

## Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen der

**Städtisches Klinikum Görlitz gGmbH**  
Girbigsdorfer Straße 1 - 3  
02828 Görlitz

-----  
- als Verantwortlicher im Sinne der DS-GVO,  
nachfolgend Auftraggeber (AG) genannt -

und der

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

-----  
- als Auftragsverarbeiter im Sinne der DS-GVO,  
nachfolgend Auftragnehmer (AN) genannt -

Dieser Vertrag zur Auftragsverarbeitung (AV-Vertrag) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der im Hauptvertrag beschriebenen Auftragsverarbeitung 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 des Auftraggebers in Berührung kommen bzw. kommen können.

Zur Einhaltung der Datenschutzbestimmungen und der ärztlichen Schweigepflicht werden ausgehend von in dem Vertrag bereits getroffenen Festlegungen folgende Maßnahmen zwischen dem Auftragnehmer und dem Auftraggeber vereinbart:

### § 1 Allgemeine Regelungen

- (1) Der Auftraggeber überträgt dem Auftragnehmer die Verantwortung dafür, dass dessen Personal im Rahmen der zu erfüllenden Arbeitsaufgaben ihm zur Kenntnis gelangende Patienten- und Beschäftigendaten
  - streng vertraulich behandelt und
  - Dritten nicht zugänglich macht.
- (2) Die Verwendung von vertraulichen Informationen ist ausschließlich im Rahmen der vereinbarten Arbeitsaufgabe und nur denjenigen gestattet, die in die jeweilige Arbeitsaufgabe eingebunden und auf Informationen angewiesen sind.

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

Aus den mit dem Auftragnehmer abgeschlossenen Verträgen ergeben sich jeweils Gegenstand und Dauer des Auftrags sowie Umfang, Zweck und Art der Datenerhebung, -verarbeitung oder -nutzung. Sämtliche in dieser Vereinbarung beschriebenen Verpflichtungen finden Anwendung auf alle Tätigkeiten, die mit den mit dem Auftragnehmer abgeschlossenen Verträgen in Zusammenhang stehen und bei denen Mitarbeiterinnen und Mitarbeiter des Auftragnehmers mit personenbezogenen Daten des Auftraggebers in Berührung kommen bzw. kommen können.



Im Einzelnen sind insbesondere die folgenden Datenarten / -kategorien Bestandteil der Verarbeitung:  
(Zutreffendes ankreuzen, ggf. Angabe bei „Sonstiges“)

### Kreis der Betroffenen

- |   |   |   |
|---|---|---|
| <input type="checkbox"/> Patienten        | <input type="checkbox"/> Mitarbeiter              | <input type="checkbox"/> Lieferanten      |
| <input type="checkbox"/> Besucher/Gäste   | <input type="checkbox"/> ehemalige Mitarbeiter    | <input type="checkbox"/> Dienstleister    |
| <input type="checkbox"/> Ansprechpartner  | <input type="checkbox"/> Bewerber                 | <input type="checkbox"/> Handelsvertreter |
| <input type="checkbox"/> Interessenten    | <input type="checkbox"/> Veranstaltungsteilnehmer | <input type="checkbox"/> Kunden/Mandanten |
| <input type="checkbox"/> Sonstiges: _____ |   |   |

### Art der Daten / Datenkategorien:

- |   |  |  |
|---|--|--|
| <input type="checkbox"/> Patientenstammdaten                              | <input type="checkbox"/> Adressdaten         | <input type="checkbox"/> Bonitätsdaten       |
| <input type="checkbox"/> Gesundheitsdaten                                 | <input type="checkbox"/> Qualifikationsdaten | <input type="checkbox"/> Vertragsdaten       |
| <input type="checkbox"/> Geburtsdaten                                     | <input type="checkbox"/> Interessen          | <input type="checkbox"/> Zahlungsdaten       |
| <input type="checkbox"/> Sozialversicherungsdaten                         | <input type="checkbox"/> Zeiterfassungsdaten | <input type="checkbox"/> Abrechnungsdaten    |
| <input type="checkbox"/> Biometrische Daten                               | <input type="checkbox"/> IT-Nutzungsdaten    | <input type="checkbox"/> Videoaufzeichnungen |
| <input type="checkbox"/> Personaldaten (Name, Adresse, Gehaltsdaten usw.) |  | <input type="checkbox"/> Planungsdaten       |
| <input type="checkbox"/> Kommunikationsdaten (Telefonnummer, E-Mail, Fax) |  |  |
| <input type="checkbox"/> Sonstiges: _____                                 |  |  |

Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des in Bezug dazu stehenden Vertrages, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüber hinausgehende Verpflichtungen ergeben.

## **§ 3 Weisungsgebundene Verarbeitung und Remonstrationspflicht**

- (1) Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisung des Auftraggebers verarbeiten, es sei denn, dass er durch das Recht der Union oder dem Recht der Mitgliedstaaten, dem der Auftragnehmer unterliegt, zur Verarbeitung verpflichtet ist. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
- (2) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf hinweisen, wenn die Befolgung einer vom Auftraggeber erteilten Weisung nach seiner Ansicht gegen die DS-GVO oder eine andere Vorschrift über den Datenschutz verstößt. Der Auftragnehmer kann in diesem Fall die Durchführung der erteilten Weisung aussetzen bzw. einstellen, bis die Weisung vom Auftraggeber schriftlich bestätigt bzw. geändert wurde.

## **§ 4 Vertraulichkeits-/Verschwiegenheitspflicht**

- (1) Der Auftragnehmer wird zur Durchführung des Vertrages nur Personen beschäftigen, die er zur Vertraulichkeit verpflichtet und in geeigneter Weise mit den Anforderungen des Datenschutzes vertraut gemacht hat. Ferner müssen die eingesetzten Personen darauf hingewiesen werden, dass das Datengeheimnis auch nach Beendigung der Tätigkeit fortbesteht. Der Auftragnehmer hat sein Personal insbesondere darauf hinzuweisen, dass Verstöße gegen datenschutzrelevante Bestimmungen strafrechtliche Folgen nach sich ziehen können. Über die Verpflichtung und Unterrichtung der Beschäftigten besteht Nachweispflicht seitens des Auftragsverarbeiters gegenüber dem Auftraggeber.
- (2) Der Gesetzgeber hat Dritte, die an der Berufsausübung eines Berufsgeheimnisträgers mitwirken, in den Straftatbestand des § 203 StGB einbezogen. Die sonstige mitwirkende Person im Sinne des § 203 StGB ist zur Geheimhaltung zu verpflichten. Die Einhaltung der Verpflichtung ist sicherzustellen. Sollte es sich bei dem Personal des Auftragnehmers um Personen handeln, die nicht der Gruppe der Berufsgeheimnisträger gemäß § 203 StGB angehören, müssen diese Mitarbeiter zusätzlich auf die Pflicht zur Geheimhaltung verpflichtet werden. Die Verpflichtung erfolgt durch den Auftragnehmer. Der Auftragnehmer muss die Verpflichtung entsprechender Mitarbeiter gegenüber dem Auftraggeber nachweisen - Anlage 1.



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

- (1) Der Auftragnehmer gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den Anforderungen des Datenschutzes gerecht wird. Er ergreift dafür alle erforderlichen technischen und organisatorischen Maßnahmen gem. Art. 32 DS-GVO. Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Während der Dauer dieses Auftrags sind diese durch den Auftragnehmer fortlaufend an die Anforderungen dieses Auftrags anzupassen und dem technischen Fortschritt entsprechend weiterzuentwickeln, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.
- (2) Der Auftragnehmer verpflichtet sich, Änderungen der technischen und organisatorischen Maßnahmen, die einen wesentlichen Einfluss auf das gewährleistete Sicherheitsniveau haben schriftlich zu dokumentieren, was auch in einem elektronischen Format erfolgen kann, und dem Auftraggeber zur Kenntnis zu geben.
- (3) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung jederzeit eine aktuelle Beschreibung der getroffenen technischen und organisatorischen Maßnahmen vorzulegen, soweit diese für den Auftragsgegenstand gem. §1 dieser Vereinbarung erforderlich ist.

