

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO zwischen

Verantwortlicher (Auftraggeber / AG):

Universitätsklinikum Leipzig AöR, Liebigstraße 18, 04103 Leipzig

Auftragsverarbeiter (Auftragnehmer / AN):

Anwendungsbereich

Bei der Erbringung der Leistungen gemäß

☐ dem Hauptvertrag (Name und Datum des Hauptvertrages): _____

☐ dem Einzelauftrag (Name und Datum des Einzelauftrages): _____

verarbeitet der Auftragnehmer personenbezogene Daten, die der Auftraggeber zur Erbringung der Leistungen zur Verfügung gestellt hat und bezüglich derer der Auftraggeber als Verantwortlicher im datenschutzrechtlichen Sinn fungiert („**Auftraggeber-Daten**“). Diese Anlage spezifiziert die Datenschutzpflichten und -rechte der Parteien im Zusammenhang mit der Verarbeitung der Auftraggeber-Daten zur Erbringung der Leistungen nach dem Hauptvertrag bzw. dem Einzelauftrag.

1. Vertragsdauer

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

☐ Die Laufzeit des Hauptvertrags endet voraussichtlich am _____.

2. Begriffsbestimmungen

Es gelten die Begriffsbestimmungen entsprechend Art. 4 DS-GVO, § 2 UWG, § 2 GeschGehG und § 2 TMG sowie SächsKHG und SächsDSGD. Sollten in den Artikeln bzw. Paragraphen sich widersprechende Darstellungen zu finden sein, gelten die Definitionen in der Rangfolge DS-GVO, Landesrecht, UWG und TMG.

3. Umfang der Beauftragung/Weisungsbefugnisse des Auftraggebers

- (1) Der Auftragnehmer wird die Auftraggeber-Daten ausschließlich im Auftrag und gemäß den Weisungen des Auftraggebers verarbeiten, sofern der Auftragnehmer nicht gesetzlich dazu verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Alle Weisungen werden in schriftlicher Form erteilt und sind ebenso zu bestätigen. Eine Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers.

- (2) Die Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer erfolgt ausschließlich in der Art, dem Umfang und zu dem Zweck wie in **Anhang 1** zu dieser Anlage spezifiziert; die Verarbeitung betrifft ausschließlich die darin bezeichneten Arten personenbezogener Daten und Kategorien betroffener Personen.
- (3) Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages bzw. des Einzelauftrages.
- (4) Der Auftraggeber behält sich das Recht zur Erteilung von Weisungen über Art, Umfang, Zwecke und Mittel der Verarbeitung von Auftraggeber-Daten und deren Änderung vor. Alle Weisungen sind zu dokumentieren.
- (5) Weisungsberechtigte Personen des Auftraggebers sind:

Zutreffende kenntlich machen	
UKL-Vorstand	JA
IT-Leitung	JA
Sonstige: (benennen)	_____

4. Leistungsort

- (1) Der Auftragnehmer wird die vertraglichen Leistungen in Deutschland erbringen, etwaige Unterauftragnehmer an den mit dem Auftraggeber in **Anhang 3** vereinbarten Leistungsstandorten in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR).
- (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 die Verlagerung 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. sicheren "Drittstaat" erbringen möchte bzw. die Leistungserbringung dorthin zu verlagern plant, wird der Auftragnehmer zuvor die schriftliche Zustimmung durch den Auftraggeber einholen.
- (6) 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.
- (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.

- (9) Jede Verlagerung in einen Drittstaat bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. Das angemessene Schutzniveau in _____

- ☐ ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);
- ☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b iVm 47 DS-GVO);
- ☐ wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c und d DS-GVO);
- ☐ wird hergestellt durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e iVm 40 DS-GVO);
- ☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f iVm 42 DS-GVO).
- ☐ wird hergestellt durch sonstige Maßnahmen: _____
(Art. 46 Abs 2 lit. a, Abs. 3 litt. a und b DS-GVO).

