Rahmenvertrag zur Auftragsverarbeitung nach Art. 28 DSGVO zwischen

Universitätsklinikum Köln -AöR-
Kerpener Str. 62, 50937 Köln,

vertreten durch den Vorstandsvorsitzenden und den Kaufmännischen Direktor
(Verantwortlicher im Sinne der DSGVO, nachfolgend „Auftraggeber“ genannt),
und

(Auftragsverarbeiter im Sinne der DSGVO, nachfolgend „Auftragnehmer“ genannt)

Präambel

Dieser Rahmenvertrag zur Auftragsverarbeitung („Rahmen-AV-Vertrag“) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien und findet Anwendung auf alle Leistungen der Auftragsverarbeitung im Sinne des Art. 28 DSGVO, die der Auftragnehmer gegenüber dem Auftraggeber auf Grundlage von bestehenden und zukünftigen Hauptverträgen (z. B. Lieferung, Service, Installation) erbringt, insbesondere auf alle Tätigkeiten, bei denen Mitarbeiterinnen und Mitarbeiter des Auftragnehmers oder von ihm Beauftragte weitere Auftragsverarbeiter Zugriff auf personenbezogene Daten des Auftraggebers oder von Dritten haben können.

Die Bestimmungen dieses Rahmenvertrages haben Vorrang gegenüber Regelungen in Einzelverträgen. Spezielle, im Einzelnen von diesem Rahmenvertrag abweichende Regelungen gehen diesem Rahmenvertrag nur dann vor, wenn sie ausdrücklich auf diesen Rahmenvertrag Bezug nehmen.

Im Falle von relevanten Änderungen der bestehenden oder bei Abschluss künftiger Hauptverträge werden die Anlagen im erforderlichen Umfang angepasst/ergänzt.

§ 1 Definitionen

Es gelten die Begriffsbestimmungen entsprechend Art. 4 DSGVO, § 2 UWG und § 1 Abs. 4 DDG sowie § 2 BDSG. Sollten in den Artikeln bzw. Paragraphen sich widersprechende Darstellungen zu finden sein, gelten die Definitionen in der Rangfolge DSGVO, Landesrecht, UWG und DDG. Weiterhin gelten folgende Begriffsbestimmungen:

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)

Unterauftragnehmer

Vom Auftragnehmer beauftragter Leistungserbringer, dessen Dienstleistung und/oder Werk der Auftragnehmer zur Erbringung der in diesem Vertrag beschriebenen Leistungen gegenüber dem Auftraggeber benötigt.

Verarbeitung im Auftrag

Verarbeitung im Auftrag ist die Verarbeitung personenbezogener Daten durch einen Auftragnehmer im Auftrag des Auftraggebers.

Weisung

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

§ 2 Gegenstand des Auftrags

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag und nach Weisung des Auftraggebers. Die konkrete Beschreibung des Gegenstandes, der Art, des Zweckes und der Dauer der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber ergeben sich aus der in bestehenden und künftigen Hauptverträgen im Sinne der Präambel enthaltenen Leistungsbeschreibung.

(2) 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.

(3) Der Auftragnehmer erhält Zugriff auf die in der ***Anlage 1*** aufgeführten personenbezogenen Daten (dadurch, dass der Auftraggeber ihm die Daten bereitstellt oder ihm einen Zugriff auf die Daten ermöglicht), bzw. der Auftraggeber erlaubt dem Auftragnehmer, die in der ***Anlage 1*** aufgeführten personenbezogenen Daten zu verarbeiten.

