

Hinweis: Der nachstehende Mustertext soll eine Orientierungshilfe bieten. Er ist je nach den Umständen des konkreten Einzelfalls anzupassen. Bei komplexen Auftragsverhältnissen werden ggf. weitere bzw. ergänzende Vertragsklauseln notwendig.

Gegenstand dieses Mustertextes sind ausschließlich datenschutzrechtliche Regelungen zur Auftragsverarbeitung. Sämtliche in diesem Mustertext beschriebenen Verpflichtungen finden Anwendungen auf alle Verarbeitungstätigkeiten, die mit einem Hauptvertrag in Zusammenhang stehen. Dieser Mustertext wurde auf Basis verschiedener, frei zugänglicher und frei verwendbarer Vorlagen erstellt, wurde jedoch nicht durch einen Fachanwalt für Datenschutzrecht juristisch geprüft.

Die einzelnen Festlegungen nach § 29 Abs.3 KDR-OG sollten vollständig in die Vereinbarung übernommen und wie eine Checkliste abgearbeitet werden. Die für das konkrete Dienstleistungsverhältnis zutreffenden Alternativen sollten angekreuzt werden. Leerfelder sind ggf. entsprechend des konkreten Auftrags auszufüllen. Vergütungs- und Haftungsregelungen zu den einzelnen Leistungen des Auftragnehmers sollten im Hauptvertrag vereinbart werden.

Auftragsverarbeitungsvertrag

zwischen dem

VERANTWORTLICHER
STRAÙE
PLZ ORT

vertreten durch

- NAME -

(Verantwortlicher im Sinne der KDR-OG, nachfolgend „Auftraggeber“ genannt)

und

Name/Firma Auftragnehmer
Straße und Hausnr.
Postleitzahl und Ort

vertreten durch

- NAME -

(Auftragsverarbeiter im Sinne der KDR-OG, nachfolgend „Auftragnehmer“ genannt)

Präambel

Dieser Auftragsverarbeitungs-Vertrag (AV-Vertrag) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus dem Hauptvertrag in ihren Einzelheiten beschriebenen Auftragsverarbeitung sowie den in § 1 „Gegenstand des Auftrags“ dargestellten Leistungen ergeben. Sie ersetzt ggfs. bestehende, ältere Datenschutzvereinbarungen und findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten des Auftraggebers verarbeiten.

Für den Orden der Barmherzige Brüder in Bayern, Körperschaft des öffentlichen Rechtes, und seine Einrichtungen gilt die Kirchliche Datenschutzregelung der Ordensgemeinschaft päpstlichen Rechts (KDR-OG) in der jeweils gültigen Fassung.

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 Gegenstand der Verarbeitung

(1) Der Auftragnehmer verarbeitet personenbezogene Daten (nachstehend „Daten“ genannt) gem. § 4 Nr. 10 KDR-OG im Auftrag des Auftraggebers nach den gesetzlichen Grundsätzen für die Verarbeitung personenbezogener Daten gem. § 7 KDR-OG.

(2) Der Gegenstand der Verarbeitung

a) ergibt sich aus dem nachfolgend genannten Hauptvertrag:

.....
.....
vom, auf den hier verwiesen wird.

b) ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

.....
.....
.....(Definition der Aufgaben)

(3) Art und Zweck der vorgesehenen Verarbeitung von Daten:

a) Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in dem unter Abs. 2 genannten Hauptvertrag.

b) Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

.....
.....
.....(Beschreibung Art und Zweck der Aufgaben)

(4) Im Einzelnen sind insbesondere folgende Daten Bestandteil der Datenverarbeitung:

a) Die Art der verwendeten personenbezogenen Daten ist im Hauptvertrag konkret beschrieben unter:

.....

b) Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien):

- Personenstammdaten
- Medizinische und pflegerische Patientendaten (Befunde, Diagnosen, ...)
- Beratungsdokumentation
- Kontaktdaten/Kommunikationsdaten (z.B. Telefon, E-Mail, IP-Adressen)
- Vertragsstammdaten (z.B. Vertragsbeziehung, Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- Daten von Beschäftigten und Mitarbeitern (z.B. Bewerbungsunterlagen, Leistungsnachweise, Urlaubsanträge etc.)
-
-
-

(5) Im Einzelnen sind insbesondere folgende Kategorien von Personen von der Datenverarbeitung betroffen:

a) Die Kategorien der durch die Verarbeitung betroffenen Personen sind im Hauptvertrag konkret beschrieben unter:

.....

b) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Patienten
- Bewohner
- Klienten
- Interessenten
- Beschäftigte
- Lieferanten
- Handelsvertreter
- Kundenhistorie

- Ansprechpartner
-
-
-

§ 2 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 § 4 Nr. 9 KDR-OG).

