Anlage 5 - **Auftragsverarbeitung**

zum TKmed® Teilnehmervertrag

Inhaltsverzeichnis

1 Präambel

Diese Anlage konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der im Teilnehmervertrag TKmed®, im Folgenden als Hauptvertrag in Bezug genommen, in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben.

Gemäß dem Hauptvertrag ist es erforderlich, dass der Auftragnehmer personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO des Auftraggebers verarbeitet, für die der Auftraggeber als datenschutzrechtlich Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO fungiert. Sämtliche in diesem Vertrag beschriebenen Verpflichtungen finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag und seine Vertragsanlagen in Zusammenhang stehen und bei denen Mitarbeiterinnen und Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte, mit personenbezogenen Daten des Auftraggebers in Berührung kommen bzw. kommen können.

Es gelten die Begriffsbestimmungen entsprechend Art. 4 DS-GVO, § 2 UWG und § 2 TMG sowie das Landesdatenschutzgesetz und ggf. das Landeskrankenhausgesetz des Landes der verantwortlichen Stelle.

Im Falle von Widersprüchen zwischen diesem Vertrag und Regelungen aus sonstigen Vereinbarungen, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus diesem Vertrag vor.

2 Verantwortlichkeit

Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenverarbeitung verantwortlich („Verantwortlicher" im Sinne des Art. 4 Ziff. 7 DS-GVO).

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.

Auftraggeber sowie Auftragnehmer müssen gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

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

3 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.

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

Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

Kündigungen bedürfen zu ihrer Wirksamkeit der Schriftform.

4 Weisungsbefugnis des Auftraggebers

Der Umgang mit den Daten des Auftraggebers 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.

Die Weisungen des Auftraggebers werden vom Auftraggeber dokumentiert und dem Auftragnehmer unmittelbar nach erfolgter Dokumentation als unterschriebene Kopie zur Verfügung gestellt.

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.

Es kann gerade vorkommen, dass eine schnelle Reaktion des Auftragnehmers erforderlich ist, welche eine vorherige schriftliche Beauftragung nicht ermöglicht. Reagiert der Auftragnehmer hier auf eine mündliche Beauftragung seitens des Auftraggebers, um Schaden von Betroffenen abzuwenden, so muss der Auftraggeber eine schriftliche Beauftragung nachreichen.
Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich (in Textform) bestätigen.

5 Leistungsort

Der Auftragnehmer wird die vertraglichen Leistungen in Deutschland erbringen, etwaige Unterauftragnehmer an den mit dem Auftraggeber in Kapitel 18.4 vereinbarten Leistungsstandorten in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR).

Erfolgt eine Leistungserbringung durch den Auftragnehmer in einem Drittland, garantiert der Auftragnehmer die Einhaltung der diesbezüglichen Vorgaben der DS-GVO und weist dies auf Verlangen nach. Dies gilt in gleicher Weise für etwaige Unterauftragnehmer.

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.

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.

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 den Auftraggeber einholen.

Bei einer Leistungserbringung in einem sicheren Drittstaat wird der Auftraggeber seine Zustimmung zur Verlagerung nicht unbillig verweigern. Die Einhaltung der diesbezüglichen Vorgaben der DS-GVO wird durch den Auftragnehmer gewährleistet.

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.

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.

6 Pflichten des Auftragnehmers

Der Auftragnehmer darf Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen.

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. Dieser Nachweis beinhaltet insbesondere die Umsetzung der aus Art. 32 DS-GVO 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 Kapitel 19 dieses Vertrags.

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.

Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen, Privatgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln. Der Auftragnehmer gewährleistet, dass alle Personen welche im Rahmen der Auftragsverarbeitung tätig sind, zusätzlich zur Wahrung des Datengeheimnisses nach Art. 28 Abs. 3 S. 2 lit. b DS-GVO, sofern notwendig, zur Wahrung des Fernmeldegeheimnisses entsprechend §88 TKG, zur Wahrung von Geschäfts- und Betriebsgeheimnisse nach §17 UWG bzw. Privatgeheimnisse nach § 203 StGB, verpflichtet sind.

Als Datenschutzbeauftragter ist beim Auftragnehmer derzeit die in Kapitel 18.5 angegebene Person benannt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich schriftlich mitzuteilen.

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 DS-GVO.

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.

Überlassene Datenträger sowie sämtliche hiervon gefertigten 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.

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.

Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde bei dem Auftragnehmer ermittelt, sofern die Auftragsverarbeitung oder die Daten des Auftraggebers von den Kontrollen oder Maßnahmen betroffen sind oder Gegenstand der Maßnahmen oder Kontrollen sind.

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.

