**Vertrag zur Auftragsverarbeitung**
**gemäß Art. 28 Datenschutz-Grundverordnung (DS-GVO)**
**zwischen**

_____

als Auftragsverarbeiter im Sinne der DS-GVO,
nachfolgend "**Auftragnehmer**" genannt

**und dem Universitätsklinikum Leipzig AöR**
als Verantwortlicher im Sinne der DS-GVO,
nachfolgend "**Auftraggeber**" genannt

Dieser Auftragsverarbeitungs-Vertrag (AV-Vertrag) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der im Vertrag

……..……..……

Name u. Datum des Hauptvertrages

(im Folgenden Hauptvertrag genannt) 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 den im Hauptvertrag bereits getroffenen Festlegungen folgende Maßnahmen zwischen dem Auftragnehmer und dem Auftraggeber vereinbart:

## § 1 Definitionen

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

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

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

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

(4) Weisung

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

## § 2 Gegenstand des Auftrags

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)
- ☐ Kundenhistorie
- ☐ 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
- ☐ Kunden
- ☐ Interessenten
- ☐ Abonnenten
- ☐ Beschäftigte
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☐ Ansprechpartner
- ☐ ……

## § 3 Verantwortlichkeit

(1) 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).

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

(3) 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. Dazu müssen alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, auf das Datengeheimnis verpflichtet und über ihre Datenschutzpflichten belehrt werden. Dabei ist jede Partei für die Verpflichtung des eigenen Personals zuständig. Ferner müssen die eingesetzten Personen darauf hingewiesen werden, dass das Datengeheimnis auch nach Beendigung der Tätigkeit fortbesteht.

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

## § 4 Dauer des Auftrags

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

## § 5 Weisungsbefugnis des Auftraggebers

(1) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Auftraggebers. Ausgenommen hiervon sind Sachverhalte, in denen dem Auftragnehmer eine Verarbeitung aus zwingenden rechtlichen Gründen auferlegt wird. Der Auftragnehmer unterrichtet soweit ihm möglich in derartigen Situationen den Auftraggeber vor Beginn der Verarbeitung über die entsprechenden rechtlichen Anforderungen. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann.

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

(3) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind von der Weisungsbefugnis des Auftraggebers gedeckt und entsprechend zu dokumentieren. Bei einer wesentlichen Änderung des Auftrags steht dem Auftragnehmer ein Widerspruchsrecht zu. Besteht der Auftraggeber trotz des Widerspruchs des Auftragnehmers auf der Änderung, so ist diese Änderung als wichtiger Grund anzusehen und erlaubt eine fristlose Kündigung des von der Weisung betroffenen AV-Vertrages sowie der von der AV-Vereinbarung betroffenen Bestandteile des entsprechenden Hauptvertrages.

(4) Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragnehmer notiert sich Datum, Uhrzeit und Person, welche die mündliche Weisung erteilte sowie den Grund, warum keine schriftliche Beauftragung erfolgen konnte.

(5) Ansprechpartner (weisungsberechtigte Personen) des Auftraggebers sind

| | Nicht Zutreffende bitte ausschließen |
|---|---|
| UKL-Geschäftsführung | |
| IT-Leitung | |
| Ärzte | Nein |
| Pflegekräfte, Arzthelferinnen | Nein |
| weitere vom Auftraggeber mit der Betreuung seiner Daten beauftragte Personen, z.B. regionale Systembetreuer | Nein |

## § 6 Leistungsort

(1) Der Auftragnehmer wird die vertraglichen Leistungen in Deutschland erbringen, etwaige Unterauftragnehmer an den mit dem Auftraggeber in Anhang 1 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.

**§ 7 Pflichten des Auftragnehmers**

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

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust treffen, die den Anforderungen der entsprechenden datenschutzrechtlichen Bestimmungen entsprechen; diese Maßnahmen muss der Auftragnehmer auf Anfrage dem Auftraggeber und ggfs. Aufsichtsbehörden gegenüber nachweisen. 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 Anlage 2 zu diesem Vertrag.

(3) Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein aussagekräftiges und aktuelles Datenschutz- und Sicherheitskonzept für diese Auftragsverarbeitung zur Verfügung.

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

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

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

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

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

(9) Als Datenschutzbeauftragter ist beim Auftragnehmer derzeit

_____

[*Name, Kontaktdaten*]

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

(10) 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 Artt. 33, 34 DS-GVO.

(11) 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.

(12) 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.

(13) 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.

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

(15) 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.

(16) 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.

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

(18) Der Auftragnehmer speichert keine identifizierenden Patientendaten auf Systemen, die außerhalb der Verfügungsgewalt des Auftraggebers liegen.

