Vertrag zur Auftragsverarbeitung

gem. Art. 28 (1) DSGVO

zwischen

› im Folgenden: „AUFTRAGGEBER“ ‹

und

apoplex medical technologies GmbH
Zweibrücker Str. 185
D-66954 Pirmasens

› im Folgenden: „AUFTRAGNEHMER“ ‹

Präambel

Der AUFTRAGGEBER möchte mit dem AUFTRAGNEHMER in eine Geschäftsbeziehung eintreten und beabsichtigt, dem AUFTRAGNEHMER zur Gewinnung medizinisch relevanter Informationen EKG-Rohdaten zu übertragen. Bei den verarbeiteten Daten handelt es sich um Aufzeichnungen von EKG-Geräten (Elektrokardiographie). Betroffene Personen sind dabei die Patienten des AUFTRAGGEBERs, für welche die entsprechende Analyse beauftragt wird. (Kategorie betroffener Personen – Art. 28(3) DSGVO)

Es handelt sich dabei grundsätzlich um personenbezogene Daten, die einen Rückschluss auf den Gesundheitszustand der Patienten zulassen. Entsprechend ist davon auszugehen, dass sich die Auftragsverarbeitung im Wesentlichen auf besondere Kategorien personenbezogener Daten gem. Art. 9 DSGVO bezieht. (Art der personenbezogenen Daten – Art. 28(3) DSGVO)

Die Verarbeitung von Nutzer- oder Mitarbeiterdaten ist grundsätzlich nicht Bestandteil der Beauftragung. Um das Ziel der Auftragsverarbeitung erreichen zu können, bedarf es grundsätzlich nur der Parameter Alter und Geschlecht sowie der EKG-Rohdaten, welche keine Rückschlüsse auf die Identität des Patienten zulassen. Entsprechend ist es nicht notwendig, Daten wie Name, Vorname oder Adresse des Patienten dem AUFTRAGNEHMER zu übermitteln. Die zur Verarbeitung notwendigen Daten und

Informationen werden daher pseudonymisiert zur Verfügung gestellt. Daher wird als weiterer Parameter eine Pseudonymisierungs-ID an den AUFTRAGNEHMER übertragen.
Die vom AUFTRAGNEHMER übernommenen Tätigkeiten können entsprechend der nachfolgenden Aufzählung zusammengefasst werden („Gegenstand der Verarbeitung“ - Art. 28 (3) DSGVO):

- Analyse von EKG-Rohdaten des AUFTRAGGEBERS
- Übertragung von Analyseergebnissen an den AUFTRAGGEBER unter Bezugnahme auf eine Pseudonymisierungs-ID
- Technische Unterstützung des AUFTRAGGEBERS, insbesondere per Fernzugriff

Der AUFTRAGGEBER verfolgt damit das Ziel, insbesondere fremdes medizinisches Wissen zu nutzen, das in der eigenen Organisation limitiert oder nicht verfügbar ist. Davon verspricht sich der AUFTRAGGEBER ferner eine hohe Qualität bei der Durchführung der Maßnahme und damit verbunden eine Verbesserung der Behandlungsmöglichkeiten durch die Gewinnung zusätzlicher behandlungsrelevanter Informationen und Werte. Darüber hinaus werden dabei Ressourcen genutzt, die dem AUFTRAGGEBER im dafür notwendigen Umfang sonst nicht zur Verfügung stehen. Zusätzlich verspricht sich der AUFTRAGGEBER eine gesetzeskonforme Umsetzung der geleisteten Tätigkeiten. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der vorbeschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit den Tätigkeiten des AUFTRAGNEHMERS für den AUFTRAGGEBER in Zusammenhang stehen und bei denen Mitarbeiter des AUFTRAGNEHMERS oder durch den AUFTRAGNEHMER beauftragte Dritte mit personenbezogenen Daten des AUFTRAGGEBERS in Berührung kommen können.

§ 1
Begriffsbestimmungen

1 Personenbezogene Daten: „*Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann*“ (Art. 4 Nr.1 DSGVO).

2 Auftragsverarbeiter (Auftragnehmer): „*Natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet*“ (Art. 4 Nr. 8 DSGVO).

3 Verarbeitung: Verarbeitung bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten im Sinne von Art. 4 Nr. 2 DSGVO.

4 Verantwortlicher: *„Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedsstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden“* (Art. 4 Nr. 7 DSGVO).

5 Dritter: *„Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten“* (Art. 4 Nr. 10 DSGVO).

6 Weisungen: Weisungen sind die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des AUFTRAGNEHMERs mit personenbezogenen Daten gerichtete mündliche oder schriftliche Anordnung des AUFTRAGGEBERs. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.

7 Technische und organisatorische Maßnahmen: Technische und organisatorische Maßnahmen sind Vorkehrungen, die getroffen werden müssen, um die Einhaltung und Überwachung des Datenschutzes zu gewährleisten. Die für diesen Vertrag maßgeblichen technischen und organisatorischen Maßnahmen sind im **Anhang 1** zu dieser Vereinbarung festgehalten.