(4) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf die in ***Anlage 1*** näher spezifizierten personenbezogenen Daten der ebenfalls in ***Anlage 1*** näher spezifizierten betroffenen Personen. Bei der Verarbeitung der nachfolgend definierten Kategorien von Daten gilt Folgendes:

a. Wenn der Auftragnehmer Gesundheitsdaten im Auftrag und nach Weisung des Auftraggebers verarbeitet, sind Gesundheitsdaten alle Informationen über den früheren, gegenwärtigen und

zukünftigen Gesundheitszustand der betroffenen Person und alle Informationen, die im Rahmen der Administration des Gesundheitswesens erfasst oder verarbeitet werden sowie alle Ergebnisse aus Laboruntersuchungen zu der betroffenen Person, inklusive genetischer Daten (insb. Art. 4 Nr. 15 DSGVO).

b. Wenn der Auftragnehmer Patientendaten im Auftrag und nach Weisung des Auftraggebers verarbeitet, sind Patientendaten personenbezogene Daten von Patienten im Rahmen der Erbringung von Gesundheitsdienstleistungen.

c. Wenn der Auftragnehmer personenbezogene Patientendaten von Betroffenen verarbeitet, die an einer klinischen Studie teilnehmen, dürfen der Auftraggeber und der Auftragnehmer in diesem Zusammenhang ausschließlich Patientendaten verarbeiten, die zuvor durch den Prüfarzt pseudonymisiert wurden. Der Auftragnehmer wird in diesem Fall ebenfalls ausschließlich pseudonyme Patientendaten verarbeiten, es sei denn, dass er gesetzlich zu einer Verarbeitung von Klardaten verpflichtet oder hierfür ausdrücklich vom Betroffenen bestimmt worden ist (insb. § 40b Abs. 6 AMG).

d. Wenn der Auftragnehmer Sozialdaten im Auftrag und nach Weisung des Auftraggebers verarbeitet, sind Sozialdaten personenbezogene Daten, die von einem Leistungsträger nach dem Sozialgesetzbuch verarbeitet werden (§ 67 Abs. 2 SGB X). Sozialdaten dürfen durch nicht-öffentliche Stellen nur im Auftrag verarbeitet werden, wenn beim Auftraggeber sonst Störungen im Betriebsablauf auftreten können oder die übertragenen Aufgaben beim Auftragnehmer erheblich kostengünstiger besorgt werden können (§ 80 Abs. 3 SGB X).

e. Wenn der Auftragnehmer Sozial- und/oder Gesundheitsdaten im Wege des Cloud-Computing-Dienstes im Auftrag und nach Weisung des Auftraggebers verarbeitet, ist ein Cloud-Computing-Dienst eine im Rahmen von Cloud Computing angebotene Dienstleistung der Informationstechnik. Dies beinhaltet unter anderem Infrastruktur, Plattformen und Software (§ 393 SGB V).

f. Wenn der Auftragnehmer Forschungsdaten im Auftrag und nach Weisung des Auftraggebers verarbeitet, sind Forschungsdaten personenbezogene Daten, die zu wissenschaftlichen oder historischen Forschungszwecken verarbeitet werden. Der Auftraggeber und der Auftragnehmer müssen in diesem Fall die Forschungsdaten pseudonymisieren, sofern dies nach dem Forschungszweck möglich ist (Art. 89 Abs. 1 DSGVO). Die Forschungsdaten sind zu löschen, sobald der Forschungszweck dies erlaubt.

g. Wenn der Auftragnehmer Beschäftigtendaten und Personalstammdaten im Auftrag und nach Weisung des Auftraggebers verarbeitet, sind Personalstammdaten alle Grundinformationen über Beschäftigte, die keiner stetigen Veränderung unterliegen, wie z. B. Vor- und Nachname, Anschrift, Bankverbindung, Personalnummer (insb. § 26 BDSG).

h. Wenn der Auftragnehmer Personalaktendaten im Auftrag und nach Weisung des Auftraggebers verarbeitet, sind Personalaktendaten die in der Personalakte gespeicherten personenbezogenen Daten, die die persönlichen und dienstlichen Verhältnisse des Beschäftigten betreffen und in einem unmittelbaren inneren Zusammenhang mit dem Beschäftigungsverhältnis stehen. Personalaktendaten von Beamten dürfen durch nicht-öffentliche Stellen nur im Auftrag verarbeitet werden, wenn beim Auftraggeber sonst Störungen im Geschäftsablauf auftreten können oder der Auftragnehmer die übertragenen Aufgaben erheblich kostengünstiger erledigen kann und die beim Auftragnehmer mit der Datenverarbeitung beauftragten Beschäftigten besonders dem Schutz der Personalakten verpflichtet sind (insb. § 91a LBG NRW).