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 DS-GVO liegen.

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.

Sofern, der Auftragnehmer Patientendaten im Auftrag verarbeitet, speichert er keine Patientendaten auf Systemen, die außerhalb der Verfügungsgewalt des Auftraggebers liegen bzw. die nicht dem Beschlagnahmeschutz unterliegen.

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.

Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren, zu dokumentieren und in geeigneter Weise gegenüber dem Auftraggeber auf Anforderung nachzuweisen.

7 Verpflichtungserklärung des Auftragnehmers zur Verschwiegenheit nach § 203 Strafgesetzbuch (StGB)

Wenn der Auftraggeber Daten verarbeitet, die einem Berufsgeheimnis nach § 203 StGB unterliegen, gilt folgendes: Der Auftragnehmer wirkt als Dienstleister an den Tätigkeiten der Berufsgeheimnisträger mit, die einer beruflichen Verschwiegenheitsverpflichtung unterliegen.

Der Auftragnehmer sowie seine Unterauftragnehmer sind zur Verschwiegenheit über alle im Rahmen der Dienstleistungs- und Supportleistungserbringung bekannt werdenden Vorgänge und Daten verpflichtet. Die Verschwiegenheitspflicht besteht auch nach Beendigung des Hauptvertrags fort.

Der Auftragnehmer ist verpflichtet, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist. Der Auftragnehmer hat seine Mitarbeiter zur Verschwiegenheit schriftlich zu verpflichten und anzuhalten, soweit sie in Erfüllung dieser Vereinbarung für den Auftraggeber tätig werden und auf die strafrechtlichen Folgen einer Verletzung der Verschwiegenheitspflicht, insbesondere auf § 203 StGB, hinzuweisen.

Der Auftragnehmer ist in Kenntnis, dass eine Verletzung dieser Schweigepflicht sowie das Unterlassen der Geheimhaltungsverpflichtung weiterer mitwirkender Personen oder Unterauftragnehmer Anlass zu einem Strafverfahren sein können. Die einschlägigen strafrechtlichen Vorschriften sind: § 203 Abs. 1, Abs. 3, Abs. 4 StGB.

Die Pflicht zur Verschwiegenheit gemäß den vorstehenden Absätzen besteht nicht, soweit der Auftragnehmer auf Grund einer behördlichen oder gerichtlichen Entscheidung zur Offenlegung von vertraulichen Informationen des Auftraggebers verpflichtet ist. Soweit dies im Einzelfall zulässig und möglich ist, wird der Auftragnehmer den Auftraggeber über die Pflicht zur Offenlegung vorab in Kenntnis setzen.

8 Fernzugriff auf Systeme des Auftraggebers bei Prüfung/Wartung 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 die in Kapitel 18.6 getroffenen Vereinbarungen zu den Rechten und Pflichten des Auftraggebers und Auftragnehmers.

9 Pflichten des Auftraggebers

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.

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

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.

Dem Auftraggeber obliegen die aus Art. 33, 34 DS-GVO resultierenden Informationspflichten gegenüber der Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen.

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

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

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

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

Der Auftraggeber hat den Auftragnehmer unter dem Aspekt ausgewählt, dass dieser hinreichenden Garantien dafür bietet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Er dokumentiert das Ergebnis seiner Auswahl.

Hierfür kann er beispielsweise Selbstauskünfte, Zertifikate und Prüfberichte beim Auftragnehmer einholen, 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.

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.

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

Während der laufenden Beauftragung berichtigt, löscht oder sperrt der Auftragnehmer die vertragsgegenständlichen Daten nur auf Anweisung des Auftraggebers.

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 den Auftraggeber. Dies gilt nicht, sofern im Hauptvertrag bereits eine entsprechende Regelung getroffen worden ist.
In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe.

Nach Abschluss der vertraglichen Arbeiten - oder früher nach Aufforderung durch den Auftraggeber - 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 dem 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.

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

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.

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.

Der Auftragnehmer berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist. Die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien übernimmt der Auftragnehmer aufgrund einer Einzelbeauftragung durch den Auftraggeber, sofern nicht im Vertrag anders vereinbart. In besonderen, vom Auftraggeber 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 den Auftraggeber weiterleiten.

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

Werden Unterauftragsverhältnisse zugelassen, gelten die folgenden zusätzlichen Vereinbarungen.

Der Auftragnehmer nimmt keinen Unterauftragnehmer ohne vorherige explizite schriftliche oder allgemeine schriftliche Genehmigung des Auftraggebers 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 des Auftragsgebers für alle im Zusammenhang mit der vertragsgegenständlichen Verarbeitung eingesetzten weiteren Unterauftragnehmer vorliegt.