8 Pseudonymisierung: „Pseudonymisierung“ ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

9 EKG: Elektrokardiogramm

10 Drittland: Ein Land, welches sich außerhalb der EU/EWR befindet.

§ 2
Vertragsgegenstand

Gegenstand dieser Vereinbarung ist die Verarbeitung personenbezogener Daten durch den AUFTRAGNEHMER im Auftrag des AUFTRAGGEBERS. Die Verarbeitung umfasst die Tätigkeiten, die unter dem Abschnitt „Präambel“ aufgeführt sind (insbesondere die Analyse von EKG-Rohdaten). Dabei sollen in erster Linie die Verfügbarkeit sowie die Vertraulichkeit und Integrität verarbeiteter personenbezogener Daten sichergestellt werden (Art und Zweck der Verarbeitung – Art. 28 (3) DSGVO).
Die Tätigkeit der Auftragsverarbeitung beschränkt sich auf die Auswertung von EKG-Rohdaten und die Gewinnung medizinisch-relevanter Informationen im Rahmen dieser Analyse. Verarbeitet werden damit pseudonymisierte EKG-Daten. (Art der personenbezogenen Daten – Art. 28 (3) DSGVO).
Wie ebenfalls bereits im Abschnitt „Präambel“ nachzulesen ist, dient die Auftragsverarbeitung dem Zweck, fremde Ressourcen zu nutzen, die in der Organisation des AUFTRAGGEBERS nicht in ausreichendem Maß verfügbar sind, auf diese Weise behandlungsrelevante Informationen zu gewinnen und dabei erforderliche Maßnahmen hinsichtlich Datenschutzes und Datensicherheit zu gewährleisten. Die Verarbeitung beschränkt sich dabei, wie vorhergehend bereits erwähnt, auf die Auswertung von EKG-Rohdaten und die Gewinnung medizinisch-relevanter Informationen im Rahmen der Analyse. („Umfang, Art und Zweck der Datenverarbeitung“ - Art. 28(3) DSGVO).

Der AUFTRAGGEBER ist im Rahmen dieses Vertrages für die Einhaltung der allgemeinen gesetzlichen und datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den AUFTRAGNEHMER sowie für die Rechtmäßigkeit der Datenverarbeitung, allein verantwortlich („Verantwortlicher“ gem. Art.4 Nr. 7 DSGVO).

Zur Ausführung der übertragenen Aufgaben ist es notwendig personenbezogene Daten in der Art zu verarbeiten, dass die Ergebnisse der Analyse unter Zuordnung zum Pseudonymisierungsschlüssel an den AUFTRAGGEBER übertragen werden. Eine Verarbeitung der EKG-Rohdaten erfolgt nicht nur beiläufig, sondern stellt den Hauptzweck der Auftragsverarbeitung dar. Daher ist davon auszugehen, dass entsprechend Art. 28(1) DSGVO eine Verarbeitung im Auftrag eines Verantwortlichen erfolgt.
Hinsichtlich eventueller weiterer Tätigkeiten im Zusammenhang mit der Auftragsverarbeitung hat der AUFTRAGNEHMER mit der gleichen Sorgfalt zu verfahren.
Betroffene Personen sind grundsätzlich alle Personen des in der Präambel genannten Personenkreises, nämlich die Patienten des AUFTRAGGEBERS, dessen EKG-Rohdaten analysiert werden. Bei den verarbeiteten personenbezogenen Daten handelt es sich um besondere Kategorien von Daten, nämlich um Gesundheitsdaten. („Art der verarbeiteten personenbezogenen Daten und Kategorien betroffener Personen“ - Art. 28(3) DSGVO). Die Berichtigung, Sperrung oder Löschung von Daten erfolgt grundsätzlich durch den AUFTRAGGEBER. (Pflichten des Verantwortlichen – Art.°28(3)° DSGVO). Die Resultate werden für einen kurzen Zeitraum beim AUFTRAGNEHMER gespeichert, damit im Falle einer Fehlübermittlung der AUFTRAGGEBER die Daten nochmals abfragen kann oder technische Probleme identifiziert werden können. Nach 3 Monaten werden sowohl Rohdaten wie auch Analysedaten beim AUFTRAGNEHMER automatisiert gelöscht.

§ 3
Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, Art der Daten und Kategorien der Betroffenen

Die Datenverarbeitung im Auftrag erfolgt zum Zwecke der Erstellung von Analysen von EKG-Rohdaten der Patienten des AUFTRAGGEBERS. Der Gegenstand der vom AUFTRAGNEHMER geschuldeten Dienst- und/oder Werkleistungen sind in der Leistungsbeschreibung der Schlaganfall-Risiko-Analyse **SRA®** konkret beschrieben.
Im Rahmen der Auftragsdurchführung werden nachfolgende Daten durch den AUFTRAGNEHMER verarbeitet:

a. **Personenstammdaten**, insbesondere Daten der Ansprechpartner und Verantwortlichen beim AUFTRAGGEBER. Dazu gehören Anrede einschließlich des akademischen Grades, Titel, Vorname, Nachname, Zugehörigkeit zum AUFTRAGGEBER und Funktion

b. **Kommunikations- und Adressdaten** (im Zusammenhang mit den Ansprechpartnern beim AUFTRAGGEBER) insbesondere Telefon, E-Mail, Handy- und/oder Faxnummer

c. **Vertragsstammdaten**, insbesondere Namen und Funktion der Unterzeichner und der aufgeführten Ansprech- und Vertragspartner

d. **Patientendaten** (Verarbeitung ist Haupttätigkeit i.S. dieses AV-Vertrags), insbesondere Geschlecht, Alter, EKG-Rohdaten, Analyseergebnisse, Pseudonymisierungs-ID

e. **Vertragsabrechnungs-, Zahlungs- und Bankverbindungsdaten** des AUFTRAGGEBERS

Die Kategorien der Betroffenen umfassen:
Die Haupttätigkeit der hier geregelten Auftragsverarbeitung zielt auf die Analyse von EKG-Rohdaten. Betroffene sind demnach Patienten des AUFTRAGGEBERS. Im Rahmen der Nebentätigkeiten, wie Kommunikation und Abstimmung mit dem AUFTRAGGEBER sowie der Rechnungsstellung, sind auch Beschäftigte, Zeichnungsberechtigte, Inhaber und Geschäftsführer des AUFTRAGGEBERS Betroffene der beim AUFTRAGNEHMER durchgeführten Datenverarbeitung.

Die Verarbeitung erfolgt an den Zweck der jeweiligen Aufgabe angepasst elektronisch oder in Papierform. Der AUFTRAGNEHMER wird die Daten nicht zu eigenen Zwecken erheben, verarbeiten oder nutzen.

Der AUFTRAGNEHMER wird die vertraglichen Leistungen in der Bundesrepublik Deutschland erbringen, etwaige Unterauftragnehmer in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR). Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des AUFTRAGGEBERS und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artikel 44 ff. EU- DSGVO erfüllt sind. Dies gilt auch für Unterauftragnehmer.