## § 6 Leistungsort

- (1) Der Auftragnehmer wird die vertraglichen Leistungen in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) oder in einem Drittland erbringen. Dies gilt in gleicher Weise für etwaige Unterauftragnehmer (5). Die zum Zeitpunkt der Auftragserteilung vereinbarten Leistungsstandorte sind in Anlage 2 dargestellt oder der Auftragnehmer stellt eigenes Konzept als Nachweis bereit. Erfolgt eine Leistungserbringung in einem Drittland, garantiert der Auftragnehmer die Einhaltung der diesbezüglichen Vorgaben der DS-GVO und weist dies nach.
- (2) Der Auftraggeber stimmt einer Verlagerung eines Ortes der Leistungserbringung innerhalb des Leistungslandes, für das bereits eine Zustimmung besteht, zu, wenn dort nachweislich ein gleiches Sicherheitsniveau gegeben ist und keine für den Auftraggeber geltenden gesetzlichen Bestimmungen gegen diese Verlagerung sprechen. Die Nachweispflicht hierzu liegt bei dem Auftragnehmer.
- (3) Bei einer Verlagerung des Ortes der Leistungserbringung in Länder, die Mitglied der EU/EWR sind und über ein diesem Vertrag genügendes und verifiziertes Datenschutzniveau verfügen, 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 die Verlagerung über Gründe informiert wird, die eine Verlagerung nicht zulassen, gilt die Zustimmung zu dieser Verlagerung seitens des Auftraggebers als erteilt.
- (5) Beabsichtigt der Auftragnehmer eine Datenverarbeitung außerhalb der EU/EWR, wird der Auftragnehmer zuvor die schriftliche Zustimmung durch den Auftraggeber einholen. Der Auftragnehmer weist in diesem Falle die Einhaltung der diesbezüglichen Vorgaben der DS-GVO nach. Verlagert der Auftragnehmer die Datenverarbeitung ohne Zustimmung des Auftraggebers dorthin, ist der Auftraggeber berechtigt, alle oder einzelne Verträge mit dem Auftragnehmer außerordentlich zu kündigen. Die Geltendmachung weitergehender Rechte bleibt dem Auftraggeber vorbehalten.

## § 7 Inanspruchnahme der Dienste weiterer Auftragsverarbeiter

- (1) Sofern es im Rahmen der Zusammenarbeit erforderlich wird, Unterauftragnehmer mit dem Umgang von vertraulichen Informationen oder geschützten Daten des Auftraggebers zu betrauen, wird der Auftragnehmer dem Auftraggeber rechtzeitig vor der beabsichtigten Beauftragung den Unterauftragnehmer benennen und die Zustimmung des Auftraggebers zur Unterbeauftragung einholen.
- (2) Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subunternehmern und holt vorab die Zustimmung des Auftraggebers ein.
- (3) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei Post- und Versanddienstleistungen.
- (4) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftraggeber, seine Pflichten aus dieser Vereinbarung dem Subunternehmer zu übertragen. Der Auftragnehmer hat sicherzustellen, dass die in dieser Vereinbarung getroffenen Regelungen auch gegenüber dem Subunternehmern gelten.



Der Auftragnehmer hat den Subunternehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über die datenschutzrelevanten Verpflichtungen des Subunternehmers und deren Umsetzung zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen bzw. direkte Kontrolle bei dem Subunternehmer. Der Auftragnehmer ist gegenüber dem Auftraggeber für die ordnungsgemäße Erfüllung der Leistungen durch die eingeschalteten Subunternehmen verantwortlich.

- (5) Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Subunternehmer die nach datenschutzrechtlichen Anforderungen erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat und einhält. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln.
- (6) Kommt ein Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Subunternehmers.