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

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.

Zum Zeitpunkt des Abschlusses dieser Vereinbarung, sind die in der Kapitel 18.11 aufgeführten Unternehmen als Unterauftragnehmer für Teilleistungen für den Auftragnehmer tätig und verarbeiten und/oder nutzen in diesem Zusammenhang auch unmittelbar die Daten des Auftraggebers. Für diese Unterauftragnehmer gilt die Einwilligung für das Tätigwerden als erteilt.

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

Ist der Auftragnehmer im Sinne dieser Vereinbarung befugt, die Dienste eines Unterauftragnehmers in Anspruch zu nehmen, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, so werden diesem Unterauftragnehmer im Wege eines Vertrags dieselben Pflichten auferlegt, die in dieser Vereinbarung zwischen dem Auftraggeber und dem Auftragnehmer festgelegt sind, insbesondere hinsichtlich der Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages sowie den in diesem AV-Vertrag beschriebenen Kontroll- und Überprüfungsrechten des Auftraggebers. 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 DS-GVO erfolgt.

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.

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

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

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.

13 Zurückbehaltungsrecht

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

14 Haftung

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

Der Auftragnehmer haftet ausschließlich für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der

- er den aus der DS-GVO resultierenden und speziell für Auftragsverarbeiter auferlegten Pflichten nicht nachgekommen ist oder
- er unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers handelte oder
- er gegen die rechtmäßig erteilten Anweisungen des Auftraggebers gehandelt hat.

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

Im Innenverhältnis zwischen Auftraggeber und Auftragnehmer haftet der Auftragnehmer für den durch eine Verarbeitung verursachten Schaden jedoch nur, wenn er

- seinen ihm speziell durch die DS-GVO auferlegten Pflichten nicht nachgekommen ist oder

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

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 der Schriftform 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

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.

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.

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. Existieren mehrere wirksame und durchführbare Bestimmungen, welche die unter Kapitel 11 genannte unwirksame Regelung ersetzen können, so muss die Bestimmung gewählt werden, welche den Schutz der Patientendaten im Sinne dieses Vertrages am besten gewährleistet.

Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

17 Rechtswahl, Gerichtsstand

Es gilt deutsches Recht.

Gerichtsstand ist der Sitz des Auftragnehmers.

Auftragnehmer	Auftraggeber
_____	_____
Ort, Datum	Ort, Datum
_____	_____
Vorname Nachname	Vorname Nachname
Position	Position
Firmenname	Firmenname

18 Anlage zum Vertrag

18.1 Leistungen des Hauptvertrages

Der Auftragnehmer erbringt für den Auftraggeber die im Hauptvertrag vereinbarten Leistungen sowie folgende Tätigkeiten zur Gewährleistung der Funktionsfähigkeit der vom Auftraggeber erworbenen NEXUS / CHILI Software, insbes.

- Installation, inkl. Updates und Upgrades
- Integration mit anderen Systemen des Auftraggebers
- Konfiguration (inkl. Benutzerdaten)
- Problemanalyse bei Störungen
- Störungsbeseitigung
- Proaktive Serverüberwachung

18.2 Ansprechpartner (weisungsberechtigte Personen) des Auftraggebers

- Geschäftsführung
- IT-Leitung
- Systembetreuer
- Ärzte

18.3 Weisungsempfänger beim Auftragnehmer

- Geschäftsführung
- Teamleitung [Support]
- IT-Leitung
- Systembetreuer

18.4 Ort der vertraglichen Leistungserbringung

Der Auftragnehmer wird die vertraglichen Leistungen in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) erbringen.

Etwaige Unterauftragnehmer werden die sie betreffenden Leistungen in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) erbringen.

18.5 Datenschutzbeauftragter des Auftragnehmers

Name:	Daniel Schropp
E-Mailadresse:	datenschutz@nexus-chili.com
Telefonnummer:	06221 / 180 79-10

18.6 Fernzugriff auf Systeme des Auftraggebers

Es wird per Fernzugriff auf das System/die Systeme zugegriffen:

Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten an Arbeitsplatzsystemen werden erst nach Freigabe durch den jeweiligen Berechtigten / zuständigen Mitarbeiter des Auftraggebers durchgeführt.

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 des Auftraggebers ausgeführt.

Die Mitarbeiter des Auftragnehmers verwenden angemessene Identifizierungs- und Verschlüsselungsverfahren.

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

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.

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.

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.

Tätigkeiten zur Fehleranalyse, bei denen ein Datenabzug der Wirkbetriebsdaten 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 (PDAs, USB-Speichersticks oder ähnliche Geräte) kopiert werden.