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

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

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

Für die Durchführung von Fernzugriffen bei der Prüfung und/oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen oder bei Fernzugriffen für andere Dienstleistungen gelten ergänzend folgende Rechte/Pflichten des Auftraggebers/Auftragnehmers:

(1) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten an Arbeitsplatzsystemen werden erst nach Freigabe durch den zuständigen, benannten Mitarbeiter des Auftraggebers durchgeführt.

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

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

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

(5) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten werden dokumentiert und protokolliert. Der Auftraggeber ist berechtigt, Prüfungs- und Wartungsarbeiten vor, bei und nach Durchführung zu kontrollieren. Bei Fernzugriffen ist der Auftraggeber - soweit technisch möglich - berechtigt, diese von einem Kontrollbildschirm aus zu verfolgen und jederzeit abzubrechen.

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

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

(8) Tätigkeiten zur Fehleranalyse, bei denen ein Datenabzug der 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.

(9) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten sowie sämtliche in diesem Zusammenhang erforderlichen Tätigkeiten, insbesondere Tätigkeiten wie Löschen, Datentransfer

oder eine Fehleranalyse, werden ausschließlich mit ausdrücklicher und dokumentierter Zustimmung des Auftraggebers und unter Berücksichtigung von technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten durchgeführt. In diesem Zusammenhang wird der Auftragnehmer die technischen und organisatorischen Maßnahmen wie im Anhang beschrieben ergreifen.

## § 9 Pflichten des Auftraggebers

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

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

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

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

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

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

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

(8) 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.

## § 10 Kontrollrechte des Auftraggebers

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

Hierfür kann er beispielsweise

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

(2) Liegt ein Verstoß des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen vor, so kann eine darauf bezogene Prüfung auch ohne rechtzeitige Anmeldung vorgenommen werden. Eine Störung des Betriebsablaufs beim Auftragnehmer sollte auch hierbei weitestgehend vermieden werden.

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

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

**§ 11 Berichtigung, Beschränkung von Verarbeitung, Löschung und Rückgabe von Datenträgern**

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

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

(3) In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe.

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

a. sämtliche im Rahmen des Auftrags in seinen Besitz gelangte Unterlagen oder Datenträger,

b. erstellte Verarbeitungsergebnisse,

c. 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.

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

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

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

(8) 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.

(9) 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.

(10) 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.

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

**§ 12 Unterauftragnehmer**

(1) 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.

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

(3) Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragnehmer 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.

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

(5) Zum Zeitpunkt des Abschlusses dieser Vereinbarung sind die in der ***Anlage*** 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.

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

(7) Ist der Auftragnehmer im Sinne dieser Vereinbarung befugt, die Dienste eines Unterauftragnehmers in Anspruch zu nehmen, um bestimmte Verarbeitungstätigkeiten im Namen 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.

(8) 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.

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

Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten 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.

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

## § 13 Zurückbehaltungsrecht

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

## § 14 Haftung

(1) Auftraggeber und Auftragnehmer haften für den Schaden, der durch eine nicht der 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.

## § 15 Schriftformklausel

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

## § 16 Salvatorische Klausel

(1) Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen der Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt.

(2) An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

(3) Erweist sich der Vertrag als lückenhaft, gelten die Bestimmungen als vereinbart, die dem Sinn und Zweck des Vertrages entsprechen und im Falle des Bedachtwerdens vereinbart worden wären.

(4) Existieren mehrere wirksame und durchführbare Bestimmungen, welche die unter § 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.

**§ 17 Rechtswahl, Gerichtsstand**

(1) Es gilt deutsches Recht.

(2) Gerichtsstand ist der Sitz des Auftraggebers.

Auftraggeber:

| | |
|---|---|
| _____ | _____ |
| Ort, Datum | Prof. Dr. med. Wolfgang E. Fleig<br>Medizinischer Vorstand und Sprecher des Vorstandes |
| _____ | _____ |
| Ort, Datum | Marco Schüller<br>Kaufmännischer Vorstand (komm.) |
| _____ | _____ |
| Ort, Datum, Firmenstempel AG | fachlicher Vertreter der einsetzenden Stelle |

Auftragnehmer:

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

Anlage(n)

| | |
|---|---|
| Anlage 1: | Unterauftragsverhältnisse beim Auftragnehmer zum Zeitpunkt der Auftragsvergabe |
| Anlage 2: | Nachweis der allgemeinen technischen und organisatorischen Maßnahmen (TOM) |
| Anlage 3: | Verpflichtung zur Beachtung des Datenschutzes, insbesondere zur Wahrung der Vertraulichkeit, und zur Wahrung des Geschäfts- und Betriebsgeheimnisses; Verpflichtung zur Geheimhaltung nach § 203 StGB |
| Anlage 4: | Übersicht der zum Zeitpunkt der Auftragserteilung vereinbarten Leistungsstandorte des Auftragnehmers |

