Vereinbarung

- zum Hauptvertrag mit der Vertragsnummer/Kennung vom -

Zwischen

Universitätsmedizin Rostock - rechtsfähige Teilkörperschaft der Universität Rostock
vertreten durch den Vorstand
Schillingallee 35
18057 Rostock

- Verantwortliche i.S.d. DSGVO - nachfolgend **Auftraggeberin** genannt –

und

Firma
Straße
PLZ, Ort
vertreten durch xxx

- Auftragsverarbeiter i.S.d. DSGVO - nachfolgend **Auftragnehmer** genannt -

über Auftragsverarbeitung gemäß Art. 28 DSGVO.

Präambel

☐ Existierender Hauptvertrag - *oder* - ☐ Hauptvertrag liegt nicht vor

Dieser Auftragsverarbeitungs-Vertrag (AV-Vertrag) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der im Hauptvertrag beschriebenen Auftragsverarbeitung bzw. aus den in § 2 „Gegenstand des Auftrags“ dargestellten Leistungen ergeben.

Sämtliche in diesem Vertrag beschriebenen Verpflichtungen finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Mitarbeiterinnen und Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten der Auftraggeberin in Berührung kommen bzw. kommen können.

§ 1 Definitionen

Es gelten die Begriffsbestimmungen entsprechend Art. 4 DSGVO, § 2 UWG und § 2 TMG sowie § 3 DSG M-V und § 32 LKHG M-V. Sollten in den Artikeln bzw. Paragraphen sich widersprechende Darstellungen zu finden sein, gelten die Definitionen in der Rangfolge DSGVO, Landesrecht, UWG und TMG. Weiterhin gelten folgende Begriffsbestimmungen:

(1) Anonymisierung
Prozess, bei dem personenbezogene Daten entweder vom für die Verarbeitung der Daten Verantwortlichen allein oder in Zusammenarbeit mit einer anderen Partei unumkehrbar so verändert werden, dass sich die betroffene Person danach weder direkt noch indirekt identifizieren lässt. (Quelle: DIN EN ISO 25237)

(2) Drittland
Ein Land, welches sich außerhalb der EU/EWR befindet.

(3) Hauptvertrag
Vertrag (i.d.R. ein Dienst- oder Werkvertrag), in welchem alle Einzelheiten der Verarbeitung beschrieben sind.

(4) Unterauftragnehmer
Vom Auftragnehmer beauftragter Leistungserbringer, dessen Dienstleistung und/oder Werk der Auftragnehmer zur Erbringung der in diesem Vertrag beschriebenen Leistungen gegenüber der Auftraggeberin benötigt.

(5) Verarbeitung im Auftrag
Verarbeitung im Auftrag ist die Verarbeitung personenbezogener Daten durch einen Auftragnehmer im Auftrag der Auftraggeberin.

(6) Weisung
Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung der Auftraggeberin. Die Weisungen werden anfänglich durch einen Hauptvertrag festgelegt und können von der Auftraggeberin danach in schriftlicher Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

§ 2 Gegenstand des Auftrags

Gegenstand der Vereinbarung ist die Verarbeitung personenbezogener Daten (nachstehend „Daten“ genannt) durch den Auftragnehmer für die Auftraggeberin in deren Auftrag und nach deren Weisung im Zusammenhang mit und in Ergänzung des Hauptvertrags. Die Vereinbarung gilt entsprechend für (Fern-) Prüfung und Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen, wenn dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Der Auftragnehmer erhält Zugriff auf folgende personenbezogene Daten (dadurch, dass die Auftraggeberin ihm die Daten bereitstellt oder ihm einen Zugriff auf die Daten ermöglicht), bzw. die Auftraggeberin erlaubt dem Auftragnehmer, folgende personenbezogene Daten zu erheben:

1. **Bezeichnung der Daten und Betroffenen**

   Datenarten:

   ☐ Personenstammdaten (z. B Mitarbeiter, Kooperationspartner, nicht med. Patientendaten)
   ☐ Medizinische Patientendaten (Befunde, Diagnosen, …)
   ☐ Kontaktdaten/Kommunikationsdaten (z. B. IP-Adressen, Telefon, E-Mail)
   ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
   ☐ Kundenhistorie
   ☐ Vertragsabrechnungs- und Zahlungsdaten
   ☐ Planungs- und Steuerungsdaten
   ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
   ☐ Sonstige:

   Bei den **Betroffenen** der oben aufgelisteten Daten handelt es sich um:

   ☐ Patienten
   ☐ Kunden
   ☐ Interessenten
   ☐ Beschäftigte
   ☐ Lieferanten
   ☐ Handelsvertreter
   ☐ Ansprechpartner
   ☐ Sonstige:

2. **Der Zugriff auf die Daten bzw. die Datenerhebung findet wie folgt statt:**

   ☐ Vor Ort auf den Geräten/Datenträgern der Auftraggeberin ohne Remote-Zugang
   ☐ Breitstellung einer gesicherten Verbindung zwischen Auftragnehmer und Auftraggeberin
      ☐ per Site to Site VPN über: UMR-Dienstleisterportal
      ☐ per Client to Site VPN über: GlobalProtect
   ☐ Übergabe der Daten von Auftraggeberin an Auftragnehmer über:

3. **Zweck der Datenverarbeitung**

   Bitte den Grund angeben (und ggf. kurz erläutern), warum die Verarbeitung der o.g. Daten durch den Auftragnehmer erfolgt, bspw. "Sichtung der Benutzeroberfläche der Software xy zur Fehleranalyse und -behebung im System, bei der eine Kenntnisnahme von den o.g. Daten nicht gewollt, aber auch nicht auszuschließen ist"

4. **Der Auftragnehmer erbringt für die Auftraggeberin folgende Prüf- bzw. Wartungstätigkeiten, bei denen eine Zugriffsmöglichkeit auf personenbezogene Daten nicht ausgeschlossen werden kann:**

   ☐ Keine
   ☐ Prüfung/Wartung vor Ort, bei denen eine Zugriffsmöglichkeit auf personenbezogene Daten nicht ausgeschlossen werden kann:
   ☐ Hardware-Diagnose per Fernzugriff für folgende Hardwareprodukt(e), bei denen eine Zugriffsmöglichkeit auf personenbezogene Daten nicht ausgeschlossen werden kann:
   ☐ Software-Prüfung/Wartung per Fernzugriff für folgende(s) Softwareprodukt(e), bei denen eine Zugriffsmöglichkeit auf personenbezogene Daten nicht ausgeschlossen werden kann:

   ☐ Sonstiges:

§ 2.1 Leistungen des Auftragnehmers

Der Auftragnehmer erbringt für die Auftraggeberin bezogen auf die in § 2 genannten Daten folgende konkrete Leistungen:

Bitte beschreiben Sie an dieser Stelle ganz konkret die Dienstleistung, die durch den Auftragnehmer erbracht wird. Ein reiner Verweis auf einen Hauptvertrag ist unzureichend. Aus dieser Beschreibung muss klar hervorgehen, in welcher Handlung/Tätigkeit des Auftragnehmers die Auftragsverarbeitung konkret besteht. Handelt es sich bspw. um eine Supportleistung mit Fernzugriff auf eine Software, sollte unter diesem Punkt Bezug zu der entsprechenden Software und den unter § 2 angekreuzten personenbezogenen Daten genommen, der genaue Supportablauf beschrieben, die Nutzungs-/Kenntnisnahmemöglichkeiten des Auftragnehmers aufgelistet und anschließend begründet werden, warum ein Datenzugriff gewollt bzw. nicht gewollt, dann aber nicht ganz auszuschließen ist.

§ 3 Verantwortlichkeit

(1) Die Auftraggeberin ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenverarbeitung verantwortlich („Verantwortliche“ i.S.d. Art. 4 Nr. 7 DSGVO).

(2) Die Inhalte dieses AV-Vertrages gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

(3) Auftraggeberin sowie Auftragnehmer müssen gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Dazu müssen alle Personen, die auftragsgemäß auf personenbezogene Daten der Auftraggeberin zugreifen können, auf das Datengeheimnis und Vertraulichkeit verpflichtet und über ihre Datenschutzpflichten belehrt werden. Dabei ist jede Partei für die Verpflichtung des eigenen Personals zuständig. Ferner müssen die eingesetzten Personen darauf hingewiesen werden, dass das Datengeheimnis auch nach Beendigung der Tätigkeit fortbesteht. Es muss von jedem Beschäftigten des Auftragnehmers, der auftragsgemäß auf personenbezogene Daten der Auftraggeberin zugreifen kann, eine Vertraulichkeitsverpflichtung nach Art. 28 Abs. 3 lit. b DSGVO unterzeichnet und bei Aufforderung durch die Auftraggeberin vom Auftragnehmer vorgelegt werden.

(4) Der Auftragnehmer verpflichtet sich gem. § 34 Abs. 5 LKHG M-V für den Fall, dass die Vorschriften des LKHG M-V keine Anwendung auf ihn finden und eine Offenbarung von Patientendaten für eine Weiterverarbeitung von Daten gem. § 34 Abs. 1 LKHG M-V durch ihn erfolgt, zur Einhaltung der Vorschriften nach § 34 Abs. 2-4 i.V.m. Abs. 1 LKHG M-V.

(5) Der Auftragnehmer verpflichtet sich gem. § 37 Abs. 6 LKHG M-V für den Fall, dass die Vorschriften des LKHG M-V keine Anwendung auf ihn finden und eine Offenbarung von Patientendaten für eine Datenverarbeitung zu Forschungszwecken gem. § 37 LKHG M-V durch ihn erfolgt, zur Einhaltung der Vorschriften nach § 37 Abs. 2-4 LKHG M-V und zur Unterwerfung der Kontrolle des Landesbeauftragten für den Datenschutz.