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.

18.7 Unterauftragsverhältnisse

Unterauftragsverhältnisse sind dem Auftragnehmer erlaubt. Unterauftragsverhältnisse bedürfen einer expliziten Genehmigung durch den Auftraggeber.

18.8 Art der Daten

- Personenstammdaten wie z. B. Mitarbeiter, Kooperationspartner, nicht-medizinische Patientendaten
- Bewohner-/ Klienten-/ Patientendaten wie z. B. Geschlecht, Vorname, Nachname, Anschrift, Telefonnummer, E-Mail-Adresse, Geburtsdatum, -ort, Kundennummer, Konfession, Familienstand, Nationalität, …
- Gesundheitsdaten wie z. B. Behinderungsgrad, Krankheiten, …

- Medizinische Patientendaten wie z. B. Krankheitsbilder, Diagnosen, Pflegestufe, Rezepte, Einstufung in DRG, …
- Kontaktdaten / Kommunikationsdaten wie z B. IP-Adressen, Telefon, E-Mail

18.9 Zweck der Datenverarbeitung

- Systemwartung, Problemanalyse und –Behebung auf dem System des Auftraggebers
- Projektbetreuung bei Umsetzung von Customizing-Aufträgen und von Implementierungsaufträgen auf dem System des Auftraggebers

18.10 Kreis der Betroffenen

- Beschäftigte, Mitarbeiter
- Patienten

18.11 Untervertragsverhältnisse beim Auftragnehmer

Name und Anschrift des Unterauftragnehmers	Beschreibung der Teilleistungen
pegasus gmbh Bayernstrasse 10 93128 Regenstauf	Hosting der zentralen TKmed-Infrastruktur
Kuck & Schmidt GmbH & Co. KG Hugo-Junkers-Straße 3 60386 Frankfurt am Main	Annahme von Störungsmeldungen *außerhalb* der Standardzeiten von: werktags (Mo-Fr.) von 08:00-17:00. Weiterleitung der Meldungen an den Nacht- und Wochenendsupport
TeamViewer Germany GmbH Jahnstraße 30 73037 Göppingen	Bereitstellen der Fernwartungs-Software im Support-Fall für Screen-Sharing, Videokonferenzen und Dateitransfer

19 Technische und organisatorische Maßnahmen der NEXUS / CHILI GmbH

19.1 Zugangskontrolle

Maßnahmen, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehren.

Die Büroräume liegen im 1. und 2. OG. Türen schließen selbständig. Fenster sind außerhalb der Bürozeiten geschlossen zu halten.
Eine Alarmanlage ist vorhanden. Die Scharfschaltung nachts erfolgt automatisch.
Das Schließsystem ist transponderbasiert. Die Schlüsselausgabe ist in einer Schlüsselliste dokumentiert.
Zugänge in das Gebäude und die Büroräume werden durch das Schließsystem protokolliert. Der Zugang zum Serverraum ist in das Schließsystem integriert. Auch alle Zugänge von außen ins Gebäude sind in das Schließsystem integriert.
Es erfolgt eine sorgfältige Auswahl des Reinigungspersonals.

19.2 Datenträgerkontrolle

Maßnahmen, die das unbefugte Lesen, Kopieren, Verändern oder Löschen von Datenträgern verhindern.

Die Mitarbeiter des AN sind per Verfahrensanweisung angehalten, keine personenbezogenen Daten des AG auf tragbaren Datenträgern (z. B. CD/DVD, USB-Sticks) zu transportieren oder zu versenden.
Stattdessen werden verschlüsselte Verbindungen oder VPN-Tunnel zur Datenübertragung genutzt.
Datenträger werden vor der Entsorgung durch sichere Löschverfahren gelöscht oder physikalisch zerstört. Ausdrucke, die personenbezogene Daten enthalten, werden vor der Entsorgung geschreddert.
Alle Mitarbeiter des AN sind per Arbeitsvertrag verpflichtet, das Datengeheimnis nach § 28 DS-GVO zu bewahren.

19.3 Speicherkontrolle

Maßnahmen, die die unbefugte Eingabe von personenbezogenen Daten sowie die unbefugte Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten verhindern.

Alle verwendeten DV Systeme unterliegen einer personenbezogenen Benutzerverwaltung.
Die Benutzerverwaltung ist zentral und LDAP-basiert, das Passwort wird verschlüsselt abgelegt.
Der Zugriff auf Anwendungen wird protokolliert.

19.4 Benutzerkontrolle

Maßnahmen, die verhindern, dass Unbefugte automatisierte Verarbeitungssysteme mit Hilfe von Datenübertragung nutzen können.