Anlage 1 zum AV-Vertrag:

**Unterauftragsverhältnisse beim Auftragnehmer zum Zeitpunkt der Auftragsvergabe**

| Name und Anschrift des Unterauftragnehmers | Beschreibung der Teilleistungen | Ort der Leistungserbringung |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Anlage 2 zum AV-Vertrag:

**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)**

| |
|---|
| |

Erläuterungen

| | Detaillierte Beschreibung der technischen und organisatorischen Maßnahmen |
|---|---|
| | Pseudonymisierung, u.a.:<br>– Trennung von Kundenstammdaten und Kundenumsatzdaten<br>– Trennung von Patienten-Kontaktdaten und Behandlungsdaten/Befunden etc.<br>– Verwendung von Personal-, Kunden-, Patienten-Kennziffern statt Namen |
| | Verschlüsselung, z. B. in stationären u. mobilen Speicher-/Verarbeitungsmedien, bei elektron. Transport):<br>– symmetrische Verschlüsselung<br>– asymmetrische Verschlüsselung |
| | Vertraulichkeit der Systeme und Dienste, die einen unautorisierten Zugang oder Zugriff auf personenbezogene Daten verhindern sollen, beim Verantwortlichen selbst oder auf dem Transportweg zu Auftragsverarbeitern oder Dritten, u.a.:<br>– Zutrittskontrolle<br>(Maßnahmen, um unbefugten Personen den (räumlichen) Zutritt zum IT-System und zu Datenträgern (auch z.B. Aktenordnern) zu verwehren)<br>– Zugangskontrolle<br>(Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können)<br>– Zugriffskontrolle<br>(Maßnahmen, die sicherstellen, dass nur die zur Benutzung eines Datenverarbeitungssystems Berechtigten und ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden (personenbezogenen) Daten zugreifen können)<br>– Weitergabekontrolle<br>(Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist)<br>– Trennungskontrolle<br>(Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können) |
| | Integrität der Systeme und Dienste, die gewährleisten, dass personenbezogene Daten nicht (unbemerkt) geändert werden können, u.a.:<br>– Eingabekontrolle<br>– insbes. organisatorische und technische Absicherung von Berechtigungen, Protokollierungsmaßnahmen, Protokoll-Auswertungen/Revision etc. |
| | Verfügbarkeit der Systeme u. Dienste, die sicherstellen, dass personenbezogene Daten dauernd und uneingeschränkt verfügbar und insbes. vorhanden sind, wenn sie gebraucht werden, u.a.:<br>– Verfügbarkeitskontrolle<br>– Auftragskontrolle |
| | Belastbarkeit der Systeme u. Dienste, die sicherstellen, dass die Systeme und Dienste so ausgelegt sind, dass auch punktuell hohe Belastungen oder hohe Dauerbelastungen von Verarbeitungen leistbar bleiben:<br>– insbes. hinsichtl. Speicher-, Zugriffs- und Leitungskapazitäten |
| | Maßnahmen, um nach einem physischen oder technischen Zwischenfall die Verfügbarkeit personenbezogenen Daten und den Zugang zu ihnen rasch wiederherzustellen, u.a.:<br>– Backup-Konzept<br>– Redundante Datenspeicherung<br>– Cloud-Services<br>– Backup-IT-Infrastruktur<br>– Backup-Rechenzentrum |
| | Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen, u.a.:<br>– Entwicklung eines Sicherheitskonzepts<br>– Prüfungen des DSB, der IT-Revision<br>– Externe Prüfungen, Audits, Zertifizierungen |

UNIVERSITÄT LEIPZIG
Medizinische Fakultät

Universitätsklinikum Leipzig
Medizin ist unsere Berufung.

Anlage 3 zum AV-Vertrag:

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

## Angaben zur Person

Anrede _____

Name, Vorname _____

Geburtsdatum _____

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 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, § 33 Abs. 2 und § 34 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-Deinstallation und die Verschrottung von Computern, inkl. der zuverlässigen Löschung von Daten.
b) Die Benutzung von Spiele-Software 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 gegen den unlauteren Wettbewerb und anderer Rechtsgrundlagen zivilrechtlich sowie strafrechtlich geahndet werden.
2. Aus der Verletzung der Vertraulichkeit ergeben sich arbeits-, straf- oder ordnungswidrigkeitsrechtliche Konsequenzen (gem. § 22 SächsDSDG 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 einzuholen.

Ort, Datum

Unterschrift

UNIVERSITÄT LEIPZIG
Medizinische Fakultät

Universitätsklinikum Leipzig
Medizin ist unsere Berufung.

