahmen der vereinbarten Arbeitsaufgabe und nur denjenigen gestattet, die in die jeweilige Arbeitsaufgabe eingebunden und auf Informationen angewiesen sind.

(3) Die Bestimmungen dieses Vertrags finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag im Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

§ 2 Gegenstand und Dauer der Verarbeitung; Spezifizierung des Arbeitsauftrags inkl. Datenarten und Kreis der Betroffenen

(1) Der Auftragnehmer erbringt für den Auftraggeber auf Grundlage des …… ("Hauptvertrag") folgende Leistungen im Bereich:
…...

Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten des Auftraggebers und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers.

Im Einzelnen sind insbesondere die folgenden Datenarten / -kategorien Bestandteil der Verarbeitung [Anmerkung: Bitte ausfüllen, sofern noch nicht im Hauptvertrag geregelt, andernfalls streichen]:

Kreis der betroffenen Personen (z.B. Patienten; Beschäftigte) (Kategorien beschreiben/aufzählen)

Art der Daten / Datenkategorien (näher spezifizieren, aufzählen)

Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den Bestimmungen dieses Vertrages nicht darüber hinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 3 Weisungsgebundene Verarbeitung und Remonstrationspflicht

(1) Der Auftragnehmer darf personenbezogene Daten ausschließlich zur Erfüllung des mit dem Auftraggeber geschlossenen Hauptvertrags und nur nach dokumentierter Weisung des Auftraggebers verarbeiten, es sei denn, dass er durch Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem der Auftragnehmer unterliegt, zur Verarbeitung verpflichtet ist. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt.

(2) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf hinweisen, wenn die Befolgung einer vom Auftraggeber erteilten Weisung nach seiner Ansicht gegen die DS-GVO oder andere gesetzliche Vorgaben verstößt. Der Auftragnehmer kann in diesem Fall die Durchführung der erteilten Weisung aussetzen bzw. einstellen, bis die Weisung vom Auftraggeber bestätigt bzw. geändert wurde.

(3) Weisungsberechtige Personen im Hinblick auf die Datenverarbeitung nach dieser Auftragsverarbeitungsvereinbarung auf Seiten des Auftraggebers sind:

[Name, Kontaktdaten]
…
…

Weisungsempfänger auf Seiten des Auftragnehmers sind:

[Name, Kontaktdaten]
…
…

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch Nachfolger bzw. Vertreter mitsamt Kontaktdaten mitzuteilen.

§ 4 Vertraulichkeits-/Verschwiegenheitspflicht

(1) Der Auftragnehmer wird zur Durchführung des Vertrages nur Personen beschäftigen, die vor der Aufnahme ihrer Tätigkeit zur Vertraulichkeit verpflichtet und in geeigneter Weise mit den Anforderungen des Datenschutzes vertraut gemacht wurden. Ferner müssen die eingesetzten Personen vor der Aufnahme ihrer Tätigkeit darauf hingewiesen werden, dass das Datengeheimnis auch nach Beendigung der Tätigkeit fortbesteht. Der Auftragnehmer hat sein Personal insbesondere darauf hinzuweisen, dass Verstöße gegen datenschutzrelevante Bestimmungen strafrechtliche Folgen nach sich ziehen können. Über die Verpflichtung und Unterrichtung der Beschäftigten besteht Nachweispflicht seitens des Auftragsverarbeiters gegenüber dem Auftraggeber.

(2) [Anmerkung: Dieser Absatz und die dazugehörige Anlage 1 sind zu streichen, wenn keine Patientendaten verarbeitet werden] Der Gesetzgeber hat Dritte, die an der Berufsausübung eines Berufsgeheimnisträgers mitwirken, in den Straftatbestand des § 203 StGB einbezogen. Die sonstige mitwirkende Person im Sinne des § 203 StGB ist zur Geheimhaltung zu verpflichten. Die Einhaltung der Verpflichtung ist sicherzustellen. Sollte es sich bei dem Personal des

Auftragnehmers um Personen handeln, die nicht der Gruppe der Berufsgeheimnisträger gemäß § 203 StGB angehören, müssen diese Mitarbeiter zusätzlich auf die Pflicht zur Geheimhaltung verpflichtet werden. Für diese Zusatzverpflichtung ist das Formular in Anlage 1 zu nutzen. Der Auftragnehmer muss die Verpflichtung entsprechender Mitarbeiter gegenüber dem Auftraggeber auf Anforderung nachweisen.