(6) Die Auftraggeberin und der Auftragnehmer sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

§ 4 Dauer des Auftrags

☐ Die Laufzeit dieses AV-Vertrages richtet sich nach der Laufzeit des Hauptvertrags, sofern sich aus den Bestimmungen dieses AV-Vertrages nicht etwas anderes ergibt.

- oder -

☐ Die Laufzeit dieses AV-Vertrages endet am tt.mm.jjjj, sofern sich aus den Bestimmungen dieses AV-Vertrages nicht etwas anderes ergibt.

- oder -

☐ Der Vertrag wird mit der Unterzeichnung wirksam und läuft auf unbestimmte Zeit. Jede Partei ist berechtigt, den Vertrag mit einer Frist von Wochen zum Monatsende/Quartalsende/Jahresende (nicht Zutreffendes bitte entfernen) zu kündigen.

(1) Es ist den Vertragspartnern bewusst, dass ohne Vorliegen eines gültigen AV-Vertrages z.B. bei Beendigung des vorliegenden Vertragsverhältnisses, keine (weitere) Auftragsverarbeitung durchgeführt werden darf.
(2) Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.
(3) Kündigungen bedürfen zu ihrer Wirksamkeit der Schriftform.

§ 5 Weisungsbefugnis der Auftraggeberin

(1) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung der Auftraggeberin. Ausgenommen hiervon sind Sachverhalte, in denen dem Auftragnehmer eine Verarbeitung aus zwingenden rechtlichen Gründen auferlegt wird. Der Auftragnehmer unterrichtet soweit ihm möglich in derartigen Situationen die Auftraggeberin vor Beginn der Verarbeitung über die entsprechenden rechtlichen Anforderungen. Die Auftraggeberin behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das sie durch Einzelweisungen konkretisieren kann.
(2) Die Weisungen der Auftraggeberin werden vom Auftragnehmer dokumentiert und der Auftraggeberin unmittelbar nach erfolgter Dokumentation als unterschriebene Kopie zur Verfügung gestellt.
(3) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind von der Weisungsbefugnis der Auftraggeberin gedeckt und entsprechend zu dokumentieren. Bei einer wesentlichen Änderung des Auftrags steht dem Auftragnehmer ein Widerspruchsrecht zu. Besteht die Auftraggeberin trotz des Widerspruchs des Auftragnehmers auf der Änderung, steht dem Auftragnehmer ein ordentliches Kündigungsrecht bezüglich des von der Weisung betroffenen AV-Vertrages sowie der von der AV-Vereinbarung betroffenen Bestandteile des entsprechenden Hauptvertrages zu. Verweigert der Auftragnehmer, die Änderung durchzuführen, steht auch der Auftraggeberin ein ordentliches Kündigungsrecht zu. Erfolgt eine Kündigung, so ist für die restliche Vertragslaufzeit weiterhin die vertraglich vereinbarte Leistung durch den Auftragnehmer zu erbringen.
(4) Mündliche Weisungen wird die Auftraggeberin unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragnehmer notiert sich Datum, Uhrzeit und Person, welche die mündliche Weisung erteilte sowie den Grund, warum keine schriftliche Beauftragung erfolgen konnte.
(5) Weisungsberechtigte Personen der Auftraggeberin sind:

Personen	**Zutreffende bitte auswählen**
Vorstände	☐ Ja / ☐ Nein
IT-Leitung	☐ Ja / ☐ Nein
Sonstige:	☐ Ja / ☐ Nein

§ 6 Leistungsort

(1) ☐ Der Auftragnehmer wird die vertraglichen Leistungen in *Deutschland* erbringen, etwaige Unterauftragnehmer an den mit der Auftraggeberin in Anhang 1 vereinbarten Leistungsstandorten in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR).

- oder -

☐ Der Auftragnehmer wird die vertraglichen Leistungen in der Europäischen Union (*EU*) oder im Europäischen Wirtschaftsraum (*EWR*) erbringen, etwaige Unterauftragnehmer an den mit der Auftraggeberin in Anhang 1 vereinbarten Leistungsstandorten der Unterauftragnehmer in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR).

- oder -

☐ Der Auftragnehmer wird die vertraglichen Leistungen in Deutschland erbringen. Etwaige Unterauftragnehmer erbringen die sie betreffenden Leistungen in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) oder in einem Drittland. Erfolgt eine Leistungserbringung durch einen Unterauftragnehmer in einem Drittland, garantiert der Auftragnehmer die Einhaltung der diesbezüglichen Vorgaben der DSGVO und weist dies auf Verlangen nach.

- oder -

☐ Der Auftragnehmer wird die vertraglichen Leistungen in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) oder in einem Drittland erbringen. Dies gilt in gleicher Weise für etwaige Unterauftragnehmer. Die zum Zeitpunkt der Auftragserteilung vereinbarten Leistungsstandorte sind in Anhang I dargestellt. Erfolgt eine Leistungserbringung in einem Drittland, garantiert der Auftragnehmer die Einhaltung der diesbezüglichen Vorgaben der DSGVO und weist dies auf Verlangen nach.

(2) Die Auftraggeberin stimmt einer Verlagerung eines Ortes der Leistungserbringung innerhalb des Leistungslandes, für das eine Zustimmung besteht, zu, wenn dort nachweislich ein gleiches Sicherheitsniveau gegeben ist und keine für die Auftraggeberin 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, wird die Auftraggeberin schriftlich informiert.

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

(5) Wenn der Auftragnehmer die geschuldeten Leistungen ganz oder teilweise von einem Standort außerhalb der EU/EWR in einem sog. sicheren „Drittstaat“ erbringen möchte bzw. die Leistungserbringung dorthin zu verlagern plant, wird der Auftragnehmer zuvor die schriftliche Zustimmung durch die Auftraggeberin einholen.

(6) Sofern die Leistungsverlagerung in ein anderes Land nach den vorstehenden Regelungen möglich ist, gilt dies entsprechend für jeglichen Zugriff bzw. jegliche Sicht auf die Daten durch den Auftragnehmer, z.B. im Rahmen von internen Kontrollen oder zu Zwecken der Entwicklung, der Durchführung von Tests, der Administration oder der Wartung.

(7) Sofern die Datenverarbeitung nach dieser Vereinbarung und den gesetzlichen Vorgaben zur Verarbeitung personenbezogener Daten im Auftrag bzw. zur Übermittlung personenbezogener Daten in das Ausland zulässig außerhalb Deutschlands erbracht werden darf, wird der Auftragnehmer für die Einhaltung und Umsetzung der gesetzlichen Erfordernisse zur

Sicherstellung eines adäquaten Datenschutzniveaus bei Standortverlagerungen und bei grenzüberschreitendem Datenverkehr Sorge tragen.

§ 7 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten nur im Rahmen des Auftrages und der Weisungen der Auftraggeberin erheben, verarbeiten oder nutzen.

(2) Der Auftragnehmer wird 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 der Auftraggeberin vor Missbrauch und Verlust treffen, die den Anforderungen der entsprechenden datenschutzrechtlichen Bestimmungen entsprechen; diese Maßnahmen muss der Auftragnehmer auf Anfrage der Auftraggeberin und ggfs. Aufsichtsbehörden gegenüber nachweisen. Dieser Nachweis beinhaltet insbesondere die Umsetzung der aus Art. 32 DSGVO resultierenden Maßnahmen.
Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative, nachweislich adäquate Maßnahmen umzusetzen. Dabei muss sichergestellt sein, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.
Eine Darstellung dieser technischen und organisatorischen Maßnahmen erfolgt in Anlage 2 zu diesem Vertrag.

(3) Der Auftragnehmer stellt der Auftraggeberin auf deren Wunsch ein aussagekräftiges und aktuelles Datenschutz- und Sicherheitskonzept für diese Auftragsverarbeitung zur Verfügung.

(4) Der Auftragnehmer selbst führt für die Verarbeitung ein Verzeichnis der bei ihm stattfindenden Verarbeitungstätigkeiten im Sinne des Art. 30 DSGVO. Er stellt auf Anforderung der Auftraggeberin die für die Übersicht nach Art. 30 DSGVO notwendigen Angaben zur Verfügung. Des Weiteren stellt er das Verzeichnis auf Anfrage der Aufsichtsbehörde zur Verfügung.

(5) Der Auftragnehmer unterstützt die Auftraggeberin bei der Datenschutzfolgenabschätzung mit allen ihm zur Verfügung stehenden Informationen. Im Falle der Notwendigkeit einer vorherigen Konsultation der zuständigen Aufsichtsbehörde unterstützt der Auftragnehmer die Auftraggeberin auch hierbei.

(6) Die Wahrung des Fernmeldegeheimnisses entsprechend § 88 TKG muss vom Auftragnehmer gewährleistet werden. Dazu muss der Auftragnehmer alle Personen, die auftragsgemäß auf Daten der Auftraggeberin mittels Mittel der Telekommunikation wie Telefon oder E-Mail zugreifen können, auf das Fernmeldegeheimnis verpflichten und über die sich daraus ergebenden besonderen Geheimhaltungspflichten belehren.

(7) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen der Auftraggeberin vertraulich zu behandeln.

(8) Weiterhin sind alle Personen des Auftragnehmers bzgl. der Pflichten zur Wahrung von Geschäfts- und Betriebsgeheimnissen der Auftraggeberin zu verpflichten und müssen auf § 17 UWG hingewiesen werden.