## **§ 8 Mitwirkungs-/Unterstützungspflichten**

- (1) Der Auftragnehmer unterstützt den Auftraggeber angesichts der Art der Verarbeitung mit geeigneten technischen organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DS-GVO genannten Rechte der betroffenen Person nachzukommen (Berücksichtigung von Betroffenenrechten hinsichtlich der Gewährleistung von Transparenz; Recht auf Auskunft; Berichtigungsrecht; Recht auf Löschung; Recht auf Einschränkung der Verarbeitung; Mitteilungsrecht bei Berichtigung und Löschung sowie Einschränkung der Verarbeitung; Recht auf Datenübertragbarkeit; Widerspruchsrecht; Rechte bei automatisierten Einzelfallentscheidungen).
- (2) Soweit ein Betroffener sich in Bezug auf die Wahrung seiner in Kapitel III der DS-GVO genannten Rechte direkt an den Auftragnehmer wendet, wird der Auftragnehmer dies zudem dem Auftraggeber unverzüglich mitteilen und ihn bei der Bearbeitung und Beantwortung des Begehrens im erforderlichen Umfang unterstützen und mitwirken.

## **§ 9 Unterstützung zur Pflichterfüllung des Auftraggebers**

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

## **§ 10 Verzeichnis von Verarbeitungstätigkeiten**

Der Auftragnehmer führt nach Art. 30(2) DS-GVO ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung. Er stellt auf Anforderung dem Auftraggeber die für die Übersicht nach Art. 30 DS-GVO notwendigen Angaben zur Verfügung.

## **§ 11 Nutzungsrechte, Löschung und Rückgabe personenbezogener Daten**

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



## § 12 Sonstige Pflichten des Auftragsverarbeiters

- (1) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen der Vereinbarung anfallende Datenschutzfragen. Ein Wechsel des Ansprechpartners ist dem Auftraggeber unverzüglich schriftlich mitzuteilen:

Datenschutzbeauftragter des AN: \_\_\_\_\_

- (2) Der Auftragnehmer unterrichtet den Auftraggeber umgehend bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder andere Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers.
- (3) Der Auftragnehmer informiert den Auftraggeber über Kontrollmaßnahmen der Aufsichtsbehörden unverzüglich und umfassend, soweit personenbezogene Daten des Auftraggebers betroffen sind.
- (4) Der Auftragnehmer benachrichtigt den Auftraggeber unverzüglich, wenn es zu Verletzungen dieser Vereinbarung oder anwendbarer Datenschutzgesetze gekommen ist.

## § 13 Pflichtennachweis und Unterstützung bei Überprüfungen

- (1) Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren und in geeigneter Weise nachzuweisen.
- (2) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DS-GVO niedergelegten Pflichten zur Verfügung. Er ermöglicht Überprüfungen – einschließlich Inspektionen –, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, und trägt zu ihrer Durchführung bei.
- (3) Bezüglich der in §13(2) genannten Inspektionen kann sich der Auftraggeber nach Anmeldung zu Prüfzwecken in den Betriebsstätten zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsdatenverarbeitung einschlägigen Datenschutzbestimmungen überzeugen. Liegt ein Verstoß des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen vor, so kann eine darauf bezogene Prüfung auch ohne rechtzeitige Anmeldung vorgenommen werden. Eine Störung des Betriebsablaufs beim Auftragnehmer sollte auch hierbei weitestgehend vermieden werden.
- (4) Zudem erbringt der Auftragnehmer den Nachweis, dass er hinreichend 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 in dem er beispielsweise
  - a) datenschutzspezifische Zertifizierungen oder Datenschutzsiegel und –prüfzeichen vorweisen kann,
  - b) eine schriftliche Selbstauskunft abgibt,
  - c) ein Testat eines Sachverständigen dazu vorlegt.