§ 5 Sicherheit der Verarbeitung/Technische und organisatorische Maßnahmen gemäß Art. 32 DS-GVO

(1) Der Auftragnehmer gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den Anforderungen des Datenschutzes gerecht wird. Er ergreift dafür alle erforderlichen technischen und organisatorischen Maßnahmen gem. Artikel 32 DS-GVO. Diese werden in **Anlage 2** spezifiziert [Anmerkung: die Maßnahmen sind vom Auftragnehmer als Anlage dem Vertrag hinzuzufügen]. Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Während der Dauer dieses Auftrags sind diese durch den Auftragnehmer fortlaufend an die Anforderungen dieses Auftrags anzupassen und dem technischen Fortschritt entsprechend weiterzuentwickeln, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

(2) Der Auftragnehmer verpflichtet sich, Änderungen der technischen und organisatorischen Maßnahmen, die einen wesentlichen Einfluss auf das gewährleistete Sicherheitsniveau haben, als Ergänzung der **Anlage 2** schriftlich zu dokumentieren, was auch in einem elektronischen Format erfolgen kann, und dem Auftraggeber zur Kenntnis zu geben.

(3) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung jederzeit eine aktuelle Beschreibung der getroffenen technischen und organisatorischen Maßnahmen vorzulegen, soweit diese für den Auftragsgegenstand gem. § 1 dieser Vereinbarung erforderlich ist.

§ 6 Leistungsort

(1) Der Auftragnehmer wird die vertraglichen Leistungen in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) oder in einem Drittland erbringen, soweit es für das jeweilige Drittland einen Angemessenheitsbeschluss nach Art. 45 DSGVO gibt. Dies gilt in gleicher Weise für etwaige Unterauftragnehmer (siehe § 7). Die zum Zeitpunkt der Auftragserteilung vereinbarten Leistungsstandorte sind in **Anlage 3** dargestellt.

(2) Der Auftraggeber stimmt einer Verlagerung eines Ortes der Leistungserbringung innerhalb des Leistungslandes, für das bereits eine Zustimmung besteht, zu, wenn dort nachweislich ein gleiches Sicherheitsniveau gegeben ist und keine für den Auftraggeber geltenden gesetzlichen Bestimmungen gegen diese Verlagerung sprechen. Die Nachweispflicht hierzu liegt bei dem Auftragnehmer.

(3) Bei einer Verlagerung des Ortes der Leistungserbringung in Länder, die Mitglied der EU / EWR sind und über ein diesem Vertrag genügendes und verifiziertes Datenschutzniveau verfügen, für die bisher keine Zustimmung vorliegt, wird der Auftraggeber schriftlich informiert.

(4) Sofern der Auftragnehmer vom Auftraggeber nicht innerhalb einer Frist von vier Wochen nach Zugang der Mitteilung gemäß Absatz 3 über die Verlagerung über Gründe informiert wird, die eine Verlagerung nicht zulassen, gilt die Zustimmung zu dieser Verlagerung seitens des Auftraggebers als erteilt.

(5) Bei einer Verlagerung des Ortes der Leistungserbringung an einen Standort außerhalb der EU/EWR in ein Drittland, wird der Auftragnehmer zuvor die Zustimmung durch den Auftraggeber einholen. Der Auftragnehmer weist in diesem Falle die Einhaltung der diesbezüglichen Vorgaben der DS-GVO nach.

(6) Sollte der Auftragnehmer außerhalb der EU ansässig sein, bestimmt der Auftragnehmer schriftlich einen Vertreter in der Union, der in einem der Mitgliedstaaten niedergelassen sein muss, welcher insbesondere für Aufsichtsbehörden und betroffene Personen bei sämtlichen Fragen im Zusammenhang mit der Einhaltung der Vorgaben der DS-GVO als Anlaufstelle dient. Der Auftragnehmer teilt dem Auftraggeber diesen Vertreter mit.