Es gibt ein zentrales Firewall/VPN System. Sicherheitsupdates werden regelmäßig eingespielt.
Die Festlegung der zugangsberechtigten Mitarbeiter und ihre Benutzerrechte werden über Benutzerprofile geregelt. Die Benutzerauthentifizierung im internen Netz erfolgt durch Benutzername und Passwort. Bei Zugriff von außen wird zusätzlich ein personenbezogenes Zertifikat verwendet.
Die automatische Sperrung der Arbeitsplatzrechner ist durch eine Verfahrensanweisung geregelt.
Berechtigungen ausscheidender Mitarbeiter werden unverzüglich nach dem Ausscheiden gesperrt.
Das Firmennetzwerk ist in unterschiedliche Bereiche für Internet, DMZ, WLAN und Internes Netz unterteilt. Die Übergänge zwischen den Bereichen sowie die Zugänge nach außen und über VPN sind durch eine zentrale Firewall gesichert.
Es wird Anti-Viren-Software eingesetzt.

19.5 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

Durch ein Rechte- und Rollenkonzept in der zentralen Benutzerverwaltung ist sichergestellt, dass Benutzer nur Zugang zu Informationen erhalten, für die sie berechtigt sind.
Alle Server werden nur durch berechtigte Systemadministratoren verwaltet, die Anzahl der Administratoren ist auf das Notwendige beschränkt.
Zugriffe auf zentrale Anwendungen werden protokolliert.

19.6 Übertragungskontrolle

Maßnahmen, die gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

Jeder Zugang von außen zum Firmennetz ist nur über verschlüsselte Verbindungen (VPN/SSH) möglich.
Zugriffe von außen werden protokolliert.

19.7 Eingabekontrolle

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

Die Benutzeridentifikation erfolgt durch die Verwendung personenbezogener Accounts.
Die für die Verarbeitung personenbezogener Daten verwendeten DB-Systeme schreiben Protokollinformationen über Eingaben, Änderungen und Löschungen von Daten.

19.8 Transportkontrolle

Maßnahmen, die gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.

Die Übertragung von personenbezogenen Daten erfolgt über verschlüsselte Verbindungen oder VPN-Tunnel. Auf die Verwendung von tragbaren Datenträgern wird verzichtet.

19.9 Wiederherstellbarkeit

Maßnahmen, die gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Ein Backup- und Recovery-Konzept gewährleistet, dass Daten im Störungsfall wiederhergestellt werden können.

19.10 Zuverlässigkeit

Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

Fehlfunktionen werden automatisiert gemeldet. Zentrale Speichermedien werden gespiegelt und Anti-Viren-Software wird eingesetzt.

19.11 Datenintegrität

Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

Ein Backup- und Recovery-Konzept gewährleistet, dass Daten im Störungsfall wiederhergestellt werden können. Zentrale Speichermedien werden gespiegelt.

19.12 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des AG verarbeitet werden können.

Falls Subunternehmer mit der Verarbeitung personenbezogener Daten des AG beauftragt werden, wird dies dem AG schriftlich angezeigt.
Für die Datenverarbeitung im Auftrag wird in diesem Fall mit dem Subunternehmer ein Vertrag gemäß DS-GVO geschlossen, in dem u.a. Kontrollrechte und Weisungsbefugnisse festgelegt sind.

19.13 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Alle verwendeten Serversysteme sind über eine USV abgesichert.
Der Serverraum ist klimatisiert, die Temperatur im Serverraum wird überwacht. In allen Räumen sind Brandmelder mit direkter Verbindung zur Feuerwehr installiert. Ebenfalls existiert eine Meldeanlage für Wassereinbrüche im Serverraum.
Alle Daten werden zentral auf redundanten RAID-Systemen gehalten und unterliegen einem mehrstufigen Backupkonzept.
Der Zugang zum Serverraum ist in das Schließsystem integriert. Nur berechtigte Personen haben Zutritt. Eine Alarmanlage ist vorhanden. Die Scharfschaltung nachts erfolgt automatisch.

19.14 Trennbarkeit

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Die Trennung von Produktiv- und Testsystemen wird über getrennte Software-Instanzen auf getrennten Maschinen (Hardware-Server oder virtuelle Maschinen) realisiert.
Personenbezogene Daten, die für die Auftragserfüllung von Systemen des AG übertragen werden müssen, werden zentral in einem eigenen SAN-Bereich mit speziellen Zugriffberechtigungen und eigenem Backupkonzept abgelegt.

19.15 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit

Die technischen und organisatorischen Maßnahmen sind Teil unseres QM-Systems, welches einer regelmäßigen Prüfung unterliegt.