(9) Als Datenschutzbeauftragter ist beim Auftragnehmer derzeit benannt:
bitte Name und Kontaktdaten angeben
Ein Wechsel des Datenschutzbeauftragten ist der Auftraggeberin unverzüglich schriftlich mitzuteilen. Der Auftragnehmer gewährleistet, dass die Anforderungen an den Datenschutzbeauftragten und seine Tätigkeit gemäß Art. 38 DSGVO erfüllt werden. Sofern kein Datenschutzbeauftragter beim Auftragnehmer benannt ist, benennt der Auftragnehmer der Auftraggeberin einen Ansprechpartner.

(10) Der Auftragnehmer unterrichtet die Auftraggeberin unverzüglich bei Verstößen des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen

Vorschriften zum Schutz personenbezogener Daten der Auftraggeberin oder der im Vertrag getroffenen Festlegungen. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen und spricht sich hierzu unverzüglich mit der Auftraggeberin ab. Der Auftragnehmer unterstützt die Auftraggeberin bei der Erfüllung der Informationspflichten gegenüber der jeweils zuständigen Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen nach Art. 33, 34 DSGVO.

(11) Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an die Auftraggeberin weiterleiten.

(12) Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum der Auftraggeberin. Der Auftragnehmer hat diese sorgfältig zu verwahren, sodass sie Dritten nicht zugänglich sind. Der Auftragnehmer ist verpflichtet, der Auftraggeberin jederzeit Auskünfte zu erteilen, soweit ihre Daten und Unterlagen betroffen sind.

(13) Ist die Auftraggeberin aufgrund geltender Datenschutzgesetze gegenüber einer betroffenen Person verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer die Auftraggeberin dabei unterstützen, diese Informationen bereitzustellen, vorausgesetzt die Auftraggeberin hat den Auftragnehmer hierzu schriftlich aufgefordert.

(14) Der Auftragnehmer informiert die Auftraggeberin unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde bei dem Auftragnehmer ermittelt.

(15) Der Auftragnehmer wird die Auftraggeberin unverzüglich darauf aufmerksam machen, wenn eine von der Auftraggeberin erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch die Auftraggeberin bestätigt oder geändert wird.

(16) Sollten die Daten der Auftraggeberin beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer die Auftraggeberin 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 bei der Auftraggeberin als Verantwortliche im Sinne der DSGVO liegen.

(17) Der Auftragnehmer verwendet die überlassenen Daten für keine anderen Zwecke als die der Vertragserfüllung und setzt auch keine Mittel zur Verarbeitung ein, die nicht von der Auftraggeberin zuvor genehmigt wurden.

(18) Der Auftragnehmer speichert keine Patientendaten auf Systemen, die außerhalb der Verfügungsgewalt der Auftraggeberin liegen bzw. die nicht dem Beschlagnahmeschutz unterliegen.

(19) Sofern der Auftragnehmer durch das Recht der Union oder Mitgliedstaaten verpflichtet ist, die Daten auch auf andere Weise zu verarbeiten, so teilt der Auftragnehmer der Auftraggeberin diese rechtlichen Anforderungen vor der Verarbeitung mit. Die Mitteilung hat zu unterbleiben, wenn das einschlägige nationale Recht eine solche Mitteilung aufgrund eines wichtigen öffentlichen Interesses verbietet.

(20) Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren, zu dokumentieren und in geeigneter Weise gegenüber der Auftraggeberin auf Anforderung nachzuweisen.

§ 8 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.

Die Auftraggeberin weist den Auftragnehmer darauf hin, dass sich Personen, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken und unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist, strafbar machen nach § 203 Abs. 4 S. 1 StGB. Zudem macht sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde.

(2) Der Auftragnehmer stellt sicher, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten der Auftraggeberin befassten Beschäftigten und andere für den Auftragnehmer tätigen Personen (z.B. Subunternehmer), die damit befasst sind, sich in Textform dazu verpflichtet haben, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren und sie über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB belehrt wurden. Die Auftraggeberin 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. Der Auftragnehmer wird etwaige Unterauftragnehmer sorgfältig auswählen und diese, soweit sie im Rahmen ihrer Tätigkeit Kenntnis von fremden Geheimnissen im Sinne dieser Vereinbarung erlangen könnten, zum Stillschweigen verpflichten. Der Auftragnehmer wird ferner etwaige Unterauftragnehmer dazu verpflichten, sämtliche von diesen eingesetzte Personen und etwaige weitere Unterauftragnehmer, die bestimmungsgemäß mit Geheimnisschutzdaten in Berührung kommen oder bei denen dies nicht auszuschließen ist, nach den zuvor genannten Grundsätzen zur Verschwiegenheit zu verpflichten und über die Folgen einer Pflichtverletzung zu belehren.
Des Weiteren werden Subunternehmer über das bestehende Schweigerecht gemäß § 53a StPO sowie den Beschlagnahmeschutz gemäß § 97 StPO informiert; dies beinhaltet auch den Hinweis auf das Recht des Berufsgeheimnisträgers über dieses Recht zu entscheiden und die damit verbundene Pflicht, unverzüglich die Auftraggeberin bzgl. der Wahrnehmung dieser Rechte zu kontaktieren.
Diese Verpflichtung gilt für sämtliche weitere Unterbeauftragungen.

- oder -

☐ Der Einsatz von Unterauftragnehmern zur Verarbeitung der Daten der Auftraggeberin ist nicht gestattet.

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

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

§ 9 Fernzugriff bei Prüfung/Wartung eines Systems oder anderen Dienstleistungen über Fernzugriffe

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 Rechte/Pflichten der Auftraggeberin/des Auftragnehmers:

(1) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten an Arbeitsplatzsystemen werden erst nach Freigabe durch den jeweiligen Berechtigten/zuständigen Mitarbeiter der Auftraggeberin durchgeführt.

(2) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten von automatisierten Verfahren oder von Datenverarbeitungsanlagen werden, sofern hierbei ein Zugriff auf personenbezogene Daten nicht sicher ausgeschlossen werden kann, ausschließlich mit Zustimmung der Auftraggeberin ausgeführt.

(3) Die Mitarbeiter des Auftragnehmers verwenden angemessene Identifizierungs- und Verschlüsselungsverfahren.

(4) Vor Durchführung von Fernzugriffen werden sich Auftraggeberin und Auftragnehmer über etwaig notwendige Datensicherheitsmaßnahmen in ihren jeweiligen Verantwortungsbereichen verständigen.

(5) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten werden dokumentiert und protokolliert. Die Dokumentation wird zumindest vom Auftragnehmer durchgeführt und enthält mindestens folgende Angaben: Wer (Name der Person und Firma, die den Fernzugriff durchführt) hat wann (Datum und Uhrzeit des Start- und Beendigungszeitpunktes des Fernzugriffs) zu welchem Zweck einen Fernzugriff durchgeführt? Die Auftraggeberin ist berechtigt, Prüfungs- und Wartungsarbeiten vor, bei und nach Durchführung zu kontrollieren. Bei Fernzugriffen ist die Auftraggeberin - soweit technisch möglich - berechtigt, diese von einem Kontrollbildschirm aus zu verfolgen und jederzeit abzubrechen.

(6) Der Auftragnehmer wird von den ihm eingeräumten Zugriffsrechten auf automatisierte Verfahren oder von Datenverarbeitungsanlagen (insb. IT-Systeme, Anwendungen) der Auftraggeberin nur in dem Umfang - auch in zeitlicher Hinsicht - Gebrauch machen, wie dies für die ordnungsgemäße Durchführung der beauftragten Wartungs- und Prüfungsarbeiten notwendig ist.

(7) Soweit bei der Leistungserbringung Tätigkeiten zur Fehleranalyse erforderlich sind, bei denen eine Kenntnisnahme (z.B. auch lesender Zugriff) oder ein Zugriff auf Wirkdaten (Produktions-/Echtdaten) der Auftraggeberin notwendig ist, wird der Auftragnehmer die vorherige Einwilligung der Auftraggeberin einholen.

(8) Tätigkeiten zur Fehleranalyse, bei denen ein Datenabzug der Wirkbetriebsdaten erforderlich ist, bedürfen der vorherigen Einwilligung der Auftraggeberin. Bei Datenabzug der Wirkbetriebsdaten wird der Auftragnehmer diese Kopien, unabhängig vom verwendeten Medium, nach Bereinigung des Fehlers löschen. Wirkdaten dürfen nur zum Zweck der Fehleranalyse und ausschließlich auf dem bereitgestellten Equipment der Auftraggeberin oder auf solchem des Auftragnehmers verwendet werden, sofern die vorherige Einwilligung der Auftraggeberin vorliegt. Wirkdaten dürfen nicht ohne Zustimmung der Auftraggeberin auf mobile Speichermedien (PDAs, USB-Speichersticks oder ähnliche Geräte) kopiert werden.

(9) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten sowie sämtliche in diesem Zusammenhang erforderlichen Tätigkeiten, insbesondere Tätigkeiten wie Löschen, Datentransfer oder eine Fehleranalyse, werden unter Berücksichtigung von technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten durchgeführt. In diesem Zusammenhang wird der Auftragnehmer die technischen und organisatorischen Maßnahmen wie im Anhang beschrieben ergreifen.

§ 10 Pflichten der Auftraggeberin

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein die Auftraggeberin verantwortlich. Die Auftraggeberin wird in ihrem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z.B. durch Einholung von Einwilligungserklärungen für die Verarbeitung der Daten) geschaffen werden, damit der Auftragnehmer die vereinbarten Leistungen rechtsverletzungsfrei erbringen kann.