§ 7 Inanspruchnahme der Dienste weiterer Auftragsverarbeiter

[Anmerkung: Bitte an dieser Stelle zw. Variante 1 und 2 wählen und das nichtzutreffende streichen]

Variante 1:

Eine Weitergabe von Aufträgen im Rahmen der in dem Vertrag vereinbarten Tätigkeiten an Subunternehmer durch den Auftragnehmer erfolgt nicht. Der Auftragnehmer nimmt keine weiteren Auftragnehmer in Anspruch.

Variante 2:

(1) Sofern es dem Auftragnehmer im Rahmen der Zusammenarbeit erforderlich wird, die vertraglich vereinbarten Leistungen unter Einschaltung eines Subunternehmers durchzuführen, hat der Auftragnehmer im Vorfeld eine Liste der zum Zeitpunkt des Abschlusses dieser Vereinbarung tätigen Subunternehmer, zur Verfügung zu stellen. Für die Subunternehmer in **Anlage 4** gilt die Einwilligung für das Tätigwerden von Seiten des Auftraggebers als erteilt.

(2) Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subunternehmern spätestens vier Wochen vor der Hinzuziehung bzw. Ersetzung in Textform, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen bei Vorliegen wichtiger Gründe gegen die Beauftragung Einspruch zu erheben. Widerspricht der Auftraggeber nicht, gilt die Hinzuziehung bzw. die Ersetzung als genehmigt.

(3) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei Post- und Versanddienstleistungen.

(4) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus dieser Vereinbarung dem Subunternehmer zu übertragen. Der Auftragnehmer hat sicherzustellen, dass die in dieser Vereinbarung getroffenen Regelungen, insbesondere auch die Prüf- und Kontrollbefugnisse des Auftraggebers, auch gegenüber dem Subunternehmer gelten und durchgesetzt werden können. Der Auftragnehmer hat den Subunternehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über die datenschutzrelevanten Verpflichtungen des Subunternehmers und deren Umsetzung zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen bzw. direkte Kontrolle bei dem Subunternehmer. Der Auftragnehmer ist gegenüber dem Auftraggeber für die ordnungsgemäße Erfüllung der Leistungen durch die eingeschalteten Subunternehmen verantwortlich.

(5) Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Subunternehmer die nach datenschutzrechtlichen Anforderungen erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat und einhält. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln.

(6) Kommt ein Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Subunternehmers.

§ 8 Mitwirkungs-/Unterstützungspflichten

(1) Der Auftragnehmer unterstützt den Auftraggeber angesichts der Art der Verarbeitung mit geeigneten technischen organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DS-GVO genannten Rechte der betroffenen Person nachzukommen (Informationspflichten/ Transparenz; Recht auf Auskunft; Berichtigungsrecht; Recht auf Löschung; Recht auf Einschränkung der Verarbeitung; Mitteilungsrecht bei Berichtigung und Löschung sowie Einschränkung der Verarbeitung; Recht auf Datenübertragbarkeit; Widerspruchsrecht; Rechte bei automatisierten Einzelfallentscheidungen).

(2) Soweit eine betroffene Person sich in Bezug auf die Wahrung der in Kapitel III der DS-GVO genannten Rechte direkt an den Auftragnehmer wendet, so reagiert der Auftragnehmer nicht selbstständig, sondern wird der Auftragnehmer dies dem Auftraggeber unverzüglich mitteilen und bei der Bearbeitung und Beantwortung des Begehrens im erforderlichen Umfang unterstützen.

§ 9 Unterstützung zur Pflichterfüllung des Auftraggebers

Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Art. 32 bis 36 DS-GVO genannten Pflichten. (Gewährleistung der Sicherheit der Verarbeitung; Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörden; Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person; Datenschutz-Folgenabschätzung und Vorherige Konsultation).

§ 10 Verzeichnis von Verarbeitungstätigkeiten

Der Auftragnehmer führt nach Art. 30 Abs. 2 DS-GVO ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung. Auf Anforderung wird dem

Auftraggeber die für die Übersicht nach Art. 30 DS-GVO notwendigen Angaben durch den Auftragnehmer zur Verfügung gestellt.