# Merkblatt zur Verpflichtung zur Vertraulichkeit

## Dienstspezifische Datenschutzhinweise

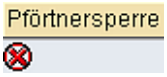
1a. Inwieweit und welche Art von **Auskünften bei Nachfragen von außerhalb am Telefon** gegeben werden dürfen, bestimmt der jeweils behandelnde Arzt. Die Auskünfte sind unter Beachtung des Patientenwillens und unter Berücksichtigung der Einzelfallsituation zu erteilen **und immer restriktiv zu handhaben** (nach der Art des Anrufes, nur Terminauskunft, ob Notfall, ggf. nur allgemeine Auskunft, Verweis an den behandelnden Arzt oder an einen vom Patienten benannten Angehörigen, separate Einbestellung, usw.).

1b. Über die Identität des Anrufenden ist sich zu vergewissern, bspw. durch Erfragen von Geburts-datum, Anschrift oder letztem Aufenthalt im UKL und/oder Vergleich der auf dem Display gezeigten Telefonnummer mit der „Nächste Angehörige“ - Telefonnummer des Patienten im SAP.

1c. Anfragen von juristischen Personen (bspw. Vereine, Unternehmen, Arbeitgeber oder Behörden) sollen immer schriftlich (auch als Fax) an das UKL gerichtet werden. Sofern telefonische Anfragen erfolgen, sind diese darauf hinzuweisen.

1d. **Im Zweifelsfall ist keine Auskunft zu erteilen.**

1e. Sofern im SAP auf der Stations- oder Ambulanzübersicht für einen Patienten die „Pförtnersperre“ eingetragen ist, bedeutet dies ein striktes Auskunftsverbot gegenüber allen (auch telefonisch)nachfragenden Privatpersonen oder unbefugten juristischen Personen, sogar darüber, ob sich der Patient überhaupt im Klinikum aufhält.




2. Die **ärztliche Schweigepflicht** gilt grundsätzlich auch gegenüber nahen Angehörigen des Patienten.
3. **Sensible Patientengespräche** dürfen von anderen Patienten nicht mitgehört werden können, ggf. ist dafür z. B. ein separater Raum zu nutzen.
4. Patientenunterlagen dürfen niemals am Stationsstützpunkt unbeaufsichtigt liegen gelassen werden und dürfen, ebenso wie Bildschirme, von anderen Patienten und Besuchern nicht einsehbar sein.
5. Patienten und ggf. begleitende Dritte dürfen in Untersuchungs- oder Behandlungsräumen nicht unbeaufsichtigt sein.
6. Sofern keine Kontrolle gewährleistet ist, sind Türen bei Verlassen des Stützpunktes oder des Dienstzimmers zu verschließen.
7. **Rezepte und Arzt-Stempel** sind für Patienten nicht sichtbar zu lagern und nach Dienstende in einem Schrank sicher vor dem Zugriff Dritter einzuschließen (dies gilt immer -auch während der Dienstzeit- für **BTM-Rezepte und das BTM-Bestellbuch**).
8. Vom Postdienst entgegengenommene Patientenpost und Pakete sind zu quittieren und dem Patienten unmittelbar zu übergeben.
9. Zu entsorgende patienten- und personalbezogene Dokumente gehören IMMER in die abgeschlossene Daten-Mülltonne, welche in der Regel im AWT-Raum steht, **keinesfalls in die normalen Papierkörbe!** Zwischenzeitlich können solche Unterlagen in einer gekennzeichneten, für Patienten nicht einsehbaren und nicht zugänglichen Ablage gesammelt werden.
10. Spam-verdächtige E-Mails sind dem Bereich 1 – Informationsmanagement per E-Mail an *spamverdacht@medizin.uni-leipzig.de* zu melden – und zwar **nur als Anlage in dieser E-Mail-Meldung. Anhänge solcher verdächtigen E-Mails dürfen keinesfalls geöffnet werden!**
11. Logins für Windows und Anwendungssoftware (z. B. SAP) dürfen ausschließlich persönlich genutzt werden und sind geheim zu halten. Die Weitergabe personengebundener Passwörter ist untersagt (darunter fällt auch z. B. das Anbringen eines „Merkzettels“ am Bildschirm). Sobald kein unmittelbarer Programmzugriff mehr erforderlich ist, hat eine Systemabmeldung zu erfolgen („ausloggen“).
12. Für Windows und SAP erfolgt nach 6 Monaten automatisch ein erzwungener Passwortwechsel.[1]
13. Das ***Laufwerk W:*** besitzt für jede Klinik einen eigenen Ordner und dient zum Speichern klinikbezogener Daten, der Zugriff ist auf die jeweiligen Klinikmitarbeiter beschränkt. Als besondere Vorsichtsmaßnahme können (versehentlich) gelöschte oder geänderte Dateien innerhalb von 4 Wochen auf Antrag des jeweiligen Ordnerverantwortlichen durch den Bereich 1 wiederhergestellt werden
14. Das ***Laufwerk V:*** ist das persönlich-dienstliche Laufwerk eines jeden Mitarbeiters, auf welches **ausschließlich** dieser Zugriff hat. **LW V:** ist von jedem PC im Medizinnetz aus zugreifbar und wird zentral durch den Bereich 1 gesichert. Ggf. lokal auf dem PC gespeicherte Daten sollen deshalb regelmäßig nach **LW V:** gesichert oder gleich dort gespeichert werden.
15. Es dürfen nur solche Fälle/Patientendaten aufgerufen und bearbeitet werden, welche sich aus der aktuellen Arbeitsaufgabe ergeben, in der Regel also nur die Fälle aktueller oder noch zu bearbeitender Patienten (etwa zur Befund- oder Terminsuche bzw. Dokumentation). **Insbesondere ist es Ihnen gem. DS-GVO, SächsKHG, SächDSDG, § 85 SGB X, § 203 StGB (Verletzung von Privatgeheimnissen) sowie im Rahmen Ihres Arbeitsvertrags untersagt, aus nicht dienstlichen Gründen Fälle/Daten Dritter (z.B. von Arbeitskollegen, Verwandten oder Bekannten) aufzurufen, einzusehen oder weiterzugeben.**
16. Bildschirme, welche durch Patienten/Besucher eingesehen werden könnten, sind durch einen Bildschirmschoner zu schützen (mit automatischer Aktivierung nach 5 Minuten).
17. Häufig genutzte Faxnummern sind einzuspeichern, um die Gefahr eines Verwählens zu vermeiden. Bei wichtigen Faxen soll eine telefonische Ankündigung beim Empfänger bzw. Rückfrage erfolgen, ob das Fax angekommen ist. Sendeberichte können bei Erfordernis dem Dokument beigeheftet werden. Das Fax - Journal ist als genereller Nachweis am Fax einzustellen und 1 Jahr aufzuheben.
18. In Soziale Medien, wie Facebook oder Twitter, gehören keine UKL-internen Informationen oder diesbezügliche Problemdiskussionen.
19. Bild-, Video- oder Tonaufnahmen von Patienten bzw. deren Verletzungen mit privaten mobilen Endgeräten, wie etwa Smartphones, und deren Weitergabe sind strengstens untersagt!
20. Gesonderte Regelungen des UKL, wie Verfahrens- und Dienstanweisungen, sind zu beachten.
21. Stellen Sie selbst Datenschutzverletzungen fest, teilen Sie dies Ihrem Vorgesetzten und auch direkt dem Datenschutzbeauftragten mit. Solche Probleme könnten u. U. zu schwerwiegenden Folgen für das UKL führen. Das UKL hat eine **gesetzlich vorgeschriebene Benachrichtigungspflicht gegenüber Patienten und Meldepflicht gegenüber Aufsichtsbehörden**, sollten Informationen in falsche Hände gelangt sein.