§ 4
Pflichten des AUFTRAGNEHMERS

1 Der AUFTRAGNEHMER darf die ihm im Rahmen der Durchführung seiner Verpflichtungen aus dem Auftragsverhältnis überlassenen oder sonst bekannt gewordenen personenbezogenen Daten nur im Rahmen der in den v.g. Verträgen vereinbarten Aufgaben/Tätigkeiten und entsprechend den Weisungen des AUFTRAGGEBERS erheben, verarbeiten und/oder nutzen. Aufgrund seiner Datenverantwortlichkeit kann der AUFTRAGGEBER während der Laufzeit und nach Beendigung der Beauftragung der oben beschriebenen Dienstleistungen die Berichtigung, Löschung, Sperrung und Herausgabe von Daten verlangen (Rückgabe und Löschung von Daten – Art. 28 (3g) DSGVO).

2 Der AUFTRAGNEHMER verpflichtet sich, die überlassenen Daten zu keinem anderen Zweck als in dieser Vereinbarung in den entsprechenden Beauftragungen geregelt zu nutzen, diese keinem Dritten zu überlassen oder die Daten über die Dauer der in dieser Vereinbarung und/oder in der Beauftragung geregelten Verarbeitung hinaus zu besitzen oder zu speichern. Der AUFTRAGNEHMER ist verpflichtet, überlassene Daten unverzüglich nach Aufforderung des AUFTRAGGEBERs, spätestens jedoch 3 Monate nach Ablauf des jeweiligen Projekts oder der jeweiligen Aktion, aus dem Produktivsystem zu löschen und versichert, keine weiteren Daten von dem AUFTRAGGEBER auf Produktivsystemen gespeichert zu haben und/oder diese weiter zu nutzen. Zurückbehaltungsrechte bestehen nicht. Gesetzliche Aufbewahrungsfristen bleiben unberührt. Der AUFTRAGNEHMER hat auf Anforderung vom AUFTRAGGEBER unverzüglich eine Bestätigung über die Löschung von Daten zu übermitteln. Überlassene Datenträger sind nach Beendigung der für den AUFTRAGGEBER erbrachten Dienstleistung / des Auftrags an diesen zurückzugeben (Rückgabe und Löschung von Daten – Art. 28 (3g) DSGVO).

3 Der AUFTRAGNEHMER sichert die Umsetzung und Einhaltung der technischen und organisatorischen Maßnahmen zu („technische und organisatorische Maßnahmen“ - Art. 25 und Art. 32 DSGVO i.V.m. Art. 28 (1) und Art. 28 (3c) DSGVO), die erforderlich sind, um nach dem Stand der Technik ein für die Verarbeitung entsprechender personenbezogener Daten ausreichendes Datenschutzniveau zu gewährleisten. Der AUFTRAGNEHMER wird hierzu in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des AUFTRAGGEBERS vor Missbrauch und Verlust treffen, die den Forderungen der gesetzlichen Vorgaben, insbesondere der DSGVO Art. 25 und Art. 32 DSGVO entsprechen. Dies beinhaltet insbesondere:

› Unbefugte vom Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, auszuschließen,

› die Nutzung der Datenverarbeitungssysteme durch Unbefugte zu verhindern,

› sicherzustellen, 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,

- sicherzustellen, 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,

- sicherzustellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des AUFTRAGGEBERs verarbeitet werden können,

- sicherzustellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind,

- sicherzustellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Die Darstellung spezieller, durch den AUFTRAGNEHMER im Einzelnen vorgenommenen Maßnahmen wird dieser Vereinbarung als **Anhang 1** beigefügt.

1 Der AUFTRAGNEHMER ist zur Mitwirkung bei der Erstellung des Verzeichnisses von Verarbeitungstätigkeiten gem. Art. 30 (1) DSGVO durch den AUFTRAGGEBER verpflichtet und hat ihm, soweit erforderlich, hierzu die notwendigen Angaben zu den Verarbeitungsvorgängen und den zugriffsberechtigten Personen zu machen. Der AUFTRAGNEHMER ist als Auftragsverarbeiter darüber hinaus verpflichtet ein Verzeichnis über Verarbeitungstätigkeiten gem. Art. 30 (2) DSGVO zu führen.

2 Die Auftragsverarbeitung ist grundsätzlich vom AUFTRAGNEHMER selbst zu erbringen. Die Beauftragung Dritter ist nur mit vorheriger schriftlicher Zustimmung des AUFTRAGGEBERs zulässig (Art. 28 (2) DSGVO). Der AUFTRAGNEHMER stellt sicher, dass die mit der Verarbeitung der Daten des AUFTRAGGEBERs befassten Mitarbeiter gemäß Art. 28 (3b) DSGVO verpflichtet und in die einschlägigen Schutzbestimmungen eingewiesen worden sind (Art. 39 (1b) DSGVO). Die Vergabe von Aufträgen an Unterauftragsverarbeiter (Unterauftragsnehmer) ist in einer Zusatzvereinbarung zu regeln, soweit dies erforderlich wird.

3 Der AUFTRAGNEHMER hat, soweit das nach den Vorschriften der DSGVO, des Bundesdatenschutzgesetzes (BDSG-Neu) oder anderer einschlägiger Rechtsvorschriften erforderlich ist, einen betrieblichen Datenschutzbeauftragten zu bestellen und ihn als Ansprechpartner dem AUFTRAGGEBER zu benennen. Dies kann über die Ergänzung der Namensliste im **Anhang 2** dieses AV-Vertrags erfolgen.

4 Datenschutzrechtliche Probleme bei der Auftragsverarbeitung, die eine Verletzung der Datenschutzgesetze darstellen oder darstellen können, sind dem AUFTRAGGEBER unverzüglich mitzuteilen („Information über Verstöße“ - Art. 28 (3) S.3 DSGVO).

