

## Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO

zwischen dem

**Universitätsklinikum Augsburg A.d.ö.R.**

Stenglinstraße 2, 86156 Augsburg

vertreten durch

den Kaufmännischen Direktor Herrn Michael Bungarten

– nachstehend Auftraggeber genannt –

und

Firmenname

Adresse des Dienstleisters

vertreten durch

Angabe des Vertretungsberechtigten

– nachstehend Auftragnehmer genannt –

### Präambel

Dieser Auftragsverarbeitungs-Vertrag (AV-Vertrag) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus dem in § 2 genannten Vertrag oder der dort beschriebenen Leistungen des Auftragnehmers ergeben.

Sämtliche in diesem Vertrag beschriebenen Verpflichtungen finden Anwendung auf alle Tätigkeiten, die mit der Auftragserfüllung 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.

### § 1 Definitionen

Es gelten die Begriffsbestimmungen entsprechend Art. 4 DS-GVO, § 2 UWG und § 2 TMG sowie Art. 27 BayKrG.

### § 2 Gegenstand des Auftrags (Bitte auswählen nach Vertragskonstellation)

- ☐ Gegenstand der Vereinbarung ist die Verarbeitung personenbezogener Daten (nachstehend „Daten“ genannt) durch den Auftragnehmer für den Auftraggeber in dessen Auftrag und nach dessen Weisung in Ergänzung des Vertrags der Parteien vom   Angabe Datum, (nachstehend „Hauptvertrag“ genannt“). Die Vereinbarung gilt entsprechend für (Fern-) Prüfung und Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen, wenn dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

- ☐ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Leistungen durch den Auftragnehmer:

### § 3 Konkretisierung des Auftragsinhalts:

Der Auftragnehmer erhält Zugriff auf folgende personenbezogene Daten (dadurch, dass der Auftraggeber ihm die Daten bereitstellt oder ihm einen Zugriff auf die Daten ermöglicht), bzw. der Auftraggeber erlaubt dem Auftragnehmer, folgende personenbezogene Daten zu erheben:

#### a) Betroffene Datenarten /-kategorien

- ☐ Personenstammdaten (z. B. Name, Geburtsdatum)
- ☐ Kontaktdaten/Kommunikationsdaten (z. B. IP-Adressen, Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Auskunftsangaben (von Dritten, z. B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☐ Planungs- und Steuerungsdaten
- ☐ Besondere Kategorien von Daten, insbesondere
  - ☐ rassische oder ethnische Herkunft
  - ☐ religiöse Überzeugung
  - ☐ weltanschauliche (philosophische) Überzeugung
  - ☐ politische Überzeugungen/Meinungen
  - ☐ Gesundheitsdaten inkl. genetischer Daten (Befunde, Diagnosen, etc. ...)
  - ☐ Biometrische Daten zur (eindeutigen) Identifizierung einer Person
  - ☐ Gewerkschaftszugehörigkeit
  - ☐ Sexualleben oder der sexuellen Orientierung

#### b) Kategorien betroffener Personen

- ☐ Patienten
- ☐ Mitarbeitende
- ☐ Bewerber
- ☐ Ehrenamtliche
- ☐ Geschäftspartner
- ☐ Angehörige
- ☐ gesetzliche Vertreter / gesetzliche Betreuer / Bevollmächtigte
- ☐ Veranstaltungsteilnehmer
- ☐ Kinder / Jugendliche
- ☐ sonstige:

Der Zugriff auf die Daten bzw. die Datenübermittlung erfolgt wie folgt:

- ☐ Übermittlung durch den Auftraggeber über:
- ☐ Bereitstellung durch den Auftraggeber über:
- c) Der Auftragnehmer erbringt für den Auftraggeber folgende Prüf- bzw. Wartungstätigkeiten, bei denen eine Zugriffsmöglichkeit auf personenbezogene Daten nicht ausgeschlossen werden kann:
  - ☐ Prüfung/**Wartung vor Ort**, bei denen eine Zugriffsmöglichkeit auf personenbezogene Daten nicht ausgeschlossen werden kann:
  - ☐ Diagnose per **Fernzugriff** für folgende Hardwareprodukt(e), bei denen eine Zugriffsmöglichkeit auf personenbezogene Daten nicht ausgeschlossen werden kann:
  - ☐ Software-Prüfung/**Wartung per Fernzugriff** für folgend(e) Softwareprodukt(e), bei denen eine Zugriffsmöglichkeit auf personenbezogene Daten nicht ausgeschlossen werden kann:

#### **§ 4 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 (Fern-) 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.