Haben Sie spezielle Fragen, so können Sie den Datenschutzbeauftragten auch direkt kontaktieren:

**Universitätsklinikum Leipzig AöR**
**Liebigstraße 18, Haus B**
**04103 Leipzig**
**z.H. Datenschutzbeauftragte**
**E-Mail: dsb@uniklinik-leipzig.de**

[1] Die letzten fünf genutzten Passwörter dürfen sich nicht wiederholen, das jeweilige Anwendungssystem gibt Hinweise zu den Mindestanforderungen an das neue Passwort, eine Anleitung finden Sie außerdem im Intranet auf der Seite von Bereich 1. Hinweise zum Generieren und Merken von Passwörtern finden Sie unter „Mitarbeiterbezogener Datenschutz“ auf der „Datenschutz“-Intranet-Seite.

**Anlage zur Datenschutzverpflichtung:**
**Auszug aus einschlägigen Rechtsgrundlagen, Straf- und Bußgeldvorschriften** Stand: Mai 2018

# Europäische Datenschutz-Grundverordnung DS-GVO

**Art. 5 Rechenschaftspflichten**

(1)Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);
c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);
f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

(2)Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können ("Rechenschaftspflicht“).

**Art. 32 Sicherheit der Verarbeitung**

(4)Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

# Sächsisches Krankenhausgesetz SächsKHG

**§ 33 Datenschutz**

(1)Soweit in diesem Gesetz nichts anderes bestimmt ist, sind die jeweils geltenden Vorschriften über den Schutz personenbezogener Daten anzuwenden. Patientendaten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer Patienten aus dem Bereich der Krankenhäuser. Patientendaten sind auch die personenbezogenen Daten von Angehörigen, anderen Bezugspersonen des Patienten sowie sonstiger Dritter, die dem Krankenhaus im Zusammenhang mit der Behandlung bekannt werden.