5 Der AUFTRAGNEHMER darf grundsätzlich seine Mitarbeiter im Rahmen der technischen Unterstützung auch von anderen Standorten als dem Sitz des Unternehmens auf die Systeme

des AUFTRAGGEBERS zugreifen lassen. Er verpflichtet sich, dabei die Einhaltung notwendiger technischer und organisatorischer Maßnahmen sicherzustellen.

6 Datenträger, die der AUFTRAGGEBER dem AUFTRAGNEHMER überlässt, sind als solche zu kennzeichnen und verbleiben im Eigentum des AUFTRAGGEBERS. Ferner sichert der AUFTRAGNEHMER zu, dass die Datenbestände, die die Auftragsverarbeitung für den AUFTRAGGEBER betreffen, strikt zu trennen sind von anderen Datenbeständen des AUFTRAGNEHMERS oder Dritter.

7 Soweit es im Rahmen der Geschäftsbeziehung erforderlich werden sollte, dass der AUFTRAGNEHMER nach den Vorgaben des AUFTRAGGEBERS Daten berichtigen und löschen sollte, wird der AUFTRAGGEBER den AUFTRAGNEHMER gesondert anweisen („Verarbeitung auf Weisung des Verantwortlichen“ - Art. 28 (3a) DSGVO).

8 Entsprechend der Vorgabe des Art. 28 (3f) DSGVO ist der AUFTRAGNEHMER zur Unterstützung des Verantwortlichen (AUFTRAGGEBER), hinsichtlich der Bestimmungen der Art. 32 bis 36 DSGVO, soweit möglich und notwendig, verpflichtet. Ein entsprechender Mehraufwand ist dem AUFTRAGNEHMER zu vergüten.

9 Der AUFTRAGNEHMER stellt dem Verantwortlichen auf Anforderung alle erforderlichen Informationen zum Nachweis der Einhaltung der Bestimmungen des Art. 28 DSGVO zur Verfügung („Zurverfügungstellung von Informationen“ – Art. 28 (3h) DSGVO). Dabei ist besonders darauf zu achten, dass sicherheitsrelevante Informationen nicht die Geschäftsräume des AUFTRAGNEHMERS, gleich in welcher Form, verlassen dürfen.

10 Der AUFTRAGNEHMER ist grundsätzlich verpflichtet, personenbezogene Daten nach Maßgabe der Weisungen des AUFTRAGGEBERS zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken. Da das eingesetzte System vollautomatisiert arbeitet ist ein manueller Eingriff nicht möglich, jedoch kann eine Berichtigung darüber erfolgen, dass der AUFTRAGGEBER die zu verarbeitenden Daten in berichtigter Form erneut sendet. Hinsichtlich der Haupttätigkeit erfolgt die Verarbeitung in pseudonymisierter und vollautomatisierter Art und Weise mit anschließender, ebenfalls automatisierter Übertragung der Analyseergebnisse zum AUFTRAGGEBER. Die anschließende Löschung der verarbeiteten Daten und der Resultate ist ebenfalls automatisiert, sodass hinsichtlich der Haupttätigkeit keine gesonderte Löschung, Berichtigung oder Sperrung erfolgen kann. Die Verarbeitung findet nicht nur automatisiert und pseudonymisiert statt, sie benötigt auch nur einen sehr geringen Zeitaufwand. Hinsichtlich weiterer verarbeiteter Daten, insbesondere auch im Zusammenhang mit den Tätigkeiten, die nicht Haupttätigkeit der in diesem Vertrag behandelten Auftragsverarbeitung sind, sind die entsprechenden Pflichten uneingeschränkt einzuhalten.

11 Soweit ein Betroffener an den AUFTRAGNEHMER mit einer Aufforderung zur Berichtigung, Löschung oder Einschränkung der Verarbeitung herantritt oder der AUFTRAGNEHMER aus anderen Gründen der Auffassung ist, dass bestimmte personenbezogene Daten vom AUFTRAG-GEBER zu berichtigen oder zu löschen sind oder deren Verarbeitung einzuschränken ist, wird der AUFTRAGNEHMER den AUFTRAGGEBER unverzüglich hierüber in Textform unterrichten. Der AUFTRAGGEBER wird dem AUFTRAGNEHMER dann die erforderlichen Weisungen erteilen.

12 Soweit der AUFTRAGNEHMER seine Leistung in den Räumlichkeiten oder unter Zugriff auf die Systeme des AUFTRAGGEBERS erbringt, unterliegt er den Kontrolleinrichtungen des AUFTRAGGEBERS (insbesondere Zutritts-, Zugangs- und Zugriffskontrolle).

13 Bei der E-Mail-Kommunikation werden die Vertragsparteien die Vertraulichkeit beachten, indem sie vertrauliche Informationen gegen unberechtigte Kenntnisnahme oder Manipulationen schützen. Hierzu können die Vertragsparteien entsprechende technische Maßnahmen, wie z.B. Verschlüsselungs- und Signaturverfahren, abstimmen.

14 Der AUFTRAGNEHMER ist nicht befugt, ohne schriftliche Einwilligung des AUFTRAGGEBERS Hard- oder Software an die Systeme des AUFTRAGGEBERS anzuschließen oder darauf zu installieren.

15 Dem AUFTRAGNEHMER ist es nicht gestattet, personenbezogene Daten in Systeme Dritter einzuspielen. Dies gilt auch für Testzwecke.

16 Der AUFTRAGNEHMER kontrolliert die Einhaltung der Bestimmungen dieser Vereinbarung mittels regelmäßiger Prüfungen in Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere auf die Einhaltung und ggf. die Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.

17 Die Herstellung von Datenportabilität und die Erteilung von Auskünften an betroffene Personen und/oder Aufsichtsbehörden im Zusammenhang dieses AV-Vertrages schuldet der AUFTRAGNEHMER grundsätzlich nicht. Soweit er zu derartigen Handlungen gesetzlich verpflichtet ist, sind diese durch den AUFTRAGGEBER gesondert zu vergüten. Eine solche Vergütung beläuft sich auf die tatsächlich angefallenen Kosten. Den Zeitaufwand hat der AUFTRAGNEHMER dem AUFTRAGGEBER nachzuweisen. Handlungen werden dabei nur auf Grundlage dokumentierter Weisungen des AUFTRAGGEBERS erbracht. Die Dokumentation erfordert insoweit jedenfalls Textform.