5. Anforderungen an Personal

- (1) Der Auftragnehmer hat alle Personen, die Auftraggeber-Daten verarbeiten, bezüglich der Verarbeitung von Auftraggeber-Daten zur Vertraulichkeit zu verpflichten. Außerdem sichert der AN zu, dass er seine mit der Auftragsverarbeitung beschäftigte Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bedingungen des Datenschutzes und dieser Vereinbarung vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet.
- (2) Der Auftragnehmer stellt sicher, dass ihm unterstellte natürliche Personen, die Zugang zu Auftraggeber-Daten haben, diese nur auf seine Anweisung verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

6. Sicherheit der Verarbeitung

- (1) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen, dabei ergreift er alle geeigneten technischen und organisatorischen Maßnahmen, die unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Auftraggeber-Daten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeber-Daten zu gewährleisten.
- (2) Der Auftragnehmer hat vor dem Beginn der Verarbeitung der Auftraggeber-Daten insbesondere die in **Anhang 2** zu dieser Anlage spezifizierten technischen und organisatorischen Maßnahmen zu ergreifen und während des Hauptvertrags aufrechtzuerhalten sowie sicherzustellen, dass die Verarbeitung von Auftraggeber-Daten im Einklang mit diesen Maßnahmen durchgeführt wird.
- (3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

7. Inanspruchnahme weiterer Auftragsverarbeiter

- (1) Der Auftraggeber genehmigt hiermit in allgemeiner Weise die Inanspruchnahme weiterer Auftragsverarbeiter durch den Auftragnehmer. Die gegenwärtig vom Auftragnehmer eingesetzten weiteren Auftragsverarbeiter sind in **Anhang 3** genannt.
- (2) Der Auftragnehmer wird den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung weiterer Auftragsverarbeiter informieren. Der Auftraggeber ist berechtigt, gegen jede beabsichtigte Änderung Einspruch zu erheben. Erhebt der Auftraggeber Einspruch, ist dem Auftragnehmer die beabsichtigte Änderung untersagt. Im Falle zugelassener Änderungen wird der Auftragnehmer die Liste der Unterauftragnehmer in **Anhang 3** entsprechend aktualisieren und dem Auftraggeber unverlangt zur Verfügung stellen.
- (3) Der Auftragnehmer wird jedem weiteren Auftragsverarbeiter vertraglich dieselben Datenschutz- und Vertraulichkeitspflichten auferlegen, die in dieser Anlage in Bezug auf den Auftragnehmer festgelegt sind. Die Inanspruchnahme weiterer Auftragsverarbeiter erfolgt unter der Einhaltung der Verpflichtung gemäß Art. 29 und Art. 32 Abs. 4 DS-GVO.
- (4) Der Auftragnehmer wird bei Bedarf vor jeder Beauftragung sowie regelmäßig während der Beauftragung überprüfen, dass die weiteren Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen ergriffen haben und diese so durchgeführt werden, dass die Verarbeitung der Auftraggeber-Daten gemäß dieser Anlage erfolgt.

8. Rechte der betroffenen Personen

- (1) Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren mit technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte betroffener Personen nachzukommen.
- (2) Der Auftragnehmer wird insbesondere:
 - den Auftraggeber unverzüglich informieren, falls sich eine betroffene Person mit einem Antrag auf Wahrnehmung ihrer Rechte in Bezug auf Auftraggeber-Daten unmittelbar an den Auftragnehmer wenden sollte;
 - dem Auftraggeber auf Anfrage alle bei ihm vorhandenen Informationen über die Verarbeitung von Auftraggeber-Daten geben, die der Auftraggeber zur Beantwortung des Antrags einer betroffenen Person benötigt und über die der Auftraggeber nicht selbst verfügt.

9. Sonstige Unterstützungspflichten des Auftragnehmers

- (1) Der Datenschutzbeauftragte beim Auftragnehmer ist:

[Name, Vorname, Kontaktdaten]

- (2) Der Auftragnehmer meldet dem Auftraggeber, unverzüglich nachdem ihm eine solche bekannt geworden ist, jede Verletzung des Schutzes von Auftraggeber-Daten, insbesondere Vorkommnisse, die zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu Auftraggeber-Daten führen. Die Meldung enthält nach Möglichkeit eine Beschreibung:
 - der Art der Verletzung des Schutzes der Auftraggeber-Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
 - der wahrscheinlichen Folgen der Verletzung des Schutzes der Auftraggeber-Daten;
 - der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes der Auftraggeber-Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

- (3) Für den Fall, dass der Auftraggeber verpflichtet ist, die Aufsichtsbehörden und/oder Betroffenen nach Art. 33, 34 DS-GVO zu informieren, wird der Auftragnehmer den Auftraggeber auf dessen Anfrage unterstützen, diese Pflichten einzuhalten. Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde bei dem Auftragnehmer ermittelt.
- (4) Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren bei etwa von ihm durchzuführenden Datenschutz-Folgenabschätzungen und sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DS-GVO unterstützen.
- (5) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch eine Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber in Kenntnis zu setzen. 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.