§ 11 Nutzungsrechte, Löschung und Rückgabe personenbezogener Daten

(1) Der Auftragnehmer erwirbt keine Rechte an den Daten des Auftraggebers. Zurückbehaltungsrechte des Auftragsverarbeiters an den Daten und etwaig vorhandenen Datenträgern des Auftraggebers sind ausgeschlossen.
(2) Überlassene Datenträger und Dokumente 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. Aufgrund einer Beauftragung durch den Auftraggeber übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien, sofern nicht im Vertrag bereits vereinbart.
(3) Nach Auftragsende sind Daten, Datenträger sowie sämtliche sonstige Materialien (auch Test- und Ausschussmaterial), die im Zusammenhang mit dem Auftragsverhältnis stehen, auf Verlangen des Auftraggebers entweder herauszugeben, aufzubewahren oder zu löschen bzw. datenschutzgerecht zu vernichten, soweit gesetzliche oder anderweitige Aufbewahrungspflichten nicht entgegenstehen.
(4) 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.

§ 12 Sonstige Pflichten des Auftragsverarbeiters

(1) Der Auftragnehmer nennt dem Auftraggeber eine Ansprechperson für im Rahmen der Vereinbarung anfallende Datenschutzfragen. Ein Wechsel der Ansprechperson ist dem Auftraggeber unverzüglich schriftlich mitzuteilen.
(2) Der Auftragnehmer unterrichtet den Auftraggeber umgehend bei Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen, bei Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers in Text- oder Schriftform. Er trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.
(3) Der Auftragnehmer informiert den Auftraggeber über Kontrollmaßnahmen der Aufsichtsbehörden unverzüglich und umfassend, soweit personenbezogene Daten des Auftraggebers betroffen sind.
(4) Der Auftragnehmer benachrichtigt den Auftraggeber unverzüglich, wenn es zu Verletzungen dieser Vereinbarung oder anwendbarer Datenschutzgesetze gekommen ist.
(5) Als Datenschutzbeauftragter ist beim Auftragnehmer derzeit _____ [Name, Kontaktdaten] benannt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich schriftlich mitzuteilen. Der Auftragnehmer gewährleistet, dass die Anforderungen an den Datenschutzbeauftragten und seine Tätigkeit gemäß Art. 38 DS-GVO erfüllt werden. Sofern kein Datenschutzbeauftragter beim Auftragnehmer benannt ist, benennt der Auftragnehmer dem Auftraggeber einen Ansprechpartner.

§ 13 Pflichtennachweis und Unterstützung bei Überprüfungen

(1) Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren und in geeigneter Weise nachzuweisen.
(2) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DS-GVO niedergelegten Pflichten zur Verfügung. Er ermöglicht Überprüfungen – einschließlich Inspektionen –, die vom Auftraggeber oder einer von ihm beauftragten Prüfstelle durchgeführt werden, und trägt zu ihrer Durchführung bei.
(3) Bezüglich der in § 13 Abs. 2 genannten Inspektionen kann sich der Auftraggeber nach 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 Auftragsdatenverarbeitung einschlägigen Datenschutzbestimmungen überzeugen. Liegt ein Verstoß des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen vor, so kann eine darauf bezogene Prüfung auch ohne rechtzeitige Anmeldung vorgenommen werden. Eine Störung des Betriebsablaufs beim Auftragnehmer sollte auch hierbei weitestgehend vermieden werden.

§ 14 Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der betroffenen Person ist der Auftraggeber verantwortlich. Der Auftraggeber wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen geschaffen werden.

(2) Der Auftraggeber wird den Auftragnehmer informieren, wenn er bei der Prüfung von Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Der Auftraggeber wird den Auftragnehmer informieren, wenn er bei der Prüfung nach § 13 Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(4) Der Auftraggeber hat die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten.

(5) Dem Auftraggeber obliegen die aus Artt. 33, 34 DS-GVO resultierenden Informationspflichten gegenüber der Aufsichtsbehörde bzw. der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person.

(6) Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest.

(7) Der Auftraggeber stellt sicher, dass die aus Art. 32 DS-GVO resultierenden Anforderungen bzgl. der Sicherheit der Verarbeitung seinerseits eingehalten werden.

§ 15 Haftung

(1) Auftraggeber und Auftragnehmer haften für den Schaden, der durch eine nicht der DS-GVO entsprechende Verarbeitung verursacht wird gemeinsam im Außenverhältnis gegenüber der jeweiligen betroffenen Person.