§ 3 Verantwortlichkeit

(1) Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenverarbeitung bei Wahrung des Schutzes des Datengeheimnisses (Art. 28 DSGVO, § 203 StGB) verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Ziff. 7 DSGVO).

(2) Die Inhalte dieses Rahmen-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) Auftraggeber sowie Auftragnehmer müssen gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Verschwiegenheit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Dazu müssen alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, auf das Datengeheimnis verpflichtet und über ihre Datenschutzpflichten belehrt werden. Dies gilt insbesondere, soweit es sich um Daten handelt, die dem Schutz von § 203 StGB unterliegen.

(4) 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.

(5) Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich Personen, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken und unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei 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, wenn sie nicht zuvor dafür Sorge getragen hat, dass die weitere mitwirkende Person zur Geheimhaltung verpflichtet wurde.

(6) 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 mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des Auftraggebers 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.

(7) Jede Partei ist für die Verpflichtung des eigenen Personals zuständig. Ferner müssen die eingesetzten Personen darauf hingewiesen werden, dass das Datengeheimnis auch nach Beendigung der Tätigkeit fortbesteht.

(8) Der Auftraggeber und der Auftragnehmer sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

(9) Sofern der Auftragnehmer eine nicht-öffentliche Stelle mit Sitz in Nordrhein-Westfalen ist und Personalaktendaten verarbeitet werden, unterwirft sich der Auftragnehmer der Kontrolle der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen. Sofern der Auftragnehmer seinen Geschäftssitz nicht in Nordrhein-Westfalen hat, erklärt er sich damit einverstanden, dass der Auftraggeber den Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen über den Abschluss dieses Vertrages informiert.

§ 4 Dauer des Auftrags

(1) Die Laufzeit dieses Rahmen-AV-Vertrages richtet sich nach der Laufzeit der Hauptverträge, sofern sich aus den Bestimmungen dieses Rahmen-AV-Vertrages nicht etwas anderes ergibt.

(2) Es ist den Vertragspartnern bewusst, dass ohne Vorliegen eines gültigen Rahmen-AV-Vertrages z. B. bei Beendigung des vorliegenden Vertragsverhältnisses, keine (weitere) Auftragsverarbeitung durchgeführt werden darf.

(3) Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

(4) Kündigungen bedürfen zu ihrer Wirksamkeit der Schriftform.

§ 5 Weisungsbefugnis des Auftraggebers

(1) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Auftraggebers. 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 den Auftraggeber vor Beginn der Verarbeitung über die entsprechenden rechtlichen Anforderungen. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann.

(2) Die Weisungen des Auftraggebers werden vom Auftraggeber in Textform dokumentiert und dem Auftragnehmer auf erste Anforderung als unterschriebene Kopie zur Verfügung gestellt.

(3) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind von der Weisungsbefugnis des Auftraggebers gedeckt und entsprechend zu dokumentieren. Bei einer wesentlichen Änderung des Auftrags steht dem Auftragnehmer ein Widerspruchsrecht zu. Besteht der Auftraggeber 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 dem Auftraggeber 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 der Auftraggeber 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) Die weisungsbefugten Personen des Auftraggebers sind die in **Anlage 4 unter Punkt 1** benannten Personen.

§ 6 Leistungsort

(1) Der Auftragnehmer wird die vertraglichen Leistungen in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) erbringen. Dies gilt in gleicher Weise für etwaige Unterauftragnehmer. Die zum Zeitpunkt der Auftragserteilung vereinbarten Leistungsstandorte sind in **Anlage 2** dargestellt. Erfolgt eine Leistungserbringung in einem Drittland, garantiert der Auftragnehmer die Einhaltung der gesetzlichen Vorgaben und weist dies auf Verlangen nach.

(2) Der Auftraggeber 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 den Auftraggeber geltenden gesetzlichen Bestimmungen gegen diese Verlagerung sprechen. Die Nachweispflicht hierzu liegt bei dem Auftragnehmer.