(2) Die Auftraggeberin hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn sie bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Die Auftraggeberin ist hinsichtlich der vom Auftragnehmer eingesetzten und von der Auftraggeberin genehmigten Verfahren zur automatisierten Verarbeitung personenbezogener Daten datenschutzrechtlich verantwortlich und hat - neben der eigenen Verpflichtung des Auftragnehmers - ebenfalls die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten.

(4) Der Auftraggeberin obliegen die aus Art. 33, 34 DSGVO resultierenden Informationspflichten gegenüber der Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen.

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

(6) Die Auftraggeberin ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

(7) Die Auftraggeberin stellt sicher, dass die aus Art. 32 DSGVO resultierenden Anforderungen bzgl. der Sicherheit der Verarbeitung ihrerseits eingehalten werden. Insbesondere gilt dies für Fernzugriffe des Auftragnehmers auf die Datenbestände der Auftraggeberin.

(8) Erteilt die Auftraggeberin Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten von der Auftraggeberin zu tragen. Sofern der vereinbarte Leistungsumfang überschritten wird, ist hierzu vorab eine gesonderte schriftliche Vereinbarung zu treffen.

§ 11 Kontrollrechte der Auftraggeberin

(1) Die Auftraggeberin hat den Auftragnehmer unter dem Aspekt ausgewählt, dass dieser hinreichend Garantien dafür bietet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Hierfür kann sie beispielsweise

- datenschutzspezifische Zertifizierungen oder Datenschutzsiegel und -prüfzeichen berücksichtigen,
- schriftliche Selbstauskünfte des Auftragnehmers einholen,
- sich ein Testat eines Sachverständigen vorlegen lassen oder
- sich nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich oder durch einen sachkundigen Dritten, der nicht in einem Wettbewerbsverhältnis zum Auftragnehmer stehen darf, von der Einhaltung der vereinbarten Regelungen überzeugen.

(2) Liegt ein Verstoß des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten der Auftraggeberin 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.

(3) Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch die Auftraggeberin im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags wird vom Auftragnehmer unterstützt. Insbesondere verpflichtet sich der Auftragnehmer, der Auftraggeberin auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind.

(4) Die Auftraggeberin hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn sie bei der Prüfung Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

§ 12 Berichtigung, Beschränkung von Verarbeitung, Löschung und Rückgabe von Datenträgern

(1) Während der laufenden Beauftragung berichtigt, löscht oder sperrt der Auftragnehmer die vertragsgegenständlichen Daten nur auf Anweisung der Auftraggeberin.

(2) Sofern eine Vernichtung während der laufenden Beauftragung vorzunehmen ist, übernimmt der Auftragnehmer die nachweislich datenschutzkonforme Vernichtung von Datenträgern und sonstiger Materialien nur aufgrund entsprechender Einzelbeauftragung durch die Auftraggeberin. Dies gilt nicht, sofern im Hauptvertrag bereits eine entsprechende Regelung getroffen worden ist.

(3) In besonderen, von der Auftraggeberin zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe.

(4) Nach Abschluss der vertraglichen Arbeiten - oder früher nach Aufforderung durch die Auftraggeberin - hat der Auftragnehmer

- sämtliche im Rahmen des Auftrags in seinen Besitz gelangte Unterlagen oder Datenträger,
- erstellte Verarbeitungsergebnisse,
- Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen

der Auftraggeberin auszuhändigen oder auf Anweisung der Auftraggeberin datenschutzkonform zu löschen bzw. zu vernichten, sofern keine gesetzliche Pflicht zur Aufbewahrung besteht. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(5) Sofern zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten entstehen, bedarf es einer vorherigen schriftlichen Vereinbarung über die Kostentragung.

(6) Soweit ein Transport des Speichermediums vor Löschung unverzichtbar ist, wird der Auftragnehmer angemessene Maßnahmen zu dessen Schutz, insbesondere gegen Entwendung, unbefugtem Lesen, Kopieren oder Verändern, treffen. Die Maßnahmen und die anzuwendenden Löschverfahren werden bei Bedarf ergänzend zu den Leistungsbeschreibungen konkretisierend vereinbart.

(7) 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 der Auftraggeberin übergeben.

(8) Die Auftraggeberin kann jederzeit, d. h. sowohl während der Laufzeit als auch nach Beendigung des Vertrages, die Berichtigung, Löschung, Verarbeitungseinschränkung (Sperrung) und Herausgabe von Daten durch den Auftragnehmer verlangen, solange der Auftragnehmer die Möglichkeit hat, diesem Verlangen zu entsprechen.

(9) Der Auftragnehmer berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn die Auftraggeberin dies anweist. Die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien übernimmt der Auftragnehmer aufgrund einer Einzelbeauftragung durch

die Auftraggeberin, sofern nicht im Vertrag anders vereinbart. In besonderen, von der Auftraggeberin zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an die Auftraggeberin weiterleiten.

(10) Sollte der Auftraggeberin eine Rücknahme der Daten nicht möglich sein, wird sie den Auftragnehmer rechtzeitig schriftlich informieren. Der Auftragnehmer ist dann berechtigt, personenbezogene Daten im Auftrag der Auftraggeberin zu löschen.

(11) Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung bzgl. einer Löschung nicht erforderlich, diese müssen gelöscht werden.

§ 13 Unterauftragnehmer

☐ Unterauftragsverhältnisse sind nicht erlaubt

Eine Weitergabe von Aufträgen der im Hauptvertrag vereinbarten Tätigkeiten an Unterauftragnehmer durch den Auftragnehmer erfolgt nicht.

- oder -

☐ Unterauftragsverhältnisse sind erlaubt (wenn ausgewählt, gelten nachfolgende Bestimmungen)

(1) Der Auftragnehmer nimmt keinen Unterauftragnehmer ohne vorherige explizite schriftliche oder allgemeine schriftliche Genehmigung der Auftraggeberin in Anspruch. Dies gilt in gleicher Weise für den Fall, dass weitere Unterauftragsverhältnisse durch Unterauftragnehmer begründet werden. Der Auftragnehmer stellt sicher, dass eine entsprechende Genehmigung der Auftraggeberin für alle im Zusammenhang mit der vertragsgegenständlichen Verarbeitung eingesetzten weiteren Unterauftragnehmer vorliegt.

(2) Die nachfolgenden Regelungen finden sowohl für den Unterauftragnehmer als auch für alle in der Folge eingesetzten weiteren Unterauftragnehmer entsprechende Anwendung.

(3) Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragnehmer die Auftraggeberin immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern, wodurch die Auftraggeberin die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Verweigert die Auftraggeberin durch ihren Einspruch die Zustimmung aus anderen als aus wichtigen Gründen, kann der Auftragnehmer den Vertrag zum Zeitpunkt des geplanten Einsatzes des Unterauftragnehmers kündigen.

(4) Die Auftraggeberin ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht. Hierbei muss jedoch jeder Unterauftragnehmer (verbundenes Unternehmen) vor Beauftragung der Auftraggeberin schriftlich angezeigt werden, sodass die Auftraggeberin bei Vorliegen wichtiger Gründe die Beauftragung untersagen kann.

(5) Zum Zeitpunkt des Abschlusses dieser Vereinbarung sind die in der Anlage 1 aufgeführten Unternehmen als Unterauftragnehmer für Teilleistungen für den Auftragnehmer tätig und verarbeiten und/oder nutzen in diesem Zusammenhang auch unmittelbar die Daten der Auftraggeberin. Für diese Unterauftragnehmer gilt die Einwilligung für das Tätigwerden als erteilt.

(6) Der Auftragnehmer muss Unterauftragnehmer unter besonderer Berücksichtigung der Eignung hinsichtlich der Erfüllung der zwischen Auftraggeberin und Auftragnehmer vereinbarten technischen und organisatorischen Maßnahmen gewissenhaft auswählen.

(7) Ist der Auftragnehmer im Sinne dieser Vereinbarung befugt, die Dienste eines Unterauftragnehmers in Anspruch zu nehmen, um bestimmte Verarbeitungstätigkeiten im Namen der Auftraggeberin auszuführen, so werden diesem Unterauftragnehmer im Wege eines Vertrags dieselben Pflichten auferlegt, die in dieser Vereinbarung zwischen der Auftraggeberin und dem Auftragnehmer festgelegt sind, insbesondere hinsichtlich der Anforderungen an Vertraulichkeit,

Datenschutz und Datensicherheit zwischen den Vertrags-partnern dieses Vertrages sowie den in diesem AV-Vertrag beschriebenen Kontroll- und Überprüfungsrechten der Auftraggeberin. Hierbei müssen ferner hinreichend Garantien dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt.

(8) Durch schriftliche Aufforderung ist die Auftraggeberin berechtigt, vom Auftragnehmer Auskunft über die datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

(9) Ein zustimmungspflichtiges Unterauftragnehmerverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei Personal-, Post- und Versanddienstleistungen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten der Auftraggeberin auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen. Die Nebenleistungen sind vorab detailliert zu benennen.

(10) Kommt der Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber der Auftraggeberin für die Einhaltung der Pflichten jenes Unterauftragnehmers.

§ 14 Zurückbehaltungsrecht

Die Einrede des Zurückbehaltungsrechts, gleich aus welchem Rechtsgrund, an den vertragsgegenständlichen Daten sowie an evtl. vorhandenen Datenträgern wird ausgeschlossen.