10. Kontrollrecht des Auftraggebers

- (1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
- (2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
- (3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch:
 - ☐ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
 - ☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
 - ☐ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
 - ☐ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach ISO 27001, BSI Grundschutz).
- (4) Für die Ermöglichung von Kontrollen durch den Auftraggeber, kann der Auftragnehmer einen Vergütungsanspruch geltend machen. Entsprechende Dienstleistungssätze sind durch die Parteien über den Hauptvertrag vereinbart.

11. Fernzugriff bei Prüfung/Wartung eines Systems oder anderen Dienstleistungen über Fernzugriffe

- ☐ Es ist kein Fernzugriff erforderlich (z. B. zu Wartungszwecken und Support).
- ☐ Es ist ein Fernzugriff erforderlich (z. B. zu Wartungszwecken und Support).

Für die Durchführung von Fernzugriffen bei der Prüfung und/oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen oder bei Fernzugriffen für andere Dienstleistungen gilt ergänzend die **Fernwartungsvereinbarung gem. [Dokumenten-ID 82946](#) des Auftraggebers**. Diese ist Vertragsbestandteil.

12. Datenlöschung und -zurückgabe

Der Auftragnehmer wird auf die Weisung des Auftraggebers hin mit Beendigung des Hauptvertrages alle Auftraggeber-Daten entweder vollständig und unwiderruflich löschen oder an den Auftraggeber zurückgeben, sofern nicht gesetzlich eine Verpflichtung des Auftragnehmers zur weiteren Speicherung der Auftraggeber-Daten besteht. Außerdem berichtigt, löscht oder sperrt der Auftragnehmer die vertragsgegenständlichen Daten nur auf Anweisung des Auftraggebers.

13. Nachweise und Überprüfungen

- (1) Der Auftragnehmer hat sicherzustellen und regelmäßig zu kontrollieren, dass die Verarbeitung der Auftraggeber-Daten mit dieser Anlage, einschließlich des in **Anhang 1** festgelegten Umfangs der Verarbeitung der Auftraggeber-Daten, sowie den Weisungen des Auftraggebers in Einklang steht.
- (2) Der Auftragnehmer wird die Umsetzung der Pflichten nach dieser Anlage in geeigneter Weise dokumentieren und dem Auftraggeber entsprechende Nachweise auf dessen Anfrage vorlegen. Der Auftragnehmer wird insbesondere dokumentieren:
 - alle Vertraulichkeitsverpflichtungen von Personen, die Auftraggeber-Daten verarbeiten;
 - alle sich in seinem Einwirkungsbereich ereignenden Verletzungen des Schutzes von Auftraggeber-Daten einschließlich aller damit im Zusammenhang stehenden Fakten, deren Auswirkungen und von ihm ergriffene Abhilfemaßnahmen;
 - alle Verträge über die Inanspruchnahme weiterer Auftragsverarbeiter und alle Prüfungen weiterer Auftragsverarbeiter im Sinne von Ziffer 7;
 - alle auf Weisung des Auftraggebers erfolgten Löschungen von Auftraggeber-Daten.
- (3) Der Auftraggeber ist berechtigt, den Auftragnehmer vor dem Beginn der Verarbeitung von Auftraggeber-Daten und regelmäßig während der Laufzeit des Hauptvertrags bezüglich der Einhaltung der Regelungen dieser Anlage, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen gemäß **Anhang 2**, selbst oder durch einen von ihm beauftragten Prüfer zu überprüfen; einschließlich durch Inspektionen. Der Auftragnehmer ermöglicht solche Überprüfungen und trägt durch alle zweckmäßigen und zumutbaren Maßnahmen zu solchen Überprüfungen bei, unter anderem durch:
 - die Gewährung der notwendigen Zugangs- und Zugriffsrechte und
 - der Bereitstellung aller notwendigen Informationen.