18 Der AUFTRAGNEHMER unterrichtet den AUFTRAGGEBER unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf die Erfüllung von Aufgaben nach diesem AV-Vertrag beziehen und der AUFTRAGNEHMER nicht aus rechtlichen, gesetzlichen oder tatsächlichen Gründen an einer Mitteilung gegenüber dem AUFTRAGGEBER gehindert ist. 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.

19 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 Erfüllung von Aufgaben nach diesem AV-Vertrag beim AUFTRAGNEHMER ausgesetzt ist, hat ihn der AUFTRAG-NEHMER nach besten Kräften zu unterstützen.

20 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 Personen gewährleistet wird.

21 Der AUFTRAGNEHMER erstattet in allen Fällen dem AUFTRAGGEBER eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des AUFTRAGGEBERS oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind (Selbstanzeigepflicht) bzw. die in den Artikeln 32 bis 36 DSGVO genannten Pflichten verletzt worden sind.

22 Es ist bekannt, dass nach Artikel 34 DSGVO Informationspflichten gegenüber den betroffenen Personen bestehen, sofern durch Fehlverhalten des AUFTRAGNEHMERS der Schutz ihrer personenbezogenen Daten verletzt worden ist. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem AUFTRAGGEBER mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des AUFTRAGGEBERS. Der AUFTRAGNEHMER hat im Benehmen mit dem AUFTRAGGEBER angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Der AUFTRAG-NEHMER ist verpflichtet, den AUFTRAGGEBER im Rahmen seiner Informationspflicht zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.

23 AUFTRAGNEHMER und AUFTRAGGEBER nehmen zur Kenntnis, dass eine nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erfolgte Mitteilung mit einem Bußgeld gemäß Artikel 83 Absätze 2) und 4) DSGVO geahndet werden kann.

24 Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der AUFTRAG-NEHMER diese umgehend dem AUFTRAGGEBER. Der AUFTRAGGEBER meldet dann entsprechend Artikel 33 DSGVO unverzüglich der zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

§ 5
Vereinbarung zur Wahrung des Berufsgeheimnisses nach § 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.

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. Unterauftragnehmer), 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 ist berechtigt, Unterauftragnehmer zur Vertragserfüllung heranzuziehen. Im Ausland dürfen Unterauftragnehmer zur Vertragserfüllung nur dann herangezogen werden, wenn der dort bestehende Schutz der Geheimnisse dem Schutz im Inland vergleichbar ist.

4 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, zur Geheimhaltung verpflichten. Der AUFTRAGNEHMER wird ferner etwaige Unterauftragnehmer dazu verpflichten, sämtliche von diesen eingesetzten Personen und etwaige weitere Unterauftragnehmer, die bestimmungsgemäß mit Geheimnisschutzdaten in Berührung kommen oder bei denen dies nicht auszuschließen ist, nach den zuvor genannten Grundsätzen zur Verschwiegenheit zu verpflichten und über die Folgen einer Pflichtverletzung zu belehren.

5 Des Weiteren werden Unterauftragnehmer, über das bestehende Schweigerecht gemäß § 53a StPO sowie den Beschlagnahmeschutz gemäß § 97 StPO informiert; dies beinhaltet auch den Hinweis bzgl. des Rechts des Berufsgeheimnisträgers, über dieses Recht zu entscheiden und der damit verbundenen Pflicht des AUFTRAGNEHMER, unverzüglich den AUFTRAGGEBER bzgl. der Wahrnehmung dieser Rechte zu kontaktieren.

6 Der AUFTRAGNEHMER wird darauf hingewiesen, dass Daten, die er im Auftrag eines Berufsgeheimnisträgers verarbeitet u. U. dem Zeugnisverweigerungsrecht von sogenannten mitwirkenden Personen unterliegen (§ 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.

7 Der AUFTRAGNEHMER wird darauf hingewiesen, dass die in seinem Gewahrsam befindlichen 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.

§ 6
Zuwiderhandlungen

Verstößt der AUFTRAGNEHMER gegen diese Vereinbarung, behält sich der AUFTRAGGEBER vor, diesen Vertrag ohne Einhaltung einer Kündigungsfrist außerordentlich zu kündigen.

§ 7
Rechte und Pflichten des Verantwortlichen (Art. 28 (3) DSGVO)

1 Der AUFTRAGGEBER ist im Rahmen der Auftragsverarbeitung für die Einhaltung der datenschutzrechtlichen Bestimmungen und damit der Zulässigkeit der Datenverarbeitung sowie der Wahrung der Rechte der Betroffenen allein verantwortlich. Der AUFTRAGNEHMER unterstützt den Verantwortlichen jedoch bei der Wahrnehmung der Rechte der Betroffenen (Art. 28 (3e) DSGVO).

2 Der AUFTRAGGEBER behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, welches er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der AUFTRAGNEHMER nur nach vorheriger Zustimmung durch den AUFTRAGGEBER erteilen.

3 Der AUFTRAGGEBER ist allein für die Pseudonymisierung der zu verarbeiteten Daten verantwortlich.

4 Mündliche Weisungen wird der AUFTRAGGEBER unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen.

5 Der AUFTRAGNEHMER hat den AUFTRAGGEBER unverzüglich darauf aufmerksam zu machen, wenn eine vom AUFTRAGGEBER erteilte Weisung seiner Meinung nach gegen die DSGVO bzw. das BDSG-Neu oder eine andere Vorschrift über den Datenschutz verstößt. Der AUFTRAGNEHMER ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen beim AUFTRAGGEBER bestätigt oder geändert wird.

6 Der AUFTRAGGEBER hat sicher zu stellen, dass ausschließlich die hierzu von ihm ermächtigten Personen Mitarbeitern des AUFTRAGNEHMERS Weisungen erteilen. Die weisungsberechtigten Personen beim AUFTRAGGEBER sind der Namensliste zu entnehmen, die diesem Vertrag als Anhang beigefügt ist. Veränderungen dieses Personenkreises sind dem AUFTRAGNEHMER unaufgefordert mitzuteilen.