#### **§ 5 Dauer des Auftrags**

- (1) Dauer des Auftrags
  - ☐ Die Laufzeit dieses AV-Vertrages richtet sich nach der Laufzeit des Hauptvertrags, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.
  - ☐ Die Laufzeit dieses AV-Vertrages endet am Datum, sofern sich aus den Bestimmungen dieses AV-Vertrages nicht etwas anderes ergibt.
  - ☐ Der Vertrag wird mit der Unterzeichnung wirksam und läuft auf unbestimmte Zeit. Jede Partei ist berechtigt, den Vertrag mit einer Frist von Frist eintragen zu kündigen.

- (2) Es ist den Vertragspartnern bewusst, dass ohne Vorliegen eines gültigen AV-Vertrages z.B. bei Beendigung des vorliegenden Vertragsverhältnisses, keine (weitere) Auftragsverarbeitung durchgeführt werden darf.
- (3) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.
- (4) Kündigungen bedürfen zu ihrer Wirksamkeit der Schriftform.

## **§ 6 Weisungsbefugnis des Auftraggebers**

- (1) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Auftraggebers. Ausgenommen hiervon sind Sachverhalte, in denen dem Auftragnehmer eine Verarbeitung aus zwingenden rechtlichen Gründen auferlegt wird. Der Auftragnehmer unterrichtet soweit ihm möglich in derartigen Situationen den Auftraggeber vor Beginn der Verarbeitung über die entsprechenden rechtlichen Anforderungen. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann.
- (2) Die Weisungen des Auftraggebers werden vom Auftraggeber dokumentiert und dem Auftragnehmer 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, steht dem Auftragnehmer ein ordentliches Kündigungsrecht bezüglich des von der Weisung betroffenen AV-Vertrages sowie der von der AV-Vereinbarung betroffenen Bestandteile des entsprechenden Hauptvertrages zu. Verweigert der Auftragnehmer, die Änderung durchzuführen, steht auch dem Auftraggeber ein ordentliches Kündigungsrecht zu. Erfolgt eine Kündigung, so ist für die restliche Vertragslaufzeit weiterhin die vertraglich vereinbarte Leistung durch den Auftragnehmer zu erbringen.
- (4) Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragnehmer notiert sich Datum, Uhrzeit und Person, welche die mündliche Weisung erteilte sowie den Grund, warum keine schriftliche Beauftragung erfolgen konnte.
- (5) Ansprechpartner (weisungsberechtigte Personen) des Auftraggebers sind in der Anlage 3 benannt.

## **§ 7 Leistungsort**

- (1) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.
- (2) Werden im Rahmen dieses Auftrages auch Daten verarbeitet, die unter ein Berufsgeheimnis im Sinne von § 203 StGB fallen, dann dürfen Unterauftragnehmer im Ausland jedoch nur dann zur Vertragserfüllung herangezogen werden, wenn der dort bestehende Schutz der Geheimnisse dem Schutz in Deutschland vergleichbar ist.

## § 8 Pflichten des Auftragnehmers

- (1) Der Auftragnehmer darf Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten.
- (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 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.
- (4) 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.
- (5) 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, auf das Fernmeldegeheimnis verpflichten und über die sich daraus ergebenden besonderen Geheimhaltungspflichten belehren.
- (6) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln.
- (7) Sofern eine gesetzliche Pflicht zur Bestellung eines Datenschutzbeauftragten bei Auftragnehmer besteht, teilt dieser dessen Namen und Kontaktdaten dem Auftraggeber mit. 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 für Datenschutzfragen. Angaben zum Datenschutzbeauftragten bzw. Ansprechpartner für Datenschutzfragen beim Auftragnehmer sind in der Anlage 3 enthalten. Ein Wechsel des Datenschutzbeauftragten bzw. des Ansprechpartners für Datenschutzfragen ist dem Auftraggeber unverzüglich schriftlich mitzuteilen.
- (8) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei Verstößen des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Informationspflichten

gegenüber der jeweils zuständigen Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen nach Art. 33, 34 DS-GVO.