## § 14 Pflichten des Auftraggebers

- (1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist der Auftraggeber verantwortlich. Der Auftraggeber wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen geschaffen werden.
- (2) Der Auftraggeber wird den Auftragnehmer unverzüglich und vollständig informieren, wenn er bei der Prüfung von Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
- (3) Der Auftraggeber wird den Auftragnehmer unverzüglich und vollständig informieren, wenn er bei der Prüfung nach § 13 Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
- (4) Der Auftraggeber hat die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten.
- (5) Dem Auftraggeber obliegen die aus Art. 33, 34 DS-GVO resultierenden Informationspflichten gegenüber der Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen.
- (6) Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest.
- (7) Der Auftraggeber stellt sicher, dass die aus Art. 32 DS-GVO resultierenden Anforderungen bzgl. der Sicherheit der Verarbeitung seinerseits eingehalten werden.



## § 15 Haftung

- (1) Auftraggeber und Auftragnehmer haften für den Schaden, der durch eine nicht der DS-GVO entsprechende Verarbeitung verursacht wird gemeinsam im Außenverhältnis gegenüber der jeweiligen betroffenen Person.
- (2) Der Auftragnehmer haftet ausschließlich für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der
  - a) er den aus der DS-GVO resultierenden 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 jedoch nur, wenn er
  - a) seinen ihm speziell durch die DS-GVO auferlegten Pflichten nicht nachgekommen ist oder
  - b) unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers oder gegen diese Anweisungen gehandelt hat.

Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

## § 16 Kündigung

- (1) Der Vertrag ist nicht gesondert, sondern nur gemeinsam mit dem Hauptvertrag, bei mehreren Hauptverträgen mit dem letztverbliebenen Hauptvertrag, zu den dort festgeschriebenen Bedingungen kündbar.
- (2) Der Auftraggeber ist zu einer außerordentlichen Kündigung des Vertrages berechtigt, wenn der Auftragnehmer trotz schriftlicher Aufforderung die in der Datenschutzvereinbarung festgelegten Leistungen nicht erbringt oder seine Pflichten nach dieser Vereinbarung verletzt.
- (3) Die Vertraulichkeits- und Verschwiegenheitspflicht (§4), gilt über die Vertragsbeendigung fort.

## § 17 Informationspflichten

- (1) Sollte die auftragsgemäße Erfüllung des Auftragsgegenstandes gemäß § 1 dieser Vereinbarung beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, informiert der Auftragnehmer den Auftraggeber unverzüglich. Der Auftragnehmer wird alle in diesem Zusammenhang Beteiligten unverzüglich darüber informieren, dass die Verfügungsbefugnisse an den Daten ausschließlich beim Auftraggeber liegen.
- (2) Bei etwaigen Widersprüchen zu datenschutzrelevanten Sachverhalten zwischen dieser Vereinbarung und dem Vertrag gehen die Regelungen dieser Vereinbarung den Regelungen des Vertrages vor.



## IT- Regelungen

Für die Durchführung von Fernzugriffen bei der Prüfung und/oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen oder bei Fernzugriffen für andere Dienstleistungen gelten ergänzend folgende Regelungen:

### § 18 Organisatorische Regelungen für Wartungsarbeiten

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

### § 19 Zusätzliche technische Maßnahmen im Falle der Fernwartung

- (1) Der Verbindungsaufbau zum Wartungsunternehmen (Auftragnehmer) erfolgt ausschließlich auf Initiative des Auftraggebers (Abstimmung des Wartungszeitpunktes), so dass die Wartungsarbeiten nur mit Wissen und Willen des Auftraggebers durchgeführt werden können.
- (2) Sicherung der Authentizität und Identifikation beim Verbindungsaufbau :
  - a) Breitbandanbindung (Point-to-Multi-Point-Verbindung)
    - Der Verbindungsaufbau über einen Breitbandanschluss muss per VPN über die zentralen VPN-Gateways der IT des SKGR erfolgen. Die VPN Verbindung arbeitet mit einer verschlüsselten Datenübertragung zwischen der IT des AN und der des AG nach aktuellem Stand der Technik.
    - Es soll eine starke Authentisierung verwendet werden. Vom BSI empfohlen ist eine Kombination aus zwei Authentisierungstechniken (Zwei-Faktor-Authentisierung). Beide eingesetzten Authentisierungstechniken müssen sich auf dem Stand der Technik befinden.
  - b) Wartungsarbeiten via direkter Softwarelösungen (z.B. „Teamviewer“)
    - Der Verbindungsaufbau erfolgt in beiderseitiger Abstimmung zwischen AN und AG. Der AN besitzt eine reguläre Lizenz für die Nutzung der eingesetzten Software.
    - Der AG teilt dem AN die Einwahldaten mit und beobachtet die Fernwartungssitzung für die Dauer der Wartungsarbeiten soweit diese während der Arbeitszeit erbracht werden.