14. Zurückbehaltungsrecht

- (1) Die Einrede des Zurückbehaltungsrechts, gleich aus welchem Rechtsgrund, an den vertragsgegenständlichen Daten sowie an evtl. vorhandenen Datenträgern wird ausgeschlossen, es sei denn, es handelt sich dabei um unbestrittene oder rechtskräftig festgestellte Forderungen.
- (2) Das UKL, soweit vom Auftragsgegenstand umfasst auch die jeweils betroffenen assoziierten oder versorgten Organisationen, haben jeweils selbstständig gegenüber dem Auftragnehmer das Recht, jederzeit die Herausgabe der im Rahmen der Nutzung der vertragsgegenständlichen Leistungen verarbeiteten und/oder neu entstehenden oder entstandenen und/oder auf den Systemen des Auftragnehmers gespeicherten und verarbeiteten Daten, Datenergebnisse oder Datenbestände des UKL oder der assoziierten oder versorgten Organisationen zu verlangen. Die Herausgabe erfolgt in einem maschinenlesbaren, dem allgemeinen Standard entsprechenden elektronischen Format. Alle Rechte, insbesondere das Nutzungsrecht an diesen Daten, Datenergebnissen oder Datenbeständen, stehen allein dem UKL oder bzw. soweit vom Auftragsgegenstand umfasst, den jeweils betroffenen assoziierten oder versorgten Organisationen als alleinberechtigtem Rechteinhaber und Nutzer zu. Als Daten sind in Anlehnung an DIN 44300 (strukturierte und unstrukturierte) Zeichen und kontinuierliche Funktionen gemeint, die aufgrund von bekannten oder unterstellten Abmachungen dem Zwecke der Verarbeitung von Informationen des UKL oder, soweit vom Auftragsgegenstand umfasst, den jeweils betroffenen assoziierten oder versorgten Organisationen dienen. Diese Daten stehen ausschließlich dem UKL oder/und, soweit vom Auftragsgegenstand umfasst, den betroffenen jeweils assoziierten oder versorgten Organisationen zu. Der Auftragnehmer hat diesbezüglich kein Recht auf Zurückbehaltung (§§ 273, 320 BGB) oder Zugriffssperrung. Etwaige urheberrechtliche Nutzungs- oder Lizenzrechte (z. B. an der Software) bleiben davon unberührt.

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

16. Schriftformklausel

Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen

Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Regelungen handelt. Das Schriftformerfordernis gilt auch für den Verzicht auf dieses Formerfordernis.

17. Salvatorische Klausel

- (1) Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen der Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt.
- (2) An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.
- (3) Erweist sich der Vertrag als lückenhaft, gelten die Bestimmungen als vereinbart, die dem Sinn und Zweck des Vertrages entsprechen und im Falle des Bedachtwerdens vereinbart worden wären.
- (4) Existieren mehrere wirksame und durchführbare Bestimmungen, welche die unter Ziff. 8 genannte unwirksame Regelung ersetzen können, so muss die Bestimmung gewählt werden, welche den Schutz der Patientendaten im Sinne dieses Vertrages am besten gewährleistet.

18. Gerichtsstand

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

Auftraggeber:

Ort, Datum	Prof. Dr. Christoph Josten Medizinischer Vorstand
------------	--

Ort, Datum	Dr. Robert Jacob Kaufmännischer Vorstand
------------	---

Ort, Datum, Firmenstempel AG	fachlicher Vertreter der einsetzenden Stelle
------------------------------	--

Auftragnehmer:

Ort, Datum, Firmenstempel AN	rechtsverbindliche Unterschrift
------------------------------	---------------------------------

Ort, Datum, Firmenstempel AN	rechtsverbindliche Unterschrift
------------------------------	---------------------------------

Anhang 1

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende Datenarten / -kategorien

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

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

- ☐ Patienten
- ☐ Abonnenten
- ☐ Beschäftigte
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☐ Ansprechpartner
- ☐

Anhang 2

Nachweis der allgemeinen technischen und organisatorischen Maßnahmen (Art. 32 Abs. 1 DS-GVO)

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen sind geeignete **technische und organisatorische Maßnahmen** zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. (Art. 32 Abs. 1 DS-GVO) Diese Maßnahmen schließen u.a. folgende Anforderungen ein, die hier genauer zu erläutern sind:

a) Pseudonymisierung personenbezogener Daten (Art. 32 Abs. 1 lit. a DS-GVO)

b) Verschlüsselung personenbezogener Daten (Art. 32 Abs. 1 lit. a DS-GVO)

c) Gewährleistung der Vertraulichkeit der Systeme und Dienste (Art. 32 Abs. 1 lit. b DS-GVO)

d) Gewährleistung der Integrität der Systeme (Art. 32 Abs. 1 lit. b DS-GVO)

e) Gewährleistung der Verfügbarkeit der Systeme und Dienste (Art. 32 Abs. 1 lit. b DS-GVO)

f) Gewährleistung der Belastbarkeit der Systeme und Dienste (Art. 32 Abs. 1 lit. b DS-GVO)

- g) Wiederherstellung der Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen nach einem physischen oder technischen Zwischenfall (Art. 32 Abs. 1 lit. c DS-GVO)