(2) Der Auftragnehmer haftet ausschließlich für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der
   a. er den aus der DS-GVO resultierenden und speziell für Auftragsverarbeiter auferlegten Pflichten nicht nachgekommen ist oder
   b. er unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers handelte oder
   c. er gegen die rechtmäßig erteilten Anweisungen des Auftraggebers gehandelt hat.

(3) Soweit der Auftraggeber zum Schadensersatz gegenüber der betroffenen Person verpflichtet ist, bleibt ihm der Rückgriff auf den Auftragnehmer vorbehalten.

(4) Im Innenverhältnis zwischen Auftraggeber und Auftragnehmer haftet der Auftragnehmer für den durch eine Verarbeitung verursachten Schaden jedoch nur, wenn er
   a. seinen ihm speziell durch die DS-GVO auferlegten Pflichten nicht nachgekommen ist oder
   b. unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers oder gegen diese Anweisungen gehandelt hat.

(5) Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

§ 16 Außerordentliches Kündigungsrecht

Der Auftraggeber ist zu einer außerordentlichen Kündigung des Hauptvertrages berechtigt, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Verantwortlichen vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar. Bei einfachen - also weder vorsätzlichen noch grob fahrlässigen - Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

§ 17 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollte die auftragsgemäße Erfüllung des Auftragsgegenstandes gem. § 1 dieses Vertrages beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder ein Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, informiert der Auftragnehmer den Auftraggeber unverzüglich. Der Auftragnehmer wird alle in diesem Zusammenhang Beteiligte unverzüglich darüber informieren, dass die Verfügungsbefugnisse an den Daten ausschließlich beim Auftraggeber liegen.

(2) Bei etwaigen Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag im Hinblick auf die Auftragsverarbeitung gehen die Regelungen dieses Vertrages vor.

(3) Änderungen und Ergänzungen dieses Vertrages und aller seiner Bestandteile einschließlich der Kündigung oder etwaiger Zusicherungen des Auftragnehmers bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Dies kann auch in einem elektronischen Format erfolgen.
(4) Es gilt deutsches Recht. Gerichtsstand ist der Sitz des Auftraggebers.
(5) Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen der Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Bestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt.

IT- Regelungen [Anmerkung: Dieser Abschnitt ist zu streichen, wenn keine Fernzugriffe erfolgen.]
Für die Durchführung von Fernzugriffen bei der Prüfung und/oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen oder bei Fernzugriffen für andere Dienstleistungen gelten ergänzend folgende Regelungen:

§ 18 Organisatorische Regelungen für Wartungsarbeiten

(1) Die Verantwortlichkeit für die Durchführung der Wartung verbleibt beim Systembetreiber (Auftraggeber). Er ist damit jederzeit im Rahmen des Wartungsauftrages gegenüber dem Auftragnehmer weisungsberechtigt.
(2) Der Auftragnehmer wird von den ihm eingeräumten Zugriffsrechten auf automatisierte Verfahren oder von Datenverarbeitungsanlagen des Auftraggebers nur in dem Umfang - auch in zeitlicher Hinsicht - Gebrauch machen, wie dies für die ordnungsgemäße Durchführung der beauftragten Wartungs- und Prüfungsarbeiten notwendig ist.
(3) Der Systemverwalter des Auftraggebers wird zur Wahrnehmung seiner Überwachungspflicht und zur Beherrschung der erforderlichen technischen Maßnahmen durch den Auftragnehmer qualifiziert.