7 Empfänger von Weisungen beim AUFTRAGNEHMER sind die Mitglieder der Geschäftsführung oder die dafür benannten Mitarbeiter. Soweit einzelne Mitarbeiter als Empfänger von Weisungen fungieren, sind diese schriftlich in der Namensliste, die dem Vertrag als **Anhang 2** beigefügt ist, zu benennen.

8 Änderungen der Kontaktpersonen sind dem anderen unverzüglich schriftlich mitzuteilen.

9 Der AUFTRAGGEBER ist für die Speicherung und Archivierung sowohl der EKG-Rohdaten wie auch der an ihn übertragenen Analysedaten und Informationen, also der Ergebnisse der

Auftragsverarbeitung, allein verantwortlich. Eine Aufbewahrungs- oder Archivierungspflicht beim AUFTRAGNEHMER besteht nicht.

10 Der AUFTRAGGEBER wird den AUFTRAGNEHMER von Fehlern beim Ergebnis der Auftragsverarbeitung unverzüglich in Kenntnis setzen.

11 Dem Verantwortlichen (AUFTRAGGEBER) obliegen die Informationspflichten, die sich aus Art. 15 DSGVO ergeben.

12 Der AUFTRAGGEBER ist verpflichtet alle erforderlichen technischen und organisatorischen Maßnahmen dem Stand der Technik gemäß umzusetzen um bei der Datenübertragung an den AUFTRAGNEHMER eine Gefährdung für dessen Systeme und Daten (z.B. durch Viren oder Malware) auszuschließen.

§ 8
Kontrollrechte

1 Der AUFTRAGGEBER ist berechtigt, die Einhaltung der Bestimmungen dieser Vereinbarung durch Kontrollen zu überprüfen, insbesondere hinsichtlich der Einhaltung der Vorschriften zum Datenschutz sowie der Gewährleistung einer angemessenen Datensicherheit im Sinne dieser Vereinbarung. Er ist berechtigt sich zur Durchführung von Kontrollen der Hilfe Dritter zu bedienen. Soweit Dritte mit Kontrollen befasst werden sollen, steht dem AUFTRAGNEHMER das Recht zu, Kontrollpersonen abzulehnen, soweit diese direkt oder indirekt Mitbewerber des AUFTRAGNEHMERS sind oder zum AUFTRAGNEHMER in einem direkten oder indirekten Wettbewerbsverhältnis stehen; dies gilt auch, soweit die mit Kontrollen beauftragten Dritten ihrerseits als verbundene Unternehmen eines direkten oder indirekten Mitbewerbers des AUFTRAGNEHMERS gelten.

2 Der AUFTRAGNEHMER stellt sicher, dass sich der AUFTRAGGEBER von der Einhaltung der Pflichten des AUFTRAGNEHMERS nach Art. 28 DSGVO überzeugen kann, soweit der Dienstbetrieb nicht unverhältnismäßig gestört wird. Der AUFTRAGGEBER ist bei einer Kontrolle zu unterstützen; dies gilt auch für von diesem beauftragte Dritte. Die Kontrollbefugnis des AUFTRAGGEBERS erstreckt sich lediglich auf Daten und Informationen des AUFTRAGGEBERS und Daten, für die der AUFTRAGGEBER alleiniger oder gemeinsamer Verantwortlicher ist, sowie technische und organisatorische Maßnahmen bei dem AUFTRAGNEHMER, die das Vertragsverhältnis zwischen dem AUFTRAGGEBER und dem AUFTRAGNEHMER betreffen.

3 Die Kontrolle des AUFTRAGNEHMERS durch den AUFTRAGGEBER ist mit einem Vorlauf von 4 Wochen anzukündigen und terminlich mit diesem abzustimmen. 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 vorherige Ankündigung vorgenommen werden. Eine Störung des Dienstbetriebs beim AUFTRAGNEHMER sollte auch hierbei weitestgehend vermieden werden.

4 Im Hinblick auf die Kontrollverpflichtungen des AUFTRAGGEBERS vor Beginn der Datenverarbeitung und während der Laufzeit dieses AV-Vertrages stellt der AUFTRAGNEHMER sicher, dass

sich der AUFTRAGGEBER von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der AUFTRAGNEHMER dem AUFTRAGGEBER auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO nach. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Sachverständige, Revision, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach ISO 27001, IT-Grundschutz des BSI etc.) erbracht werden.

5 Für die Ermöglichung von Kontrollen durch den AUFTRAGGEBER kann der AUFTRAGNEHMER einen Vergütungsanspruch geltend machen. Eine solche Vergütung beläuft sich auf die tatsächlich angefallenen Kosten. Den Zeitaufwand hat der AUFTRAGNEHMER dem AUFTRAGGEBER nachzuweisen. Sollten im Rahmen dieser Kontrollen dem AUFTRAGNEHMER Kosten durch Unterauftragnehmer entstehen, so werden diese ohne Aufschlag dem AUFTRAGGEBER von dem AUFTRAGNEHMER weiterberechnet.

§ 9
Unterauftragnehmer

1 Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Tätigkeiten, die unter dem Abschnitt „Präambel“ aufgeführt sind (insbesondere die Analyse von EKG-Rohdaten) beziehen. Nicht hierzu gehören Nebenleistungen, die der AUFTRAGNEHMER z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen 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 Die Beauftragung von Unterauftragnehmern durch den AUFTRAGNEHMER zur Erfüllung seiner Verpflichtungen aus diesem AV-Vertrag und der Leistungsbeschreibung Schlaganfall-Risiko-Analyse **SRA®**, soweit personenbezogene Daten, die in der alleinigen oder gemeinsamen Verantwortung des AUFTRAGGEBERS stehen, erfolgt mit vorheriger Zustimmung des AUFTRAGGEBERS oder allgemeiner schriftlicher Genehmigung, die jedenfalls in Textform zu erteilen ist. Nimmt der AUFTRAGNEHMER die Dienste von Unterauftragnehmern in Anspruch wird er diese nach Maßgabe des Art. 28 Abs. 4 DSGVO verpflichten und diesen dieselben Datenschutzpflichten auferlegen, denen auch der AUFTRAGNEHMER nach diesem AV-Vertrag unterliegt. Zu diesem Zweck müssen insbesondere die mit dem Unterauftragnehmer zu vereinbarenden technischen und organisatorischen Maßnahmen ein gleichwertiges Schutzniveau aufweisen. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der AUFTRAGNEHMER die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der vorherigen Zustimmung des AUFTRAGGEBERS, die in Textform zu erteilen ist.