- h) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 Abs. 1 lit. d DS-GVO)

Anhang 3

Unterauftragsverhältnisse beim Auftragnehmer zum Zeitpunkt der Auftragsvergabe

Name und Anschrift des Unterauftragnehmers	Beschreibung der Teilleistungen	Ort der Leistungserbringung

Anhang 4

Vertraulichkeitserklärung

zur Beachtung des Datenschutzes, insbesondere zur Wahrung der Vertraulichkeit, und zur Wahrung des Geschäfts- und Betriebsgeheimnisses

☐ Anlage zum Vertrag: _____

☐ Einmaliger Auftrag am: _____

Firma / Organisation _____

Adresse _____

Name, Vorname, Geburtsdatum des Vertretungsberechtigten bzw. des Einzelverpflichteten _____

Hiermit bestätigt der Auftragnehmer, dass alle Mitarbeiter und sonstigen von ihm beauftragten Personen zur Einhaltung der nachfolgenden Regelungen verpflichtet sind.

Nach Art. 5 DS-GVO sowie gem. § 203 StGB i.V.m. § 1 VerpflG in der jeweils geltenden Fassung werden Sie wie folgt auf die Wahrung der Vertraulichkeit sowie die sonstigen bei Ihrer Tätigkeit zu beachtenden Vorschriften über den Datenschutz (wie beispielsweise das SächsKHG und das Sächsische Datenschutzdurchführungsgesetz (SächsDSdG) und das Geschäfts-, Betriebsgeheimnis sowie den Umgang mit Software verpflichtet:

Aufgrund Ihrer arbeitsvertraglichen bzw. sonstigen vertraglichen Bindung zur zeitweiligen Aufgabenerfüllung (bspw. als Dienstleister, oder Gastarzt, Hospitant, Praktikant, Schüler u. ä.) am/für das Universitätsklinikum Leipzig AöR (UKL), der Medizinischen Fakultät der Universität Leipzig (MF) bzw. der Medizinischen Berufsfachschule (MBFS) sind Sie zur Wahrung

1. des Geschäfts- und Betriebsgeheimnisses
2. der Vertraulichkeit beim Umgang mit personenbezogenen Daten (Datenschutz)
3. dem ordnungsgemäßen Umgang mit Software

verpflichtet.

1. Geschäfts- oder Betriebsgeheimnis

Sie sind zur Geheimhaltung aller Informationen verpflichtet, die Ihnen im Zusammenhang mit der übernommenen Aufgabe bekannt werden und die nicht offenkundig sind. Dies gilt sowohl für Informationen über das UKL, die MF und die MBFS sowie auch über deren Geschäftspartner. Diese Geheimhaltungsvorschrift besteht auch nach Beendigung Ihrer Tätigkeit fort.

2. Vertraulichkeit beim Umgang mit personenbezogenen Daten (Datenschutz)

Es ist Ihnen untersagt, personenbezogene Daten ohne entsprechende Befugnis, die sich nach Art. 6 und Art. 9 DS-GVO, § 28 und § 29 SächsKHG sowie § 3 und § 4 SächsDSdG nur aus einer Rechtsvorschrift (u. a. Gesetz, Rechtsverordnung, Satzung) oder der Einwilligung des Betroffenen ergeben kann, zu verarbeiten.

"**Verarbeitung**" bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Dies ist unabhängig davon, ob diese Daten in Erfüllung Ihrer Dienstaufgaben oder rein zufällig zu Ihrer Kenntnis gelangt sind.

"**Personenbezogene Daten**" sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; in Dateiform oder als Akte (z.B. Aufzeichnungen auf maschinell lesbaren Datenträgern, Angaben auf Formularen und Karteikarten, allg. Arbeitsunterlagen, Röntgenbilder, Ultraschall-Aufnahmen, CT/MRT-Schnittbilder, Mikrofilme, Bild- und Tonträger u. a.) Unter personenbezogenen Daten sind nicht nur Daten von Mitarbeitern zu verstehen, sondern vor allem auch Patientendaten, einschließlich von deren Angehörigen, anderer Bezugspersonen oder sonstiger Dritter. Gesundheitsdaten unterliegen als Kategorie besonderer personenbezogener Daten einem ausgesprochen hohen Schutz.