§ 19 Zusätzliche technische Maßnahmen im Falle der Fernwartung

(1) Der Verbindungsaufbau zum Wartungsunternehmen (Auftragnehmer) erfolgt ausschließlich auf Initiative des Auftraggebers (Abstimmung des Wartungszeitpunktes), so dass die Wartungsarbeiten nur mit Wissen und Willen des Auftraggebers durchgeführt werden können.
(2) Sicherung der Authentizität und Identifikation beim Verbindungsaufbau:
   a. Breitbandanbindung (Point-to-Multi-Point-Verbindung)
      - Der Verbindungsaufbau über einen Breitbandanschluss muss per VPN über die zentralen VPN-Gateways des Geschäftsbereichs IT des UKD erfolgen, für die ein Hochgeschwindigkeitszugang zum Internet über das X-WiN des DFN zur Verfügung steht
      - Es soll eine starke Authentisierung verwendet werden. Vom BSI empfohlen ist eine Kombination aus zwei Authentisierungstechniken (Zwei-Faktor-Authentisierung). Beide eingesetzten Authentisierungstechniken müssen sich auf dem Stand der Technik befinden.
   b. Wählverbindung (Point-to-Point-Verbindung)
      - Der Verbindungsaufbau über eine Wählverbindung (ISDN) muss über den zentralen Einwahlrouter des Medizinischen Rechenzentrums erfolgen, für den ein mehrkanaliger S2M-Anschluss zur Verfügung steht
      - Die Authentisierung erfolgt über die einwählende Telefonnummer und einen vereinbarten Usernamen
      - Das Wartungspasswort
        - ist für jeden Fernwartungsvorgang neu zu vereinbaren (Löschen des Accounts beim Auftraggeber nach Beendigung der Wartung); **oder**
        - es ist verschlüsselt über die Leitung zu übertragen.
(3) Sicherung der Integrität der Daten des Auftraggebers:
      - Müssen im Ausnahmefall zur Realisierung der Wartungsaufgabe Patientendaten in die Fernwartungszentrale des Auftragnehmers (und zurück) übertragen werden, so ist zur Verhinderung von Abhören, Datenverfälschung oder Datenverlust eine Verschlüsselung dieser Daten während der Übertragung erforderlich (Hardware- oder Software-Verschlüsselung). Das eingesetzte Verschlüsselungsverfahren und das Schlüsselmanagement sind als Anlage zum Wartungsvertrag zu dokumentieren.
      - Eine VPN Verbindung erfolgt verschlüsselt mittels 3DES Verschlüsselung (Data Encryption Standard) oder einem höheren Authentisierungsverfahren (z.B. AES).

- Der Auftragnehmer hat alle in seine Fernwartungszentrale übernommenen personenbezogenen Daten nach Abschluss jedes Wartungsvorganges unverzüglich und datenschutzgerecht zu löschen.

§ 20 Protokollierung / Nachweispflicht bei der Wartung bzw. Fernwartung

Wartungsaktivitäten an datenschutzrelevanten IT-Systemen sind nachweispflichtig.

- Der Auftragnehmer hat alle Aktivitäten und den Grund der Fernwartungsarbeiten nachweisbar zu dokumentieren.
- Mindestangaben im Protokoll müssen sein:
  - Grund der Wartung
  - Zeitpunkt
  - durchführende Person
  - Wartungsaktivitäten
  - durchgeführte Zugriffe auf den Echtdatenbestand (personenbezogene Daten).
- Zum Nachweis der Wartungsarbeiten sollte vorzugsweise die Verwendung einer determinierten Protokollierungs-Software vereinbart werden. Im Ausnahmefall ist eine manuelle Protokollierung zulässig.
- Die Protokolldateien werden beim Auftraggeber mindestens ein Jahr datenschutzgerecht aufbewahrt.

Im Falle der Fernwartung gilt zusätzlich:

- Der Auftragnehmer hat dem Systemverwalter des Auftraggebers die zu erfolgende Fernwartung schriftlich per E-Mail oder Fax anzukündigen.
- Der Auftragnehmer hat dem Systemverwalter des Auftraggebers die erfolgte Fernwartung schriftlich per E-Mail oder Fax als beendet zu erklären und parallel dazu einen Statusbericht abzugeben. Der Statusbericht muss in schriftlicher Form erfolgen und enthält Protokolle und / oder Dokumentationen.

_____

[Ort], Unterschriften Auftragnehmer

_____

[Ort], Unterschriften Auftraggeber

Anlage 1: [Anmerkung: Anlage nur erforderlich, wenn Patientendaten betroffen sind; ansonsten streichen, bitte Nummerierung der Anlage im Dokument entsprechend anpassen!] Verpflichtung zur Geheimhaltung nach § 203 StGB
Anlage 2: Technische und organisatorische Maßnahmen des Auftragnehmers gemäß Art. 32 DS-GVO
Anlage 3: Liste der zum Zeitpunkt der Auftragserteilung vereinbarten Leistungsstandorte des Auftragnehmers
Anlage 4: Liste der zum Zeitpunkt der Auftragserteilung tätigen Subunternehmen inkl. Leistungsstandorte