§ 15 Haftung

(1) Auftraggeberin und Auftragnehmer haften für den Schaden, der durch eine nicht der DSGVO 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
- er den aus der DSGVO resultierenden und speziell für Auftragsverarbeiter auferlegten Pflichten nicht nachgekommen ist oder
- er unter Nichtbeachtung der rechtmäßig erteilten Anweisungen der Auftraggeberin handelte oder
- er gegen die rechtmäßig erteilten Anweisungen der Auftraggeberin gehandelt hat.

(3) Soweit die Auftraggeberin zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihr der Rückgriff auf den Auftragnehmer vorbehalten.

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

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

§ 16 Schriftformklausel

Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Regelungen handelt. Das Schriftformerfordernis gilt auch für den Verzicht auf dieses Formerfordernis.

§ 17 Salvatorische Klausel

(1) 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 Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt.
(2) An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.
(3) Erweist sich der Vertrag als lückenhaft, gelten die Bestimmungen als vereinbart, die dem Sinn und Zweck des Vertrages entsprechen und im Falle des Bedachtwerdens vereinbart worden wären.
(4) Existieren mehrere wirksame und durchführbare Bestimmungen, welche die unter Abs. 1 genannte unwirksame Regelung ersetzen können, so muss die Bestimmung gewählt werden, welche den Schutz der Patientendaten im Sinne dieses Vertrages am besten gewährleistet.

§ 18 Rechtswahl und Gerichtsstand

(1) Es gilt deutsches Recht.
(2) Gerichtsstand ist der Sitz der Auftraggeberin.

Anlagen

Anlage 1: Unterauftragsverhältnis beim Auftragnehmer zum Zeitpunkt der Auftragsvergabe

Anlage 2: Nachweis der allgemeinen technischen und organisatorischen Maßnahmen

Anlage 3: Ergänzende Hinweise zu § 8 zur Wahrung des Berufsgeheimnisses nach § 203 StGB

Anlage 4: Ergänzende Hinweise zum Patientendatenschutz gem. LKHG M-V

_____ , den _____ _____
Ort Datum Auftraggeber

_____ , den _____ _____
Ort Datum Auftraggeber

_____ , den _____ _____
Ort Datum Auftragnehmer

Anlage 1: Unterauftragsverhältnis beim Auftragnehmer zum Zeitpunkt der Auftragsvergabe

☐ Das Ausfüllen dieser Anlage ist nicht erforderlich, da keine Unterauftragsverhältnisse bestehen.

Folgende ausschließliche Unterauftragsverhältnisse beim Auftragnehmer bestehen zum Zeitpunkt der Auftragsvergabe:

Name und Anschrift des Unterauftragnehmers	Beschreibung der Teilleistungen	Ort der Leistungserbringung

Anlage 2: Nachweis der allgemeinen technischen und organisatorischen Maßnahmen

Es werden folgende technische und organisatorische Maßnahmen i. S. d. Art. 32 DSGVO von der Auftraggeberin und dem Auftragnehmer für die im Hauptvertrag und/oder alleinig im AV-Vertrag vereinbarte Leistungserfüllung getroffen. Diese Maßnahmen sollen dazu dienen, langfristig und umfangreich ein angemessenes Schutzniveau für die personenbezogenen Daten zu gewährleisten und die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen.

Im Nachfolgenden sind alle zutreffenden Maßnahmen vom Auftragnehmer **anzukreuzen.** Ist eine Maßnahme nicht relevant bzw. wird diese in abgeänderter Form realisiert, ist dies entsprechend zu **begründen**.

Für den Geltungsbereich dieses AV-Vertrages liegen folgende Zertifizierungen[1] des Informationssicherheitsmanagementsystems (ISMS) vor:

☐ BSI IT-Grundschutz	Zertifikatsnummer:	gültig bis:
☐ ISO 27001	Zertifikatsnummer:	gültig bis:
☐ Branchenspezifischer Sicherheitsstandard (B3S)	Zertifikatsnummer:	gültig bis:
☐ Sonstige:	Zertifikatsnummer:	gültig bis:

I. Vertraulichkeit (Art. 32 Ziff. 1 DSGVO)

1. Zutrittskontrolle

Es gilt entsprechende Maßnahmen zu realisieren, die geeignet sind, um unbefugten Personen den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Dazu zählen u. a. Angaben zur Gebäudesicherung (bei mehreren Orten bitte eine differenzierte Auflistung der jeweiligen Sicherungsmaßnahmen nach einzelnen Orten, Rechenzentren usw. vornehmen).

☐ Es sind keine Maßnahmen diesbezüglich erforderlich, weil:

☐ Es existieren keine Maßnahmen diesbezüglich, weil:

[1] das jeweils gültige Zertifikat (inkl. Nennung des Geltungsbereiches) ist dieser Anlage beizufügen

☐ Es existieren Maßnahmen diesbezüglich in folgender Form:

☐ **Schließkonzept**

- ☐ dokumentierte/r Vergabe/Entzug von Zutritts-Berechtigungen
- ☐ personifiziertes Zutrittsmedium (bspw. Schlüssel, Zutrittsausweis, Zutrittskarte)
- ☐ auf das Minimum eingeschränkter Personen-kreis für Server- und IT-Betriebsräume
- ☐ Richtlinie zur Herstellung eines Verschluss-zustandes (Fenster, Türen etc.)
- ☐ Begleitung von Besuchern in Server- und IT-Betriebsräume
- ☐ Besucherprotokollierung für Server- und IT-Betriebsräume

Bemerkung bzw. Begründung bei Irrelevanz:

☐ **Zutrittskontrolle für Serverräume**

- ☐ permanent
- ☐ außerhalb der regulären Arbeitszeiten
- ☐ selbstverriegelndes System bzw. Türknauf
- ☐ zyklische Kontrolle auf Unregelmäßigkeiten

Bemerkung bzw. Begründung bei Irrelevanz:

☐ **Zutrittskontrolle für IT-Betriebsräume**

- ☐ permanent
- ☐ außerhalb der regulären Arbeitszeiten
- ☐ selbstverriegelndes System bzw. Türknauf
- ☐ zyklische Kontrolle auf Unregelmäßigkeiten

Bemerkung bzw. Begründung bei Irrelevanz:

☐ **Zutrittskontrollen an Gebäudeeingängen**

- ☐ permanent
- ☐ außerhalb der regulären Arbeitszeiten
- ☐ mittels Schließanlage
- ☐ mittels Pförtnerdienst
- ☐ mittels Wachdienst

Bemerkung bzw. Begründung bei Irrelevanz:

☐ **Pförtnerdienst**

- ☐ permanent
- ☐ außerhalb der regulären Arbeitszeiten

Bemerkung bzw. Begründung bei Irrelevanz:

☐ **Wachdienst**

- ☐ permanent
- ☐ außerhalb der regulären Arbeitszeiten

Bemerkung bzw. Begründung bei Irrelevanz:

☐ **Alarm-/Einbruchmeldeanlagen**

- ☐ Fenster und Türen
- ☐ Server- und IT-Betriebsräume

Bemerkung bzw. Begründung bei Irrelevanz:

☐ **optisch-elektronische Überwachung**
- ☐ permanent
- ☐ außerhalb der regulären Arbeitszeiten

Bemerkung bzw. Begründung bei Irrelevanz:

☐ **Sorgfältige Auswahl von Reinigungs-personal**
- ☐ Zutritt besteht permanent
- ☐ Zutritt erfolgt ausschließlich begleitet

Bemerkung bzw. Begründung bei Irrelevanz:

☐ **Sonstiges**

2. Zugangskontrolle

Es gilt entsprechende Maßnahmen zu realisieren, die geeignet sind um zu verhindern, dass Datenverarbeitungssysteme von unbefugten Personen genutzt werden können.

☐ Es sind keine Maßnahmen diesbezüglich erforderlich, weil:

☐ Es existieren keine Maßnahmen diesbezüglich, weil:

☐ Es existieren Maßnahmen diesbezüglich in folgender Form:

☐ **personifizierte Benutzerprofile**
- ☐ dokumentierte Erstellung/Sperrung von Benutzerprofilen
- ☐ Authentifikation via Benutzername und Passwort
- ☐ gültige Passwortrichtlinie für alle IT-Systeme (definierte Zeichenlänge:)
- ☐ Nutzer besitzen grundsätzlich keine administrativen Berechtigungen (Trennung von Administratoren- und Nutzer-Accounts)
- ☐ dokumentierte Änderung von Berechtigungen

Bemerkung bzw. Begründung bei Irrelevanz:

☐ **allgemeine Gerätesicherheit**
- ☐ IT-Systeme sind grundsätzlich zugangsgeschützt
- ☐ Pflicht zum Sperren beim Verlassen von IT-Systemen
- ☐ zeitgesteuerte automatische Bildschirmsperre
- ☐ Pre-Boot-Authentication
- ☐ grundsätzliche Sperrung aller nichtbenötigten Schnittstellen (USB, Bluetooth etc.)
- ☐ zugangsgeschützte Aufbewahrung von Datenträgern
- ☐ für neue Hard-/Software existiert vor Inbetriebnahme ein Freigabeprozess
- ☐ Einsatz von Anti-Virenschutzsystemen
- ☐ Einsatz von Firewall-Systemen
- ☐ Einsatz von Intrusion-Detection/Prevention-Systemen
- ☐ Zugangsschutz zum internen Netzwerk via 802.1x und/oder NAC.System

☐ Einsatz von Mobile-Device-Management-systemen (u. a. Fernlöschmöglichkeiten)

Bemerkung bzw. Begründung bei Irrelevanz:

☐ **Heim- und Telearbeitsplätze**

☐ gültige Sicherheitsrichtlinie bzw. Verfahrens-beschreibung für Fernzugänge
☐ Einsatz von verschlüsselten Fernzugängen (bspw. via verschlüsselten VPN)
☐ Einsatz einer 2-Faktor-Authentifizierung

Bemerkung bzw. Begründung bei Irrelevanz:

☐ **Sonstiges**

3. Zugriffskontrolle

Es gilt entsprechende Maßnahmen zu realisieren, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems berechtigten Personen 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.