In Ausnahmefällen kann die Leistung ohne Überwachung erbracht werden.

- nach Beendigung der Wartung wird die Software ebenso beendet, sodass ein erneuter Aufruf nicht möglich ist.
- (3) Sicherung der Integrität der Daten des Auftraggebers:
    - Müssen im Ausnahmefall zur Realisierung der Wartungsaufgabe personenbezogene Daten in die Fernwartungszentrale des Auftragnehmers (und zurück) übertragen werden, so ist zur Verhinderung von Abhören, Datenverfälschung oder Datenverlust eine Verschlüsselung dieser Daten während der Übertragung erforderlich (Hardware- oder Software-Verschlüsselung). Das eingesetzte Verschlüsselungsverfahren und das Schlüsselmanagement sind als Anlage zum Wartungsvertrag zu dokumentieren.
    - Eine VPN Verbindung erfolgt verschlüsselt mittels 3DES Verschlüsselung (Data Encryption Standard) oder einem höheren Authentisierungsverfahren (z.B. AES).
    - Der Auftragnehmer hat alle in seine Fernwartungszentrale übernommenen personenbezogenen Daten nach Abschluss jedes Wartungsvorganges unverzüglich und datenschutzgerecht zu löschen.

### § 20 Protokollierung / Nachweispflicht bei der Wartung bzw. Fernwartung

Wartungsaktivitäten an datenschutzrelevanten IT-Systemen sind nachweispflichtig.

- Der Auftragnehmer hat alle Aktivitäten und den Grund der Fernwartungsarbeiten nachweisbar zu dokumentieren.
- Mindestangaben im Protokoll müssen sein:
  - Grund der Wartung



- Zeitpunkt
  - durchführende Person
  - Wartungsaktivitäten
  - durchgeführte Zugriffe auf den Echtdatenbestand (personenbezogene Daten).
- Zum Nachweis der Wartungsarbeiten sollte eine geeignete Art der Protokollierung wie zum Beispiel der Versand einer E-Mail an das zentrale Postfach [fernwartungen@klinikum-goerlitz.de](mailto:fernwartungen@klinikum-goerlitz.de) genutzt werden.
  - Eine manuelle, revisionssichere Protokollierung ist ebenfalls zulässig.
  - Die Protokolldateien werden beim Auftraggeber mindestens 1 Jahr datenschutzgerecht aufbewahrt.
- Im Falle der Fernwartung gilt zusätzlich:

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

## § 21 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.

## § 22 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 § 11 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.

## § 23 Rechtswahl, Gerichtsstand

- (1) Es gilt deutsches Recht.
- (2) Gerichtsstand ist der Sitz des Auftraggebers.

Görlitz, den \_\_\_\_\_  
(Ort, Datum)

\_\_\_\_\_  
(Ort, Datum)

\_\_\_\_\_  
Unterschrift (Auftraggeber)

\_\_\_\_\_  
Unterschrift (Auftragnehmer)

Städtisches Klinikum Görlitz gGmbH  
Geschäftsführung

### Anlage:

Anlage 1: Verpflichtung zur Geheimhaltung nach § 203 StGB

Anlage 2: Liste der zum Zeitpunkt der Auftragserteilung vereinbarten Leistungsstandorte