3 Bei der Unterbeauftragung sind dem AUFTRAGGEBER beim Unterauftragnehmer Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Dies umfasst auch das Recht des AUFTRAGGEBERS, vom AUFTRAGNEHMER auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis zu erhalten.

4 Der AUFTRAGGEBER stimmt der Beauftragung der in Anhang 3 aufgeführten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zu.

5 Im Fall einer allgemeinen schriftlichen Genehmigung informiert der AUFTRAGNEHMER den AUFTRAGGEBER immer über jede beabsichtigte Änderung der in Anhang 3 aufgeführten Unterauftragnehmer in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern, wodurch der AUFTRAGGEBER die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Verweigert der AUFTRAGGEBER durch seinen Einspruch die Zustimmung aus anderen als aus wichtigen Gründen, kann der AUFTRAGNEHMER den Vertrag kündigen.

§ 10
Haftung

1 Der AUFTRAGNEHMER haftet dem AUFTRAGGEBER für die schuldhafte Verursachung von Schäden im Zusammenhang mit der Ausführung der Auftragsverarbeitung und/oder dieser Vereinbarung.

2 Der AUFTRAGGEBER haftet für den Ersatz von Schäden, die ein Betroffener wegen einer unzulässigen oder falschen Auftragsverarbeitung erleidet, wobei ihm der Rückgriff beim AUFTRAGNEHMER vorbehalten bleibt.

§ 11
Nachvertragliche Verpflichtungen

1 Nach Beendigung der Auftragsverarbeitung hat der AUFTRAGNEHMER dem AUFTRAGGEBER sämtliche Unterlagen und soweit relevant, Arbeitsergebnisse auszuhändigen.

2 Die Datenträger, die Datenbestände bzgl. der Auftragsverarbeitung für den AUFTRAGGEBER enthalten, sind datenschutzgerecht zu löschen, bzw. an den AUFTRAGGEBER zurückzugeben. Elektronisch übertragene Daten, die personenbezogene Daten enthalten, sind datenschutzgerecht zu löschen. Gesetzliche Aufbewahrungspflichten bleiben unberührt. Test- und Ausschussmaterialien sind dem AUFTRAGGEBER auszuhändigen oder auf dessen Wunsch zu vernichten.

3 Der AUFTRAGNEHMER hat kein Zurückbehaltungsrecht bzgl. der verarbeiteten Daten und der dazugehörigen Datenträger.

§ 12
Vertragsdauer / Kündigung

1 Der Vertrag wird mit der Unterzeichnung wirksam und läuft auf unbestimmte Zeit.

2 Dieser Vertrag findet auf alle zwischen den Vertragsparteien vereinbarten Aufträge des AUFTRAGGEBERS an den AUFTRAGNEHMER Anwendung.

3 Jede Vertragspartei ist berechtigt, den Vertrag mit einer Frist von 4 Wochen zum Quartalsende zu kündigen.

4 Verweigert der AUFTRAGGEBER durch seinen Einspruch die Zustimmung zu einer Änderung und/oder Ergänzung von Anhang 3 aus anderen als aus wichtigen Gründen, kann der AUFTRAGNEHMER den Vertrag zum Zeitpunkt des geplanten Einsatzes des Unterauftragnehmers kündigen.

5 Das Recht zur außerordentlichen Kündigung bleibt hiervon unberührt. Ein solches soll für die Vertragsparteien insbesondere dann gegeben sein, wenn die jeweils andere Vertragspartei gegen vertragliche Verpflichtungen dieser Vereinbarung verstößt.

§ 13
Schlussbestimmungen

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 und das Eigentum an den Daten ausschließlich beim AUFTRAGGEBER als „Verantwortlicher“ im Sinne der Europäischen Datenschutzgrundverordnung (DSGVO) liegen.

2 Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile 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. Mündliche Nebenabreden sind nicht vereinbart.

3 Anwendbares Recht ist das Recht der Bundesrepublik Deutschland.

4 Gerichtsstand für alle Streitigkeiten aus dieser Vereinbarung ist Zweibrücken.
Erfüllungsort ist Pirmasens.

5 Die Rechtsunwirksamkeit einer Bestimmung berührt die Rechtswirksamkeit der anderen Vertragsteile nicht. Die Vertragsparteien verpflichten sich, eine unwirksame Bestimmung durch eine wirksame Regelung zu ersetzen, die ihr im wirtschaftlichen Ergebnis am nächsten kommt und dem Vertragszweck am besten entspricht. Das gilt sinngemäß für unvollständige Klauseln.

_____, den _____ Pirmasens, den_____

_____ _____

<Name des Unterzeichners> (AUFTRAGGEBER)

Albert Hirtz, Geschäftsführer (AUFTRAGNEHMER)

Anhang 1

Darstellung der technischen und organisatorischen Maßnahmen des AUFTRAGNEHMERs

Aufgaben:

- Verarbeitung von EKG-Rohdaten
- Übertragung von Analyseergebnissen
- Sonstige Kommunikation
- Fernwartung / Support

Datenübertragung

Die Übergabe und der Transport der Dokumente haben so gesichert zu erfolgen, dass ein Verlust derselben auf dem Transportweg ausgeschlossen werden kann. Üblicherweise kommt hier ein Verschlüsselungsverfahren zum Tragen, dass nach dem Stand der Technik als sicher angesehen werden kann.