**(2)Patientendaten dürfen unbeschadet anderer Rechtsvorschriften verarbeitet werden, soweit**

**1. dies im Rahmen des Behandlungsverhältnisses auf vertraglicher Grundlage mit einem Angehörigen eines Gesundheitsberufs, der dem Berufsgeheimnis unterliegt, oder durch andere Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, erforderlich ist; die Verarbeitung von Daten zu diesen Zwecken richtet sich nach den für die genannten Personen geltenden Geheimhaltungspflichten, oder,**
**2. dies zur Ausbildung oder Fortbildung erforderlich ist und dieser Zweck nicht in vertretbarer Weise mit anonymisierten Daten erreichbar ist.**

Beruht die Verarbeitung auf einer Einwilligung des Patienten, bedarf diese einer schriftlichen Erklärung, die auch elektronisch erfolgen kann, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.

(3)Eine Übermittlung von Patientendaten an Personen und Stellen außerhalb des Krankenhauses ist nur zulässig, soweit sie erforderlich ist

1. zur Erfüllung einer gesetzlich vorgeschriebenen Behandlungs- oder Mitteilungspflicht,
2. a) zur Entscheidungsfindung der Krankenkassen, ob und inwieweit Präventions-, Rehabilitations- oder andere komplementäre Maßnahmen angezeigt sind,

   b) zur Durchführung des Behandlungsvertrages einschließlich der Nachbehandlung, soweit der Patient nach Hinweis auf die beabsichtigte Übermittlung nicht etwas anderes bestimmt hat,
3. zur Abwehr von gegenwärtigen Gefahren für das Leben, die Gesundheit oder die persönliche Freiheit des Patienten oder eines Dritten, sofern diese Rechtsgüter das Geheimhaltungsinteresse des Patienten deutlich überwiegen,
4. zur Durchführung qualitätssichernder Maßnahmen in der Krankenversorgung, wenn das Interesse der Allgemeinheit an der Durchführung der beabsichtigten Maßnahme die schutzwürdigen Belange des Patienten erheblich überwiegt,
5. zur Durchführung eines mit der Behandlung zusammenhängenden gerichtlichen Verfahrens,
6. zur Feststellung der Leistungspflicht, Abrechnung und Überprüfung der Wirtschaftlichkeit durch die Sozialleistungsträger,
7. zur Unterrichtung der Angehörigen, soweit der Patient nicht seinen gegenteiligen Willen kundgetan, hat oder sonstige Anhaltspunkte bestehen, dass eine Übermittlung nicht angebracht ist.
8. oder sie in einer anderen Rechtsvorschrift geregelt ist.

In anderen Fällen ist eine Übermittlung von Daten nur mit Einwilligung des Patienten zulässig. Absatz 2 Satz 2 und 3 gilt entsprechend.

(4)Dem Patienten ist auf Antrag kostenfrei Einsicht, insbesondere in seine Krankendaten zu gewährleisten.

Soweit Auskunfts- und Einsichtsansprüche medizinische Daten des Patienten betreffen, darf sie nur der behandelnde Arzt erfüllen. Die Auskunfts- und Einsichtsansprüche können im Interesse der Gesundheit des Patienten begrenzt werden; durch berechtigte Geheimhaltungsinteressen Dritter werden sie eingeschränkt.

(5)Nach Abschluss der Behandlung unterliegen personenbezogene Daten, die in automatisierten Verfahren gespeichert und direkt abrufbar sind, dem alleinigen Zugriff der jeweiligen Fachabteilung. Dies gilt nicht für diejenigen Daten, die für das Auffinden der sonstigen Patientendaten erforderlich sind. Die Eröffnung des Direktzugriffs auf den Gesamtdatenbestand für andere Stellen im Krankenhaus ist unter den Voraussetzungen des Absatzes 2 nur mit Zustimmung der Fachabteilung zulässig.

(6)Der Krankenhausträger hat einen Datenschutzbeauftragten zu benennen.

(7)Soweit sich das Krankenhaus bei der Verarbeitung von Patientendaten eines Auftragsverarbeiters bedient, ist insbesondere sicherzustellen, dass dieser die § 203 des Strafgesetzbuches entsprechende Schweigepflicht einhält.

**§ 34 Datenschutz bei Forschungsvorhaben**

(1) Ärzte dürfen Patientendaten, die innerhalb ihrer Fachabteilung oder bei Hochschulen innerhalb ihrer medizinischen Einrichtungen, in den Universitätskliniken oder in sonstigen medizinischen Einrichtungen gespeichert sind, für eigene wissenschaftliche Forschungsvorhaben verarbeiten. Satz 1 gilt entsprechend für sonstiges wissenschaftliches Personal dieser Einrichtungen, soweit es der Geheimhaltungspflicht des § 203 des Strafgesetzbuches unterliegt.