- (9) 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) 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.
- (11) Ist der Auftraggeber aufgrund geltender Datenschutzgesetze gegenüber einer betroffenen Person verpflichtet, Auskünfte zur Verarbeitung 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.
- (12) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde bei dem Auftragnehmer ermittelt.
- (13) 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.
- (14) 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.
- (15) 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.
- (16) Der Auftragnehmer speichert keine Patientendaten auf Systemen, die außerhalb der Verfügungsgewalt des Auftraggebers liegen bzw. die nicht dem Beschlagnahmeschutz unterliegen.
- (17) 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.
- (18) Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren, zu dokumentieren und in geeigneter Weise gegenüber dem Auftraggeber auf Anforderung nachzuweisen.

### **§ 8.1 Pflicht des Auftragnehmers zur Einhaltung der Geheimnisschutzregeln beim Auftraggeber**

Der Auftragnehmer verpflichtet sich bei der Auftragserfüllung auch folgende Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen.

#### ☐ Wahrung des Berufsgeheimnisses nach § 203 StGB (Einhaltung der Schweigepflicht)

- (1) Im Rahmen dieses Auftrages werden auch Daten verarbeitet, die unter ein Berufsgeheimnis (im Sinne von § 203 StGB) fallen. Der Auftragnehmer verpflichtet sich über Berufsgeheimnisse

- (2) Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben erforderlich ist.

Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich Personen, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken und unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist, strafbar machen nach § 203 Abs. 4 S. 1.

Zudem macht sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Geheimnis offenbart, und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde.

- (3) Der Auftragnehmer stellt sicher, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des Auftraggebers befassten Beschäftigten und andere für den Auftragnehmer tätigen Personen (z. B. Unterauftragnehmer), die damit befasst sind, sich in Textform dazu verpflichtet haben, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren und sie über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB belehrt wurden.
- (4) Der Auftragnehmer wird darauf hingewiesen, dass Daten, die er im Auftrag eines Berufsgeheimnisträgers verarbeitet u. U. dem Zeugnisverweigerungsrecht von sogenannten mitwirkenden Personen unterliegen (§ 53a Strafprozessordnung (StPO)). Entsprechend § 53a StPO entscheidet jedoch der Berufsgeheimnisträger über die Ausübung des Schweigerechts. Im Falle einer Befragung wird der Auftragnehmer unter Hinweis auf § 53a StPO dieser widersprechen und unverzüglich den Auftraggeber informieren, der daraufhin bzgl. der Wahrnehmung des Schweigerechts entscheidet.
- (5) Der Auftragnehmer wird darauf hingewiesen, dass die in seinem Gewahrsam befindlichen Geheimnisschutzdaten dem Beschlagnahmeverbot gemäß § 97 Abs. 2 StPO unterliegen. Die Daten dürfen nicht ohne das Einverständnis des Auftraggebers (Berufsgeheimnisträger) herausgegeben werden. Im Falle einer Beschlagnahme wird der Auftragnehmer dieser widersprechen und unverzüglich den Auftraggeber informieren.

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

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

- (1) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten an Arbeitsplatzsystemen werden erst nach Freigabe durch den jeweiligen Berechtigten / zuständigen Mitarbeiter des Auftraggebers durchgeführt.
- (2) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten von automatisierten Verfahren oder von Datenverarbeitungsanlagen werden, sofern hierbei ein Zugriff auf personenbezogene Daten nicht sicher ausgeschlossen werden kann, ausschließlich mit 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 abubrechen.
- (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 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.

## **§ 10 Pflichten des Auftraggebers**

- (1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Der Auftraggeber wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z. B. durch Einholung von Einwilligungserklärungen für die Verarbeitung der Daten) geschaffen werden, damit der Auftragnehmer die vereinbarten Leistungen rechtsverletzungsfrei erbringen kann.
- (2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
- (3) Der Auftraggeber ist hinsichtlich der vom Auftragnehmer eingesetzten und vom Auftraggeber genehmigten Verfahren zur automatisierten Verarbeitung personenbezogener Daten datenschutzrechtlich verantwortlich und hat – neben der eigenen Verpflichtung des Auftragnehmers – ebenfalls die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten.
- (4) Dem Auftraggeber obliegen die aus Art. 33, 34 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) 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.
- (8) Erteilt der Auftraggeber Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, ist hierzu vorab eine gesonderte schriftliche Vereinbarung zu treffen.