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

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

(5) Wenn der Auftragnehmer die geschuldeten Leistungen ganz oder teilweise von einem Standort außerhalb der EU/EWR in einem sog. „Drittstaat“ erbringen möchte bzw. die Leistungserbringung dorthin zu verlagern plant, wird der Auftragnehmer zuvor die schriftliche Zustimmung durch den Auftraggeber einholen. Sofern kein angemessenes Datenschutzniveau im Sinne des Art. 45 DSGVO besteht, muss ein angemessenes Datenschutzniveau mittels geeigneter Garantien im Sinne des Art. 46 DSGVO hergestellt werden. Sofern die Leistungserbringung Sozialdaten betrifft, ist die Verarbeitung nur zulässig in der EU, dem EWR oder wenn sonst ein Angemessenheitsbeschluss nach Art. 45 DSGVO vorliegt (§ 80 Abs. 2 SGB X). Wenn im Rahmen der Leistungserbringung Sozial- und Gesundheitsdaten im Wege eines Cloud-Computing-Dienstes verarbeitet werden, ist die Verarbeitung nur zulässig in der EU, dem EWR, der Schweiz oder wenn sonst ein Angemessenheitsbeschluss im Sinne des Art. 45 DSGVO vorliegt und wenn die datenverarbeitende Stelle, d.h. der Anbieter der Cloud-Dienste, eine Niederlassung in Deutschland hat (§ 393 Abs. 2 SGB V).

(6) Bei einer Leistungserbringung zu einem Leistungsort, bei dem ein angemessenes Datenschutzniveau vorliegt, wird der Auftraggeber seine Zustimmung zur Verlagerung nicht unbillig verweigern. Die Einhaltung der diesbezüglichen Vorgaben der DSGVO wird durch den Auftragnehmer gewährleistet und nachgewiesen.

(7) 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.

(8) 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 und dies nachweisen.

§ 7 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers 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 des Auftraggebers vor Missbrauch und Verlust treffen, die den Anforderungen der entsprechenden datenschutzrechtlichen

Bestimmungen entsprechen; diese Maßnahmen muss der Auftragnehmer auf Anfrage dem Auftraggeber und ggfs. Aufsichtsbehörden gegenüber nachweisen, dies umfasst insbesondere die Pflicht, die Mitarbeiter gesondert zur Verschwiegenheit zu verpflichten. 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. Dieses Schutzniveau muss mindestens das Niveau der Informationssicherheitsanforderungen für Lieferanten der Uniklinik Köln erreichen (das entsprechende Dokument finden Sie unter: https://www.uk-koeln.de/?pbid=234282). Die Uniklinik Köln empfiehlt zudem Auftragnehmern, ein Managementsystem für den Datenschutz bzw. die Informationssicherheit umzusetzen. Dabei können anerkannte Standards wie zum Beispiel die ISO/IEC 27001 oder der BSI IT-Grundschutz als Grundlagen dienen. Wesentliche Änderungen sind zu dokumentieren.

Eine Darstellung dieser technischen und organisatorischen Maßnahmen erfolgt in **Anlage 3** zu diesem Vertrag.

(3) Der Auftragnehmer stellt dem Auftraggeber auf dessen 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 dem Auftraggeber 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 den Auftraggeber bei der Datenschutzfolgenabschätzung mit allen ihm zur Verfügung stehenden Informationen. Im Falle der Notwendigkeit einer vorherigen Konsultation der zuständigen Aufsichtsbehörde unterstützt der Auftragnehmer den Auftraggeber auch hierbei.

(6) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von fremden Geheimnissen, oder ein Betriebs- oder Geschäftsgeheimnis sowie Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln. Dem Auftragnehmer ist bekannt, dass er im Rahmen seiner Tätigkeit für den Auftraggeber als mitwirkende Person i.S.d. § 203 Abs. 3 StGB gilt und damit der Schweigepflicht unterliegt und diese einhält.