(2) Zu Zwecken der wissenschaftlichen Forschung ist die Übermittlung von Patientendaten an Dritte und die Verarbeitung durch sie zulässig, soweit der Patient eingewilligt hat. § 33 Abs. 2 Satz 2 und 3 gilt entsprechend.

(3) Der Einwilligung des Patienten bedarf es nicht, wenn der Zweck eines bestimmten Forschungsvorhabens nicht auf andere Weise erfüllt werden kann und

1. das berechtigte Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse des Patienten erheblich

überwiegt oder

2. es nicht zumutbar ist, die Einwilligung einzuholen und schutzwürdige Belange des Patienten nicht beeinträchtigt werden.

Die übermittelnde Stelle hat den Empfänger, die Art der zu übermittelnden Daten, die betroffenen Patienten und das Forschungsvorhaben aufzuzeichnen.

(4) Sobald es der Forschungszweck erlaubt, sind die personenbezogenen Daten derart zu verändern, dass sie keine Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person mehr sind. Soweit dies nicht möglich ist, sind die Merkmale, mit deren Hilfe ein Personenbezug hergestellt werden kann, gesondert zu speichern, sobald es der Forschungszweck erlaubt; die Merkmale sind zu löschen, sobald der Forschungszweck erreicht ist.

(5) Soweit die Bestimmungen dieses Gesetzes auf den Empfänger von Patientendaten keine Anwendung finden, dürfen sie nur übermittelt werden,

1. wenn sich der Empfänger verpflichtet,
   a) die Daten nur für das von ihm genannte Forschungsvorhaben zu verwenden,
   b) die Bestimmungen des Absatzes 4 einzuhalten und
   c) dem Sächsischen Datenschutzbeauftragten auf Verlangen Einsicht und Auskunft zu gewähren, und
2. wenn der Empfänger nachweist, dass bei ihm die technischen und organisatorischen Voraussetzungen vorliegen, um der Verpflichtung nach Nummer 1 Buchst. b zu entsprechen.

## Sächsisches Datenschutzdurchführungsgesetz SächsDSDG

**§ 22 Ordnungswidrigkeiten**

(1) Ordnungswidrig handelt, wer entgegen den Vorschriften dieses Gesetzes oder einer anderen Rechtsvorschrift über den Schutz personenbezogener Daten, die nicht offenkundig sind, verarbeitet oder die Übermittlung durch unrichtige Angaben erschleicht.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfundzwanzigtausend Euro geahndet werden.

(4) Wer eine der in Absatz 1 bezeichneten Handlungen gegen Entgelt oder in der Absicht begeht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Der Versuch ist strafbar.

## Urheberrechtsgesetz UrhG

**§ 106 Unerlaubte Verwertung urheberrechtlich gesicherter Werke**

(1) Wer in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten ein Werk oder eine Bearbeitung oder Umgestaltung eines Werkes vervielfältigt, verbreitet oder öffentlich wiedergibt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

**§ 3 MantelTVÄ UKL, Verschwiegenheit**

(2) Ärzte haben über interne Angelegenheiten, insbesondere Angelegenheiten, deren Geheimhaltung durch gesetzliche Vorschriften vorgesehen oder vom Arbeitgeber angeordnet ist, Verschwiegenheit zu wahren; dies gilt auch über die Beendigung des Arbeitsverhältnisses hinaus. Die Regelung betrifft auch Schriftstücke, Aufzeichnungen und bildliche Darstellungen.

**§ 3 HTV UKL, Verschwiegenheit**

(2) Die Beschäftigten haben über Angelegenheiten, deren Geheimhaltung durch gesetzliche Vorschriften vorgesehen oder vom Arbeitgeber angeordnet ist, Verschwiegenheit zu wahren; dies gilt auch über die Beendigung des Arbeitsverhältnisses hinaus.

**§ 3 TVöD Länder**

(2) Die Beschäftigten haben über Angelegenheiten, deren Geheimhaltung durch gesetzliche Vorschriften vorgesehen oder vom Arbeitgeber angeordnet ist, Verschwiegenheit zu wahren; dies gilt auch über die Beendigung des Arbeitsverhältnisses hinaus.

**§ 3 TV-Ä**

(2) Die Ärzte haben über Angelegenheiten, deren Geheimhaltung durch gesetzliche Vorschriften vorgesehen oder vom Arbeitgeber angeordnet ist, Verschwiegenheit zu wahren; dies gilt auch über die Beendigung des Arbeitsverhältnisses hinaus. Bei Unterlagen, die ihrem Inhalt nach von der ärztlichen Schweigepflicht erfasst werden, darf der Arbeitgeber nur die Herausgabe an den ärztlichen Vorgesetzten verlangen.