## **§ 11 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.

## § 12 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 Haupt-Vertrag 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
  - sämtliche im Rahmen des Auftrags in seinen Besitz gelangte Unterlagen oder Datenträger,
  - erstellte Verarbeitungsergebnisse,
  - Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehendem Auftraggeber auszuhändigen oder auf Anweisung des Auftraggebers datenschutzkonform zu löschen bzw. zu vernichten, sofern keine gesetzliche Pflicht zur Aufbewahrung besteht. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
- (5) 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.

## § 13 Unterauftragnehmer

- (1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
- (2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) wie folgt beauftragen: ☐  
 Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen nicht zur Begründung von Unterauftragsverhältnissen mit Unterauftragnehmern befugt.
  - ☐ Die vertraglich vereinbarten Leistungen werden unter Einschaltung der in Anlage 1 genannten Unterauftragnehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Unterauftragnehmern befugt, soweit er den Auftraggeber hiervon vorab in Kenntnis setzt und dieser der Beauftragung des Unterauftragnehmers vorab schriftlich oder in dokumentiertem elektronischen Format zugestimmt hat.
- (3) 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.
- (4) 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.
- (5) Kommt der Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Unterauftragnehmers.
- (6) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers. Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.
- (7) Sofern Unterauftragnehmer im Rahmen ihrer Tätigkeit Kenntnis von fremden Geheimnissen im Sinne dieser Vereinbarung erlangen könnten, wird sie der Auftragnehmer zur Geheimhaltung verpflichtet. Der Auftragnehmer wird ferner etwaige Unterauftragnehmer dazu verpflichten, sämtliche von diesen eingesetzten Personen und etwaige weitere Unterauftragnehmer, die bestimmungsgemäß mit Geheimnisschutzdaten in Berührung kommen oder bei denen dies nicht auszuschließen ist, zur Verschwiegenheit zu verpflichten und über die Folgen einer Pflichtverletzung zu belehren. Des Weiteren werden Unterauftragnehmer, über das bestehende Schweigerecht gemäß § 53a StPO sowie den Beschlagnahmenschutz gemäß § 97 StPO informiert; dies beinhaltet auch den Hinweis bzgl. des Rechts des Berufsgeheimnisträgers, über dieses Recht zu entscheiden und der damit verbundenen Pflicht des Auftragnehmers, unverzüglich den Auftraggeber bzgl. der Wahrnehmung dieser Rechte zu kontaktieren.

## **§ 14 Zurückbehaltungsrecht**

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

## **§ 15 Haftung**

- (1) Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.
- (2) Der Auftragnehmer stellt den Auftraggeber auf erstes Anfordern von sämtlichen Ansprüchen frei, die betroffene Personen gegen den Auftraggeber wegen der Verletzung einer dem Auftragnehmer durch die DSGVO auferlegten Pflicht oder der Nichtbeachtung oder Verletzung einer vom Auftraggeber in dieser AV-Vereinbarung oder einer gesondert erteilten Anweisung geltend machen.
- (3) Die Parteien stellen sich jeweils von der Haftung frei, wenn / soweit eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einer betroffenen Person eingetreten ist, verantwortlich ist. Im Übrigen gilt Art. 82 Absatz 5 DS-GVO.
- (4) Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

## **§ 16 Vertragsstrafe**

Bei Verstößen des Auftragnehmers gegen die Regelungen dieses Vertrages zur Einhaltung des Datenschutzes, wird pro Verstoß eine Vertragsstrafe bis zu 5 % des Auftragswerts vereinbart, soweit der Verstoß nicht unverzüglich behoben wird und es durch den Verstoß zu keinem Schaden gekommen ist oder kein Schaden droht. Die geltend gemachte Vertragsstrafe wird auf dem Auftraggeber zustehende Haftungsansprüche nach Ziffer 15 angerechnet.

## **§ 17 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.

## **§ 18 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 § 18 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.

## **§ 19 Rechtswahl, Gerichtsstand**

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

Augsburg, den \_\_\_\_\_

\_\_\_\_\_, den \_\_\_\_\_

\_\_\_\_\_  
Universitätsklinikum Augsburg

Name:  
Funktion:  
Bereich / Klinik:

\_\_\_\_\_  
Auftragnehmer

Name:  
Funktion:

Augsburg, den \_\_\_\_\_

\_\_\_\_\_  
Universitätsklinikum Augsburg

Name:  
Funktion:  
Bereich / Klinik:

Anlage 1: Liste der Unterauftragnehmerverhältnisse

Anlage 2: Technisch-organisatorischen Maßnahmen beim Auftragnehmer

Anlage 3: Kontaktpersonen