Absicherung von E-Mails

Zum Versenden von sensiblen Daten per E-Mail steht beim AUFTRAGNEHMER das Verschlüsselungsverfahren S/MIME in einer dem Stand der Technik entsprechenden Variante zur Verfügung.

Betriebssicherheit

Der AUFTRAGGEBER hält technische Ressourcen, soweit vertretbar redundant vor, um eine hohe Verfügbarkeit des Dienstes zu gewährleisten.

Speicherung der Daten beim Auftragsverarbeiter (AUFTRAGNEHMER)

Die verarbeiteten Daten und die Resultate werden für maximal 3 Monate beim Auftragnehmer gespeichert und danach dort unwiederbringlich gelöscht. Die Server sind in einem ausreichend gesicherten Rechenzentrum untergebracht. Der Zugang, Zutritt und Zugriff zu den Systemen ist nur besonders berechtigten Personen möglich.

Schutz vor Malware und Viren

Alle Systeme des AUFTRAGNEHMERs verfügen über Schutzsoftware um eine Gefährdung durch Viren, Trojaner und anderen schädliche Einflüsse so gering wie möglich zu halten. Antivirensysteme müssen mindestens einmal am Tag aktualisiert werden. Sämtliche Schutzsoftware muss dem Stand der Technik entsprechen.

Elektrische Absicherung

Die Server, welche im Rahmen der Auftragsverarbeitung eingesetzt werden, sind durch ausreichend dimensionierte unterbrechungsfreie Stromversorgungen abgesichert.

Absicherung durch Firewall

Der AUFTRAGNEHMER ist verpflichtet seine eigenen Netzwerke und Systeme, in denen Daten des AUFTRAGGEBERS gespeichert werden, durch eine für professionelle Zwecke geeignete Firewall zu sichern. Bezüglich einer Firewall wird regelmäßig dafür Sorge getragen, dass die Firewall dem Stand der Technik entspricht und stets auf dem aktuellen Stand gehalten wird, was Software-Releases und Sicherheits-Patches angeht.

Sensibilisierung für Belange des Datenschutzes

Der AUFTRAGNEHMER hat seine Mitarbeiter regelmäßig hinsichtlich der Belange des Datenschutzes und der Datensicherheit zu sensibilisieren. Die Mitarbeiter, welche auf Systeme des AUFTRAGGEBERS zugreifen, sind auf das Datengeheimnis zu verpflichten.

Infrastruktur

Der AUFTRAGNEHMER trägt dafür Sorge, dass die Server auf denen personenbezogene Daten im Auftrag des AUFTRAGGEBERS verarbeitet werden, ausreichend gekühlt oder klimatisiert werden und das Umfeld der Server den Vorgaben der ISO 27001 entspricht. Die erforderlichen Maßnahmen beziehen auch den Zutrittsschutz zu den Anlagen mit ein.

Regelmäßige Überprüfungen technischer und organisatorischer Maßnahmen

Unabhängig von eventuellen Zertifizierungen lässt der AUFTRAGNEHMER einmal jährlich einen Audit durchführen und feststellen, wo hinsichtlich technischer und organisatorischer Maßnahmen ein Anpassungsbedarf besteht. Dabei orientiert sich der Audit am jeweiligen Stand der Technik.

Information über Bedrohungen

Sobald eine potenzielle Bedrohung auf Systemen des AUFTRAGNEHMERs entdeckt oder vermutet wird, von denen auf Systeme des AUFTRAGGEBERS zugegriffen wird, informiert der AUFTRAGNEHMER sofort den AUFTRAGGEBER und trifft Maßnahmen, die eine Ausbreitung der Bedrohung auf Systeme des AUFTRAGGEBERS verhindern. Gleiches gilt für die Systeme des AUFTRAGGEBERS, wenn durch die Datenübertragung zum AUFTRAGNEHMER dessen Systeme gefährdet werden könnten.

Löschen von Daten/Kopien/Datensicherungen

Nach Verarbeitungs-, Auftrags oder Vertragsende werden personenbezogene Daten, soweit keine Rückgabe an den AUFTRAGGEBER erforderlich ist oder verlangt wird, vollständig und unverzüglich, jedoch spätestens nach Ablauf von drei Monaten aus den produktiven Systemen gelöscht bzw. vernichtet. Gesetzliche Aufbewahrungspflichten bleiben unberührt.

Rückgabe von Datenträgern/Kopien/Datensicherungen

Nach Verarbeitungs-, Auftrags- oder Vertragsende werden überlassene Datenträger mit personenbezogenen Daten unverzüglich jedoch spätestens nach Ablauf von drei Monaten an den AUFTRAGGEBER zurückgegeben.

Anhang 2

Namensliste

1 Ansprechpartner / Weisungsbefugter beim AUFTRAGGEBER

Name	Funktion	E-Mail	Sonst. Erreichbarkeit

2 Datenschutzbeauftragter des AUFTRAGGEBERS

Name	E-Mail	Sonst. Erreichbarkeit

3 Ansprechpartner / Weisungsempfänger beim AUFTRAGNEHMER

Name	**Funktion**	**E-Mail**	**Sonst. Erreichbarkeit**

4 Datenschutzbeauftragter des AUFTRAGNEHMERs

Name	E-Mail	Sonst. Erreichbarkeit

Anhang 3

Folgende Unterauftragsnehmer erbringen Teilleistungen für den AUFTRAGNEHMER

Unterauftragnehmer	Anschrift / Land	Art des Unterauftrages
GIG Management GmbH	Universitätsstraße 142 44977 Bochum Deutschland	kardiologische Befundung im Rahmen von **SRA®**+
First Soft GmbH & Co. KG Softwareentwicklung	Schulstraße 12 35440 Linden Deutschland	Installation und Service HL7-Schnittstelle **SRA®**-to-KIS
Deutsche Telekom Healthcare and Security Solutions GmbH	Friedrich-Ebert-Allee 140 53113 Bonn Deutschland	Telekom Health Cloud Cloud Speicherdienst Datenarchivierung