Der Auftragnehmer hat schriftlich einen Datenschutzbeauftragten benannt, der seine Tätigkeit gemäß Art. 37, 38 DSGVO (weisungsfrei und unabhängig) ausübt. Der Auftraggeber kann mit dem Datenschutzbeauftragten des Auftragnehmers direkten Kontakt aufnehmen; die Kontaktdaten sind in der **Anlage 2** unter Punkt 1 benannt.

Sofern der Auftragnehmer nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen, so benennt er einen Ansprechpartner für die Fragen zum Datenschutz im Rahmen dieser Auftragsverarbeitung. Diese Kontaktdaten sind in der **Anlage 2 unter Punkt 1** benannt.

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich schriftlich mitzuteilen. Der Auftragnehmer gewährleistet, dass die Anforderungen an den Datenschutzbeauftragten und seine Tätigkeit gemäß Art. 38 DSGVO erfüllt werden. Sofern kein Datenschutzbeauftragter beim Auftragnehmer benannt ist, benennt der Auftragnehmer dem Auftraggeber einen Ansprechpartner.

(7) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei Verstößen 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. Er trifft

die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab. Der Auftragnehmer unterstützt den Auftraggeber 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.

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

(9) Überlassene Datenträger sowie sämtliche hiervon gefertigte Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, sodass sie Dritten nicht zugänglich sind. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit seine Daten und Unterlagen betroffen sind.

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

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

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

(13) 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 Verantwortlichen im Sinne der DSGVO liegen.

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

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

(16) Der Auftragnehmer verarbeitet im Rahmen von klinischen Studien ausschließlich pseudonyme Patientendaten, es sei denn, dass er gesetzlich zu einer Verarbeitung von Klardaten verpflichtet oder hierfür ausdrücklich vom Betroffenen bestimmt worden ist. Erhält der Auftragnehmer davon Kenntnis, dass er unberechtigten Zugriff auf nicht-pseudonyme Patientendaten hat oder erhalten wird, hat er unverzüglich alle mit diesen Daten zusammenhängenden Verarbeitungsvorgänge einzustellen und den Auftraggeber hiervon unverzüglich in Textform zu unterrichten (insb. § 40 Abs. 6 AMG).

(17) Der Auftragnehmer verarbeitet Sozial- und/oder Gesundheitsdaten im Wege eines Cloud-Computing-Diensts nur, wenn die in § 6 Absatz 5 Satz 4 genannten Voraussetzungen gegeben und wenn nach dem Stand der Technik angemessene technische und organisatorische Maßnahmen zur Gewährleistung der Informationssicherheit ergriffen worden sind, wenn ein aktuelles C5-Testat des Cloud-Anbieters im Hinblick auf die C5-Basiskriterien für die im Rahmen des Cloud-Computing-

Dienstes eingesetzten Cloud-Systeme und die eingesetzte Technik vorliegt und wenn die im Prüfbericht des Testats enthaltenen, korrespondierenden Kriterien für Kunden umgesetzt sind (§ 393 SGB V).