## Gesetz gegen den unlauteren Wettbewerb UWG

**§ 17 Verrat von Geschäfts- und Betriebsgeheimnissen**

(1) Wer als eine bei einem Unternehmen beschäftigte Person ein Geschäfts- oder Betriebsgeheimnis, das ihr im Rahmen des Dienstverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Dienstverhältnisses unbefugt an jemand zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, mitteilt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft..

(2) ...

(3) Der Versuch ist strafbar.

(4) In besonders schweren Fällen ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. gewerbsmäßig handelt,
2. bei der Mitteilung weiß, dass das Geheimnis im Ausland verwertet werden soll, oder
3. eine Verwertung nach Absatz 2 Nr. 2 im Ausland selbst vornimmt.

# Strafgesetzbuch StGB

**§ 202 StGB, Verletzung des Briefgeheimnisses**

(1) Wer unbefugt
1. einen verschlossenen Brief oder ein anderes verschlossenes Schriftstück, die nicht zu seiner Kenntnis bestimmt sind, öffnet oder
2. sich vom Inhalt eines solchen Schriftstücks ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wenn die Tat nicht in § 206 *(Post- und Fernmeldegeheimnis)* mit Strafe bedroht ist.

(2) Ebenso wird bestraft, wer sich unbefugt vom Inhalt eines Schriftstücks, das nicht zu seiner Kenntnis bestimmt und durch ein verschlossenes Behältnis gegen Kenntnisnahme besonders gesichert ist, Kenntnis verschafft, nachdem er dazu das Behältnis geöffnet hat.

**(3) Einem Schriftstück im Sinne der Absätze 1 und 2 steht eine Abbildung gleich.**

**§ 202 a StGB, Ausspähen von Daten**

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft..

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

**§ 202 b StGB, Abfangen von Daten**

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

**§ 202 c StGB, Vorbereiten des Ausspähens und Abfangens von Daten**

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

**§ 202 d, Datenhehlerei**

(1) Wer Daten (§ 202a Absatz 2), die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Die Strafe darf nicht schwerer sein als die für die Vortat angedrohte Strafe.

(3) Absatz 1 gilt nicht für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. ...

**Auszug aus dem Strafgesetzbuch (StGB)**

**§ 203 StGB, Verletzung von Privatgeheimnissen**

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,

2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung,

….

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

(2) Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1.Amtsträger,

2.für den öffentlichen Dienst besonders Verpflichteten,

3.Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt,

4….

5. öffentlich bestelltem Sachverständigen, der auf die gewissenhafte Erfüllung seiner Obliegenheiten auf Grund eines Gesetzes förmlich verpflichtet worden ist, oder

6. Person, die auf die gewissenhafte Erfüllung ihrer Geheimhaltungspflicht bei der Durchführung wissenschaftlicher Forschungsvorhaben auf Grund eines Gesetzes förmlich verpflichtet worden ist, anvertraut worden oder sonst bekanntgeworden ist.

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

(2a) (weggefallen)

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

(4) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als mitwirkende Person oder als bei den in den Absätzen 1 und 2 genannten Personen tätiger Beauftragter für den Datenschutz bekannt geworden ist. Ebenso wird bestraft, wer 1.

als in den Absätzen 1 und 2 genannte Person nicht dafür Sorge getragen hat, dass eine sonstige mitwirkende Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind,

2. als im Absatz 3 genannte mitwirkende Person sich einer weiteren mitwirkenden Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, bedient und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind, oder

3. nach dem Tod der nach Satz 1 oder nach den Absätzen 1 oder 2 verpflichteten Person ein fremdes Geheimnis unbefugt offenbart, das er von dem Verstorbenen erfahren oder aus dessen Nachlass erlangt hat.

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

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

**§ 204 StGB, Verwertung fremder Geheimnisse**

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

(2) § 203 Abs. 4 gilt entsprechend

**§ 263 a StGB, Computerbetrug**

(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, dass er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflusst, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) § 263 (Betrug) Abs. 2 bis 7 gilt entsprechend.

**§ 269 StGB, Fälschung beweiserheblicher Daten**

(1) Wer zur Täuschung im Rechtsverkehr beweiserhebliche Daten so speichert oder verändert, dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte oder veränderte Daten gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.
(2) Der Versuch ist strafbar.
(3) § 267 Abs. 3 und 4 gilt entsprechend.

**§ 270 StGB, Täuschung im Rechtsverkehr bei Datenverarbeitung**

Der Täuschung im Rechtsverkehr steht die fälschliche Beeinflussung einer Datenverarbeitung im Rechtsverkehr gleich.

**§ 303 a StGB, Datenveränderung**

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
(2) Der Versuch ist strafbar

## Telekommunikationsgesetz TKG

**§ 88 Fernmeldegeheimnis**

(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.
(2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.
(3) Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.

Anlage 4:

**Übersicht der zum Zeitpunkt der Auftragserteilung vereinbarten Leistungsstandorte des Auftragnehmers**