Eine Verletzung der standesrechtlichen "**Ärztlichen Schweigepflicht**" (Muster-Berufsordnung für Ärzte, Apotheker) ist nach Strafgesetzbuch auch für die "**berufsmäßig tätigen Gehilfen**" unter Strafe gestellt, d.h. auch für Gesundheits- und Krankenpfleger/-innen, Hebammen/Entbindungspfleger, Med.-technische Assistenten/Assistentinnen, Diätassistenten/-assistentinnen, Arzthelfer/-innen, Praktikanten/Praktikantinnen, Verwaltungspersonal usw.

3. Ordnungsgemäßer Umgang mit Software

Der nicht ordnungsgemäße Erwerb von Computer-Software stellt einen Verstoß gegen das Urheberrecht dar und kann sowohl gegenüber dem UKL / der MF als auch gegenüber dem Mitarbeiter straf- und zivilrechtlich geahndet werden. Weiterhin besteht eine Gefahr hinsichtlich des Einsatzes von schadenstiftender Software (illegale Software-Kopien, Viren u. a.).

Deshalb ist festgelegt:

- a) Software muss grundsätzlich ordnungsgemäß erworben und installiert werden (auch Demonstrations- und Test-Software). Der Erwerb erfolgt über den Bereich 1 – Informationssysteme des UKL, ebenso die Installation bzw. diese in Absprache. Analog für die Software-Einstallation und die Verschrottung von Computern, inkl. der zuverlässigen Löschung von Daten.

Revisionsnummer: 001/07.2023

- b) Die Benutzung von Software, die nicht der direkten Aufgabenerfüllung dient, ist grundsätzlich untersagt.
- c) Installierte Viren-Scanner dürfen nicht abgeschaltet bzw. deinstalliert werden.

Rechtsfolgen

1. Verstöße gegen das Geschäfts- oder Betriebsgeheimnis können auf der Grundlage des Gesetzes zum Schutz von Geschäftsgeheimnissen und anderer Rechtsgrundlagen zivilrechtlich sowie strafrechtlich geahndet werden.
2. Aus der Verletzung der Vertraulichkeit ergeben sich arbeits-, straf- oder ordnungswidrigkeitsrechtliche Konsequenzen (gem. § 22 SächsDSGDG Geldbuße bis zu 25 T€, als Straftat bis zu 2 Jahren Freiheitsstrafe).
3. Die Verbreitung / Benutzung illegal kopierter Software kann nach dem Urheberrechtsgesetz geahndet werden.
4. Die Verbreitung / Benutzung von schadensstiftender Software kann strafrechtlich verfolgt werden.
5. Verstöße lösen auch zivilrechtliche Schadenersatzansprüche aus.

Ein Merkblatt mit Erläuterungen und den relevanten Rechtsvorschriften sowie eine Kopie der Verpflichtungserklärung werden ausgehändigt. Weitere Informationen mit datenschutzrelevanten Regelungen ergeben sich aus den Dienstvereinbarungen und Dienstanweisungen sowie weiteren innerbetrieblichen Regelungen.

Verpflichtung nach § 203 StGB

Des Weiteren erkläre ich, die Anforderungen des § 203 StGB und die strafrechtlichen Folgen einer Verletzung zu kennen.

Soweit ich hierzu nicht gesetzlich bereits verpflichtet bin erkläre ich Folgendes:

1. Ich verpflichte mich zur gewissenhaften Einhaltung und Erfüllung der gesetzlichen Anforderungen. Insbesondere ist mir bekannt, dass meine Verschwiegenheit auch nach Beendigung des Vertragsverhältnisses, gleich welcher Art dieses ist, uneingeschränkt und zeitlich unbefristet fortbesteht.
2. Ich verpflichte mich darüber hinaus alle meine Mitarbeiter (Bestandsmitarbeiter und zukünftige neue Mitarbeiter), die im Rahmen des gegenständlichen Auftrages bzw. Vertragsverhältnisses mit den der besonderen Verschwiegenheitspflicht unterliegenden Daten in Berührung kommen, ebenso wirksam nach § 203 StGB zu verpflichten.
3. Ich sichere zu, soweit in Erfüllung des Auftrages durch mich / unser Unternehmen Dritte (Subunternehmer) oder Geschäftspartner (im Rahmen eines mehrstufigen Vertragsverhältnisses) zum Einsatz kommen, für eine gleiche Verpflichtung Sorge zu tragen. Über die strafrechtlichen Konsequenzen einer fehlerhaften oder mangelnden Verpflichtung bin ich informiert.

In allen Zweifelsfragen werde ich entsprechenden Rechtsrat vor einer Offenbarung von Geheimnissen, welche § 203 StGB unterliegen einholen.

Ort, Datum

Unterschrift, Firmenstempel