(18) Sofern der Auftragnehmer Personalaktendaten eines Beamten im Auftrag des Auftraggebers verarbeitet, muss er neben den datenschutzrechtlichen auch die beamtenrechtlichen Vorschriften einhalten, insb. § 91a Landesbeamtengesetz NRW. Die beamtenrechtlichen Vorschriften über die Führung von Personalakten gemäß § 50 Beamtenstatusgesetz und §§ 83 bis 92 Landesbeamtengesetz NRW sind entsprechend auch auf alle nicht beamteten Beschäftigten anzuwenden, soweit nicht die Besonderheiten des Tarif- und Arbeitsrechts hinsichtlich der Aufnahme und Entfernung von bestimmten Vorgängen und Vermerken eine abweichende Behandlung erfordern. Wenn der Auftragnehmer Personalakten eines Beamten oder eines nicht beamteten Beschäftigten teilweise oder ausschließlich elektronisch führt und dafür Papierdokumente in elektronische Dokumente überträgt und in der elektronischen Akte speichert, muss er entsprechend dem Stand der Technik sicherstellen, dass die elektronischen Dokumente mit den Papierdokumenten bildlich und inhaltlich übereinstimmen, wenn sie lesbar gemacht werden. Die übertragenen Papierdokumente sind nach der Übertragung in elektronische Dokumente zu vernichten, sobald ihre weitere Aufbewahrung nicht mehr aus rechtlichen Gründen oder zur Qualitätssicherung des Übertragungsvorgangs erforderlich ist. Der Auftragnehmer darf nur Beschäftigten, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, Zugang zur Personalakte gewähren und dies auch nur, soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist. Die mit Angelegenheiten der Innenrevision beauftragten Beschäftigten dürfen Zugang zur Personalakte erhalten, soweit sie die zur Durchführung ihrer Aufgaben erforderlichen Erkenntnisse andernfalls nur mit unverhältnismäßigem Aufwand oder unter Gefährdung des Prüfzwecks gewinnen könnten. Der Auftragnehmer muss spätestens nach Beendigung des Auftrags zur Datenverarbeitung überlassene Datenträger zurückgeben und die bei ihm gespeicherten Daten löschen, sobald diese für die Erfüllung des Auftrags nicht mehr benötigt werden (insb. § 91a LBG NRW).

(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 dem Auftraggeber 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 dem Auftraggeber auf Anforderung nachzuweisen.

§ 8 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 des Auftraggebers/Auftragnehmers:

(1) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten an Arbeitsplatzsystemen werden erst nach Freigabe durch den jeweiligen Berechtigten / zuständigen Mitarbeiter des Auftraggebers 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 vorheriger Zustimmung des Auftraggebers ausgeführt.

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

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

(5) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten werden dokumentiert und protokolliert. Der Auftraggeber ist berechtigt, Prüfungs- und Wartungsarbeiten vor, bei und nach Durchführung zu kontrollieren. Bei Fernzugriffen ist der Auftraggeber – 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) des Auftraggebers nur in dem Umfang – auch in zeitlicher Hinsicht – Gebrauch machen, wie dies für die ordnungsgemäße Durchführung der beauftragten Wartungs- und Prüfungsarbeiten notwendig ist.

(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) des Auftraggebers notwendig ist, wird der Auftragnehmer die vorherige Einwilligung des Auftraggebers einholen.

(8) Tätigkeiten zur Fehleranalyse, bei denen ein Datenabzug der Wirkdaten erforderlich ist, bedürfen der vorherigen Einwilligung des Auftraggebers. 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 des Auftraggebers oder auf solchem des Auftragnehmers verwendet werden, sofern die vorherige Einwilligung des Auftraggebers vorliegt. Wirkdaten dürfen nicht ohne Zustimmung des Auftraggebers auf mobile Speichermedien (Smartphones/Notebooks, 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.

§ 9 Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Der Auftraggeber wird in seinem 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) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Der Auftraggeber ist hinsichtlich der vom Auftragnehmer eingesetzten und vom Auftraggeber 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) Dem Auftraggeber obliegen die aus Art. 33, 34 DSGVO resultierenden Informationspflichten gegenüber der Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen.

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

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

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

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

§ 10 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unter dem Aspekt ausgewählt, dass dieser hinreichende 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. Er dokumentiert das Ergebnis seiner Auswahl.

Hierfür kann er beispielsweise

a) datenschutzspezifische Zertifizierungen oder Datenschutzsiegel und -prüfzeichen berücksichtigen,

b) schriftliche Selbstauskünfte des Auftragnehmers einholen,

c) sich ein Testat eines Sachverständigen vorlegen lassen oder

d) 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 des Auftraggebers oder der im Vertrag getroffenen Festlegungen vor, so kann eine darauf bezogene Prüfung auch ohne rechtzeitige Anmeldung vorgenommen werden. Eine Störung des Betriebsablaufs beim Auftragnehmer sollte auch hierbei weitestgehend vermieden werden.

(3) Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftraggeber 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, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind.

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

§ 11 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 des Auftraggebers.