☐ Es sind keine Maßnahmen diesbezüglich erforderlich, weil:

☐ Es existieren keine Maßnahmen diesbezüglich, weil:

☐ Es existieren Maßnahmen diesbezüglich in folgender Form:

☐ **Verwaltung von Zugriffsberechtigungen**

☐ gültiges Berechtigungskonzept
☐ Zugriffsberechtigungsvergaben erfolgen auf schriftlichen Antrag innerhalb eines revisions-sicheren Genehmigungsworkflows
☐ Vergabe von Zugriffsberechtigungen (Lesen, Schreiben, Ändern) auf Laufwerks-, Ordner- und Dateiebene via Berechtigungsgruppen
☐ Anwendung des Least-Privilege-Prinzips

Bemerkung bzw. Begründung bei Irrelevanz:

☐ **Protokollierung von Zugriffs-berechtigungen**

☐ Protokollierung von Authentifizierungs-vorgängen (insb. An- und Abmeldungen)

Bemerkung bzw. Begründung bei Irrelevanz:

☐ **Einsatz von Verschlüsselungsverfahren**

☐ Datenträgerverschlüsselung auf mobilen IT-Systemen (u. a. Smartphones, Laptops etc.)
☐ Datenträgerverschlüsselung auf stationären IT-Systemen
☐ Kommunikationsverschlüsselung zwischen hausinternen IT-Systemen *innerhalb* der Institution

☐ Kommunikationsverschlüsselung zwischen hausinternen IT-Systemen *außerhalb* der Institution
☐ Kommunikationsverschlüsselung zwischen hausinternen IT-Systemen und Vertragspartnern

Bemerkung bzw. Begründung bei Irrelevanz:

☐ **Sonstiges**

4. Trennungsgebot

Es gilt entsprechende Maßnahmen zu realisieren, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet und auch gespeichert werden können.

☐ Es sind keine Maßnahmen diesbezüglich erforderlich, weil:

☐ Es existieren keine Maßnahmen diesbezüglich, weil:

☐ Es existieren Maßnahmen diesbezüglich in folgender Form:

☐ **Mandantentrennung** ☐ physisch ☐ logisch

Bemerkung bzw. Begründung bei Irrelevanz:

☐ **Trennung von Test- und Produktivsystemen**
Bemerkung bzw. Begründung bei Irrelevanz:

☐ **Getrennte und zugangsgeschützte Aufbewahrung der jeweiligen Zuordnungsdatei im Zusammenhang der Verarbeitung von pseudonymisierten Daten**

Bemerkung bzw. Begründung bei Irrelevanz:

☐ **Sonstiges**

II. Integrität

1. Eingabekontrolle (Audit Trail)

Es gilt entsprechende Maßnahmen zu realisieren, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

☐ Es sind keine Maßnahmen diesbezüglich erforderlich, weil:

☐ Es existieren keine Maßnahmen diesbezüglich, weil:

☐ Es existieren Maßnahmen diesbezüglich in folgender Form:

☐ **Protokollierung für kundendaten-speichernde Systeme**

- ☐ Zugriffe auf Betriebssystem- und Anwendungssystemebene
- ☐ stichprobenartige Auswertung der Protokolldaten
- ☐ Eingabe, Veränderung und Löschung von Daten auf Dateiebene

Bemerkung bzw. Begründung bei Irrelevanz:

☐ **Sonstiges**

2. Weitergabekontrolle

Es gilt entsprechende Maßnahmen zu realisieren, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

☐ Es sind keine Maßnahmen diesbezüglich erforderlich, weil:

☐ Es existieren keine Maßnahmen diesbezüglich, weil:

☐ Es existieren Maßnahmen diesbezüglich in folgender Form:

☐ **Sicherer physischer Transport von Datenträgern**

- ☐ ausschließliche Weitergabe an autorisierte Personen
- ☐ Nutzung von sicheren Transportbehältern/ -verpackungen
- ☐ Datenträgerverschlüsselung
- ☐ sorgfältige Auswahl von Transport-dienstleistern bzw. Transportpersonal
- ☐ dokumentierter Transport

Bemerkung bzw. Begründung bei Irrelevanz:

☐ **Datenträgerentsorgung**

- ☐ gem. Sicherheitsrichtlinie im Rahmen eines vordefinierten und dokumentierten Workflows nach dem aktuellen Stand der Technik
- ☐ sichere physische Löschung von Daten-trägern vor Wiederverwendung
- ☐ Einsatz von normenkonformen Akten-vernichtern

☐ Kooperation mit zertifizierten Dienstleistern

Bemerkung bzw. Begründung bei Irrelevanz:

☐ **Einsatz von elektronischen Signaturen/ Zertifikaten**
☐ zur Identitätsbestätigung
☐ zum verschlüsselten Datentransport

Bemerkung bzw. Begründung bei Irrelevanz:

☐ **Sonstiges**

III. Verfügbarkeit und Belastbarkeit

Es gilt entsprechende Maßnahmen zu realisieren, die gewährleisten, dass personenbezogene Daten gegen unbeabsichtigte Zerstörung oder Verlust geschützt sind.

☐ Es sind keine Maßnahmen diesbezüglich erforderlich, weil:

☐ Es existieren keine Maßnahmen diesbezüglich, weil:

☐ Es existieren Maßnahmen diesbezüglich in folgender Form:

- ☐ Einsatz von unterbrechungsfreien Stromversorgungen und Netzersatzanlagen
- ☐ angemessene Klimatisierung der IT-Infrastruktur
- ☐ Einsatz von Geräten zur Überwachung der Temperatur/Feuchtigkeit in IT-Betriebs-/Serverräumen
- ☐ angepasste Aufteilung der Stromkreise
- ☐ Blitzschutzeinrichtungen
- ☐ Feuer- und Rauchmeldeanlagen
- ☐ Einhaltung von Brandschutzvorschriften
- ☐ Vorliegen eines gültigen Backup- und Wiederherstellungskonzeptes
- ☐ Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort
- ☐ Überprüfung der Wiederherstellbarkeit von Datensicherungen
- ☐ Testverfahren für neu einzusetzende Hard- und Software
- ☐ Vorliegen eines gültigen Notfallplans
- ☐ Patch- und Änderungsmanagement

Bemerkung bzw. Begründung bei Irrelevanz:

☐ Sonstiges: _____

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

1. Auftragskontrolle

Es gilt Maßnahmen zu realisieren, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen der Auftraggeberin verarbeitet werden können.

Es existieren Maßnahmen diesbezüglich in folgender Form:

- **konsequente Einholung von Verpflichtungserklärungen im Rahmen der Auftragserteilung von Dienstleistern**
- **Auswahl der Auftragnehmer erfolgt unter Sorgfaltsgesichtspunkten (insb. hinsichtlich Datenschutz und Informationssicherheit)**
- **Verpflichtung der Mitarbeiter/innen des Auftragnehmers auf Vertraulichkeit**
- **Verpflichtung der Mitarbeiter/innen des Auftragnehmers auf die Verschwiegenheit gemäß § 203 StGB**
- **Vereinbarung von wirksamen Kontrollrechten gegenüber dem Auftragnehmer**
- **kontinuierliche Überprüfung des Auftragnehmers hinsichtlich der vertraglich vereinbarten Schutzmaßnahmen**

☐ **Vorabüberprüfung der beim Auftraggeber dokumentierten Sicherheitsmaßnahmen**

Bemerkung bzw. Begründung bei Irrelevanz:

☐ **Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer**

Bemerkung bzw. Begründung bei Irrelevanz:

☐ **Sicherstellung der rechtskonformen Datenlöschung im Zuge der Auftragsbeendigung**

Bemerkung bzw. Begründung bei Irrelevanz:

☐ **Sonstiges**

2. Sonstige Maßnahmen

Es existieren sonstige Maßnahmen in folgender Form:

- **Verpflichtung zur regelmäßigen Schulung der Mitarbeiter/innen hinsichtlich der geltenden datenschutzrechtlichen Bestimmungen sowie der Informationssicherheit**
- **Führen eines Verzeichnisses von Verarbeitungstätigkeiten gem. Art. 30 DSGVO**

☐ **Etablierung eines Prozesses zur Durchführung der Datenschutz-Folgenabschätzung**

Bemerkung bzw. Begründung bei Irrelevanz:

☐ **Etablierung eines Prozesses zur Wahrung der Betroffenenrechte**

Bemerkung bzw. Begründung bei Irrelevanz:

☐ **Sonstiges**

Anlage 3: Ergänzende Hinweise zu § 8 des AV-Vertrags

§ 203 Verletzung von Privatgeheimnissen Strafgesetzbuch (StGB)

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als
   1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,
   2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung,
   3. Rechtsanwalt, Kammerrechtsbeistand, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten oder Organ oder Mitglied eines Organs einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft,
   4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist,
   5. Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes,
   6. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder
   7. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstelle

   anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als
   1. Amtsträger,
   2. für den öffentlichen Dienst besonders Verpflichteten,
   3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt,
   4. Mitglied eines für ein Gesetzgebungsorgan des Bundes oder eines Landes tätigen Untersuchungsausschusses, sonstigen Ausschusses oder Rates, das nicht selbst Mitglied des Gesetzgebungsorgans ist, oder als Hilfskraft eines solchen Ausschusses oder Rates,
   5. öffentlich bestelltem Sachverständigen, der auf die gewissenhafte Erfüllung seiner Obliegenheiten auf Grund eines Gesetzes förmlich verpflichtet worden ist, oder
   6. Person, die auf die gewissenhafte Erfüllung ihrer Geheimhaltungspflicht bei der Durchführung wissenschaftlicher Forschungsvorhaben auf Grund eines Gesetzes förmlich verpflichtet worden ist,

   anvertraut worden oder sonst bekanntgeworden ist. Einem Geheimnis im Sinne des Satzes 1 stehen Einzelangaben über persönliche oder sachliche Verhältnisse eines anderen gleich, die für Aufgaben der öffentlichen Verwaltung erfaßt worden sind; Satz 1 ist jedoch nicht anzuwenden, soweit solche Einzelangaben anderen Behörden oder sonstigen Stellen für Aufgaben der öffentlichen Verwaltung bekanntgegeben werden und das Gesetz dies nicht untersagt.