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

(3) In besonderen, vom Auftraggeber zu bestimmenden Fällen erfolgt eine Aufbewahrung bzw. Übergabe der betreffenden Datenträger. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(4) Nach Abschluss der vertraglichen Arbeiten – oder früher nach Aufforderung durch den Auftraggeber – hat der Auftragnehmer

a) sämtliche im Rahmen des Auftrags in seinen Besitz gelangten Unterlagen oder Datenträger,

b) erstellte Verarbeitungsergebnisse,

c) Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehendem Auftraggeber auszuhändigen oder auf Anweisung des Auftraggebers datenschutzkonform zu löschen bzw. zu vernichten, sofern keine gesetzliche Pflicht zur Aufbewahrung besteht. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(5) 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.

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

(7) Der Auftraggeber 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.

(8) Sollte dem Auftraggeber eine Rücknahme der Daten nicht möglich sein, wird er den Auftragnehmer rechtzeitig schriftlich informieren. Der Auftragnehmer ist dann berechtigt, personenbezogene Daten im Auftrag des Auftraggebers zu löschen.

§ 12 Unterauftragnehmer

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in **Anlage 2 Punkt 3** (*sofern zutreffend*) genannten Unterauftragnehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Unterauftragnehmern („Unterauftragnehmerverhältnis“) befugt, soweit er den Auftraggeber hiervon vorab in Kenntnis setzt und dieser der Beauftragung des Unterauftragnehmers schriftlich zugestimmt hat.

Der Auftragnehmer ist verpflichtet, Unterauftragsnehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Bei der Einschaltung von Unterauftragsnehmern hat der Auftragnehmer diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) ggf. direkt gegenüber den Unterauftragsnehmern wahrnehmen kann. Sofern eine Einbeziehung von Unterauftragsnehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Unterauftragsnehmer ein angemessenes Datenschutzniveau gewährleistet ist. Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Unterauftragsnehmern nachweisen. Die Einschaltung eines Unterauftragnehmers mit Sitz außerhalb der EU/des EWR ist entgegen § 6 Absatz 1 ausnahmsweise zulässig, wenn die in § 6 Absatz 5 genannten Voraussetzungen erfüllt sind.

(2) Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragnehmer den Auftraggeber immer über jede beabsichtigte Änderung 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 zum Zeitpunkt des geplanten Einsatzes des Unterauftragnehmers kündigen.

(3) Der Auftraggeber 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 dem Auftraggeber schriftlich angezeigt werden, sodass der Auftraggeber bei Vorliegen wichtiger Gründe die Beauftragung untersagen kann.

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

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

(6) Ein zustimmungspflichtiges Unterauftragnehmerverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei Personal-, Post- und Versanddienstleistungen, sofern sichergestellt werden kann, dass ein Zugriff auf personenbezogene Daten für den Unterauftragnehmer nicht möglich ist. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen. Die Nebenleistungen sind vorab detailliert zu benennen.

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

§ 13 Zurückbehaltungsrecht

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

§ 14 Haftung

(1) Auftraggeber 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 insbesondere für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der

a) er denen aus der DSGVO resultierenden und speziell für Auftragsverarbeiter auferlegten Pflichten nicht nachgekommen ist oder

b) er unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers handelte oder

c) er gegen die rechtmäßig erteilten Anweisungen des Auftraggebers gehandelt hat.

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

(4) Im Innenverhältnis zwischen Auftraggeber und Auftragnehmer haftet der Auftragnehmer für den durch eine Verarbeitung verursachten Schaden insbesondere, wenn er

a) seinen ihm speziell durch die DSGVO auferlegten Pflichten nicht nachgekommen ist oder

b) unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers oder gegen diese Anweisungen gehandelt hat.

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

§ 15 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.

§ 16 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 § 16 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.

§ 17 Rechtswahl, Gerichtsstand

(1) Es gilt deutsches Recht.

(2) Gerichtsstand ist der Sitz des Auftraggebers.

Auftraggeber:

Ort, Datum	(Unterschrift)
	(Unterschrift)

Auftragnehmer:

Ort, Datum	(Unterschrift)
	(Unterschrift)