(3) Kein Offenbaren im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen. Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.

(4) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als mitwirkende Person oder als bei den in den Absätzen 1 und 2 genannten Personen tätiger Beauftragter für den Datenschutz bekannt geworden ist. Ebenso wird bestraft, wer
   1. als in den Absätzen 1 und 2 genannte Person nicht dafür Sorge getragen hat, dass eine sonstige mitwirkende Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind,
   2. als im Absatz 3 genannte mitwirkende Person sich einer weiteren mitwirkenden Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, bedient und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind, oder
   3. nach dem Tod der nach Satz 1 oder nach den Absätzen 1 oder 2 verpflichteten Person ein fremdes Geheimnis unbefugt offenbart, das er von dem Verstorbenen erfahren oder aus dessen Nachlass erlangt hat.

(5) Die Absätze 1 bis 4 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.

(6) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

§ 204 Verwertung fremder Geheimnisse Strafgesetzbuch (StGB)

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein Betriebs- oder Geschäftsgeheimnis, zu dessen Geheimhaltung er nach § 203 verpflichtet ist, verwertet, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) § 203 Absatz 5 gilt entsprechend.

§ 205 Strafantrag Strafgesetzbuch (StGB)

(1) In den Fällen des § 201 Abs. 1 und 2 und der §§ 202, 203 und 204 wird die Tat nur auf Antrag verfolgt. Dies gilt auch in den Fällen der §§ 201a, 202a, 202b und 202d, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

(2) Stirbt der Verletzte, so geht das Antragsrecht nach § 77 Abs. 2 auf die Angehörigen über; dies gilt nicht in den Fällen der §§ 202a, 202b und 202d. Gehört das Geheimnis nicht zum persönlichen Lebensbereich des Verletzten, so geht das Antragsrecht bei Straftaten nach den §§ 203 und 204 auf die Erben über. Offenbart oder verwertet der Täter in den Fällen der §§ 203 und 204 das Geheimnis nach dem Tod des Betroffenen, so gelten die Sätze 1 und 2 sinngemäß.

§ 53a Zeugnisverweigerungsrecht der mitwirkenden Personen Strafprozessordnung (StPO)

(1) Den Berufsgeheimnisträgern nach § 53 Absatz 1 Satz 1 Nummer 1 bis 4 stehen die Personen gleich, die im Rahmen
   1. eines Vertragsverhältnisses,
   2. einer berufsvorbereitenden Tätigkeit oder
   3. einer sonstigen Hilfstätigkeit

   an deren beruflicher Tätigkeit mitwirken. Über die Ausübung des Rechts dieser Personen, das Zeugnis zu verweigern, entscheiden die Berufsgeheimnisträger, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann.

(2) Die Entbindung von der Verpflichtung zur Verschwiegenheit (§ 53 Absatz 2 Satz 1) gilt auch für die nach Absatz 1 mitwirkenden Personen.

§ 97 Beschlagnahmeverbot Strafprozessordnung (StPO)

(1) Der Beschlagnahme unterliegen nicht
   1. schriftliche Mitteilungen zwischen dem Beschuldigten und den Personen, die nach § 52 oder § 53 Abs. 1 Satz 1 Nr. 1 bis 3b das Zeugnis verweigern dürfen;
   2. Aufzeichnungen, welche die in § 53 Abs. 1 Satz 1 Nr. 1 bis 3b Genannten über die ihnen vom Beschuldigten anvertrauten Mitteilungen oder über andere Umstände gemacht haben, auf die sich das Zeugnisverweigerungsrecht erstreckt;
   3. andere Gegenstände einschließlich der ärztlichen Untersuchungsbefunde, auf die sich das Zeugnisverweigerungsrecht der in § 53 Abs. 1 Satz 1 Nr. 1 bis 3b Genannten erstreckt.

(2) Diese Beschränkungen gelten nur, wenn die Gegenstände im Gewahrsam der zur Verweigerung des Zeugnisses Berechtigten sind, es sei denn, es handelt sich um eine elektronische Gesundheitskarte im Sinne des § 291a des Fünften Buches Sozialgesetzbuch. Die Beschränkungen der Beschlagnahme gelten nicht, wenn bestimmte Tatsachen den Verdacht begründen, dass die zeugnisverweigerungsberechtigte Person an der Tat oder an einer Datenhehlerei, Begünstigung, Strafvereitelung oder Hehlerei beteiligt ist, oder wenn es sich um Gegenstände handelt, die durch eine Straftat hervorgebracht oder zur Begehung einer Straftat gebraucht oder bestimmt sind oder die aus einer Straftat herrühren.

(3) Die Absätze 1 und 2 sind entsprechend anzuwenden, soweit die Personen, die nach § 53a Absatz 1 Satz 1 an der beruflichen Tätigkeit der in § 53 Absatz 1 Satz 1 Nummer 1 bis 3b genannten Personen mitwirken, das Zeugnis verweigern dürfen.

(4) Soweit das Zeugnisverweigerungsrecht der in § 53 Abs. 1 Satz 1 Nr. 4 genannten Personen reicht, ist die Beschlagnahme von Gegenständen unzulässig. Dieser Beschlagnahmeschutz erstreckt sich auch auf Gegenstände, die von den in § 53 Abs. 1 Satz 1 Nr. 4 genannten Personen den an ihrer Berufstätigkeit nach § 53a Absatz 1 Satz 1 mitwirkenden Personen anvertraut sind. Satz 1 gilt entsprechend, soweit die Personen, die nach § 53a Absatz 1 Satz 1 an der beruflichen Tätigkeit der in § 53 Absatz 1 Satz 1 Nummer 4 genannten Personen mitwirken, das Zeugnis verweigern dürften.

(5) Soweit das Zeugnisverweigerungsrecht der in § 53 Abs. 1 Satz 1 Nr. 5 genannten Personen reicht, ist die Beschlagnahme von Schriftstücken, Ton-, Bild- und Datenträgern, Abbildungen und anderen Darstellungen, die sich im Gewahrsam dieser Personen oder der Redaktion, des Verlages, der Druckerei oder der Rundfunkanstalt befinden, unzulässig. Absatz 2 Satz 3 und § 160a Abs. 4 Satz 2 gelten entsprechend, die Beteiligungsregelung in Absatz 2 Satz 3 jedoch nur dann, wenn die bestimmten Tatsachen einen dringenden Verdacht der Beteiligung begründen; die Beschlagnahme ist jedoch auch in diesen Fällen nur zulässig, wenn sie unter Berücksichtigung der Grundrechte aus Artikel 5 Abs. 1 Satz 2 des Grundgesetzes nicht außer Verhältnis zur Bedeutung der Sache steht und die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Täters auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Anlage 4: Ergänzende Hinweise zum Patientendatenschutz gem. LKHG M-V

§ 33 LKHG M-V Rechtmäßigkeit der Datenverarbeitung

(1) Die Verarbeitung personenbezogener Daten von Patientinnen und Patienten durch das Krankenhaus ist zulässig, soweit dies zur Erfüllung des mit den Patientinnen und Patienten oder zu deren Gunsten abgeschlossenen Behandlungsvertrages einschließlich der Erfüllung der ärztlichen Dokumentationspflicht und der Pflegedokumentation, zur sozialen und seelsorgerlichen Betreuung der Patientinnen und Patienten und zur Leistungsabrechnung und Abwicklung von Ansprüchen, die mit der Behandlung im Zusammenhang stehen, erforderlich ist.

(2) Soweit dies gemäß Absatz 1 erforderlich ist, dürfen die Daten gegenüber Behandlungseinrichtungen anderer Fachrichtungen desselben Krankenhauses offenbart werden. Die Offenbarung gegenüber Dritten außerhalb des Krankenhauses zu Zwecken des Absatzes 1 oder der Durchführung einer Mit- oder Nachbehandlung ist nur zulässig, soweit diese ihrerseits zur Verarbeitung der Daten befugt sind und die Patientin oder der Patient nichts anderes bestimmt hat.

(3) Die Offenbarung der personenbezogenen Daten zum Zweck der Unterrichtung von Angehörigen oder anderen Bezugspersonen ist zulässig, wenn kein gegenteiliger Wille durch die Patientin oder den Patienten kundgetan wurde, die Einwilligung der Patientin oder des Patienten nicht rechtzeitig erlangt werden kann und keine sonstigen Anhaltspunkte dafür bestehen, dass eine Übermittlung nicht angebracht ist.

§ 34 LKHG M-V Weitere Verarbeitung von Daten

(1) Eine Verarbeitung personenbezogener Daten von Patientinnen und Patienten zu einem anderen als in § 33 Absatz 1 genannten Zweck ist nur zulässig, wenn dies

1. zur Geltendmachung von zivilrechtlichen Ansprüchen des Krankenhauses oder zur Abwehr entsprechender Ansprüche sowie zur Verfolgung von Straftaten oder Ordnungswidrigkeiten Dritter,
2. zur Durchführung qualitätssichernder Maßnahmen,
3. zu Planungszwecken und Wirtschaftlichkeits- und Organisationsuntersuchungen,
4. zu im öffentlichen Interesse liegenden Forschungszwecken nach § 37,
5. zur im Krankenhaus durchgeführter Aus-, Fort- und Weiterbildung in ärztlichen oder anderen Fachberufen des Gesundheitswesens,
6. zur Rechnungsprüfung durch den Krankenhausträger, einer von ihm beauftragten Wirtschaftsprüferin oder eines von ihm beauftragten Wirtschaftsprüfers oder den Landesrechnungshof und zur Überprüfung der Wirtschaftlichkeit durch Beauftragte gemäß § 113 des Fünften Buches Sozialgesetzbuch oder
7. zur Meldung nach § 15b Absatz 2 des Gesetzes über den Öffentlichen Gesundheitsdienst über die Durchführung einer Kinderuntersuchung nach § 26 Absatz 1 des Fünften Buches Sozialgesetzbuch in Verbindung mit der Kinder-Richtlinie des Gemeinsamen Bundesausschusses

erforderlich ist.

(2) Zu Zwecken nach Absatz 1 Nummer 2, 3 und 5 sind die Daten in einer Weise zu verarbeiten, bei der die Identifizierung von betroffenen Personen nicht oder nicht mehr möglich ist. Sind die Zwecke auf diese Weise nicht zu erreichen, ist die Verarbeitung von pseudonymisierten Daten zulässig, soweit nicht überwiegende schutzwürdige Interessen der betroffenen Person entgegenstehen. Die pseudonymisierten Daten sind zu anonymisieren oder zu löschen, sobald der Zweck es zulässt, spätestens jedoch nach Ablauf eines Jahres nach der Zweckänderung. Die Einschränkung gilt nicht, wenn Aus-, Fort- oder Weiterzubildende unter der Aufsicht von Fachpersonal unmittelbar an der Erfüllung des Behandlungsvertrages mitwirken.

(3) Die Verarbeitung zum Zweck des Absatzes 1 Nummer 1 und 6 darf nur durch oder unter der Verantwortung von Personen erfolgen, die einem Berufsgeheimnis unterliegen.

(4) Empfänger, denen nach diesem Gesetz personenbezogene Daten von Patientinnen und Patienten offenbart werden, haben diese Daten unbeschadet sonstiger Datenschutzbestimmungen und Geheimhaltungspflichten in demselben Umfang geheim zu halten wie das Krankenhaus selbst.

(5) Soweit die Vorschriften dieses Gesetzes auf Empfänger, denen die Daten zu den Zwecken nach Absatz 1 offenbart werden, keine Anwendung finden, ist eine Offenbarung nur zulässig, wenn die Empfänger sich zur Einhaltung der Vorschriften nach Absatz 2 bis 4 verpflichten.

(6) Soweit personenbezogene Daten von Patientinnen und Patienten an andere Empfänger offenbart werden, hat der Verantwortliche die Zwecke und Rechtsgrundlagen der Offenbarung, die Empfänger, die Kategorien der offenbarten Daten und den Kreis der betroffenen Personen zu dokumentieren. Der Datenschutzbeauftragte des Krankenhauses ist zu beteiligen.

§ 37 LKHG M-V Datenverarbeitung für Forschungszwecke

(1) Die Verarbeitung und Nutzung von personenbezogenen Daten von Patientinnen und Patienten, die im Rahmen des § 33 Absatz 1 erhoben worden sind, sind für Forschungszwecke zulässig, wenn die Patientinnen und Patienten eingewilligt haben.

(2) Ohne Einwilligung der Patientinnen und Patienten dürfen die Daten nach Absatz 1 nur für bestimmte, im öffentlichen Interesse liegende Forschungsvorhaben verarbeitet werden, soweit

1. schutzwürdige Belange der Patientinnen und Patienten wegen der Art der Daten, ihrer Offenkundigkeit oder der Art ihrer Nutzung nicht beeinträchtigt werden oder
2. das für die Aufsicht für das Krankenhaus zuständige Ministerium festgestellt hat, dass das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange der Patientinnen und Patienten erheblich überwiegt und der Zweck des Forschungsvorhabens auf andere Weise, insbesondere mit anonymisierten Daten, nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(3) Personenbezogene Daten von Patientinnen und Patienten sind für Forschungszwecke zu anonymisieren. Kann der Forschungszweck auf diese Weise nicht erreicht werden, ist die Verarbeitung mit pseudonymisierten Daten zulässig. Eine Treuhandstelle mit Sitz in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den europäischen Wirtschaftsraum, deren Mitarbeiterinnen und Mitarbeiter einem Berufsgeheimnis oder einer vergleichbaren gesetzlichen Verschwiegenheitspflicht unterliegen, kann zur Pseudonymisierung und der Speicherung der Merkmale, mit deren Hilfe ein Patientenbezug hergestellt werden kann, im Rahmen der Auftragsverarbeitung nach Artikel 28 oder einer gemeinsamen Verantwortlichkeit nach Artikel 26 der Datenschutz-Grundverordnung herangezogen werden.

(4) Jede weitere Verarbeitung der Daten unterliegt den Anforderungen nach Absatz 1 bis 3. Der Verantwortliche hat sich vor der Offenbarung davon zu überzeugen, dass der Empfänger bereit und in der Lage ist, diese Vorschriften einzuhalten. Die Forschung betreibende Stelle darf Patientendaten nur mit schriftlicher Einwilligung der betroffenen Person veröffentlichen.

(5) Ärztinnen und Ärzte dürfen für eigene Forschungszwecke Dateien mit personenbezogenen Daten ihrer Patientinnen und Patienten nur mit Einwilligung der betroffenen Person anlegen.

(6) Soweit die Vorschriften dieses Gesetzes auf den Empfänger keine Anwendung finden, dürfen personenbezogene Daten von Patientinnen und Patienten nur offenbart werden, wenn der Empfänger sich verpflichtet, die Vorschriften nach Absatz 2 bis 4 einzuhalten und sich insoweit der Kontrolle des Landesbeauftragten für den Datenschutz unterwirft.

§ 38 LKHG M-V Datenverarbeitung im Auftrag

(1) Der Verantwortliche darf die Verarbeitung von personenbezogenen Daten von Patientinnen und Patienten einem Auftragnehmer übertragen, wenn

1. Störungen im Betriebsablauf sonst nicht vermieden werden können,
2. die Datenverarbeitung dadurch erheblich kostengünstiger gestaltet werden kann oder
3. das Krankenhaus seinen Betrieb einstellt.

Dem Auftragnehmer dürfen Patientendaten nur insoweit offenbart werden, als dies für die Auftragserfüllung erforderlich ist.

(2) Eine über drei Monate hinausgehende Speicherung von Patientendaten durch einen Auftragnehmer ist außerhalb des Krankenhauses nur zulässig, wenn die Patientendaten auf getrennten Datenträgern gespeichert sind, die der Auftragnehmer für den Krankenhausträger verwahrt.

(3) Soweit die Auftragsverarbeitung nicht auf eine ausdrückliche Einwilligung der Patientinnen und Patienten gestützt werden kann, ist die Verarbeitung im Auftrag nur durch Personen zulässig, die einem Berufsgeheimnis nach § 203 Absatz 1 und 2 des Strafgesetzbuches unterliegen oder nach § 203 Absatz 4 des Strafgesetzbuches zur Verschwiegenheit verpflichtet sind.

(4) Übernimmt ein Auftragnehmer nach einer Betriebseinstellung eines Krankenhauses den gesamten Bestand der Patientendaten, gelten für ihn als verantwortliche Stelle hinsichtlich der Verarbeitung dieser Daten die Vorschriften dieses Abschnitts. Bei der Übernahme ist vertraglich sicherzustellen, dass die Patientinnen und Patienten für die Dauer von zehn Jahren nach Abschluss der Behandlung oder Untersuchung auf Verlangen in gleicher Weise wie bisher beim Krankenhaus Auskunft und Einsicht erhalten.

(5) Eine Auftragsverarbeitung außerhalb des Geltungsbereichs des Grundgesetzes ist nur zulässig, wenn die Patientin oder der Patient in die Auftragsverarbeitung im Ausland ausdrücklich eingewilligt hat oder der Auftragsverarbeiter nach dem Recht seines Sitzlandes selbst einer gesetzlichen Geheimhaltungspflicht unterliegt.

§ 39 LKHG M-V Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen den Vorschriften dieses Gesetzes personenbezogene Daten, die nicht offenkundig sind,

1. erhebt, speichert, unbefugt verwendet, verändert, übermittelt, weitergibt, zum Abruf bereithält oder löscht,
2. abruft, einsieht, sich anderweitig verschafft, durch Vortäuschung falscher Tatsachen an sich oder andere zu übermitteln veranlasst oder
3. bei zu Forschungszwecken nach § 37 Absatz 3 pseudonymisierten Daten einen Personenbezug herstellt.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße von bis zu 50 000 Euro geahndet werden.

Ist die Handlung gleichzeitig eine Ordnungswidrigkeit nach Artikel 83 Absatz 4 bis 6 der Datenschutz-Grundverordnung, finden die Bestimmungen der Absätze 1 und 2 keine Anwendung.