(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. Sofern die personenbezogenen Daten des Auftraggebers dem Regelungsbereich des § 203 StGB (Berufsgeheimnisse) unterliegen, werden alle Personen, die auftragsgemäß auf diese personenbezogenen Daten des Auftraggebers zugreifen können, auf die Verschwiegenheitspflicht gem. § 203 StGB verpflichtet und über ihre Geheimhaltungspflichten belehrt.

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

§ 3 Dauer des Auftrags

(1) Die Laufzeit dieses Vertrags (Dauer des Auftrags zur Verarbeitung) ist wie folgt festgelegt:

- Die Dauer des Auftrags zur Verarbeitung (Laufzeit) entspricht der Laufzeit des Hauptvertrags.
- Die Dauer des Auftrags zur Verarbeitung (Laufzeit) ist befristet zum
- Der Auftrag zur Verarbeitung ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von zum gekündigt werden.

(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) Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

(4) Kündigungen bedürfen zu ihrer Wirksamkeit der Schriftform.

§ 4 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, die er durch Einzelweisungen konkretisieren kann.

(2) 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.

(3) Weisungsberechtigte Personen des Auftraggebers sind: (Name und Kontaktdaten)

(4) Weisungsempfänger beim Auftragnehmer sind: (Name und Kontaktdaten)

§ 5 Leistungsort

Der Auftragnehmer wird die vertraglichen Leistungen ausschließlich in der Europäischen Union (EU), im Europäischen Wirtschaftsraum (EWR) oder Schweiz erbringen. Dies gilt in gleicher Weise für etwaige Unterauftragnehmer. Eine Verlagerung außerhalb der EU/EWR ist nur unter den Voraussetzungen des § 40 KDR-OG zulässig. Erfolgt eine Leistungserbringung in einem Drittland, garantiert der Auftragnehmer die Einhaltung der diesbezüglichen Vorgaben des § 40 KDR-OG und weist dies auf Verlangen nach. Wenn der Auftragnehmer die geschuldeten Leistungen ganz oder teilweise von einem Standort außerhalb der/des 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 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 für den Auftraggeber maßgeblichen 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 § 26 KDR-OG 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 1 zu diesem Vertrag.

- Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann zusätzlich erfolgen durch:
- die Einhaltung genehmigter Verhaltensregeln gemäß § 29 Abs. 6 KDR-OG;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß § 29 Abs. 6 KDR-OG;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz).

(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 § 31 KDR-OG. Er stellt dem Auftraggeber auf Anforderung die für die Übersicht nach § 31 KDR-OG notwendigen Angaben zur Verfügung. Des Weiteren stellt er das Verzeichnis auf Anfrage der Aufsichtsbehörde zur Verfügung.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Datenschutz-Folgenabschätzung gem. § 35 KDR-OG mit allen ihm zur Verfügung stehenden Informationen. Im Falle der Notwendigkeit einer vorherigen Konsultation der zuständigen Aufsichtsbehörde gem. § 35 KDR-OG unterstützt der Auftragnehmer den Auftraggeber auch hierbei.

(6) Die Wahrung des Fernmeldegeheimnisses entsprechend § 3 TDDDG muss vom Auftragnehmer gewährleistet werden. Dazu muss der Auftragnehmer alle Personen, die auftragsgemäß auf Daten des Auftraggebers mittels Telekommunikation wie Telefon oder E-Mail zugreifen können, 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) 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 § 37 KDR-OG erfüllt werden. Sofern kein Datenschutzbeauftragter beim Auftragnehmer benannt ist, benennt der Auftragnehmer dem Auftraggeber einen Ansprechpartner.

(9) 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 gem. § 33 und § 34 KDR-OG.

(10) 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.

(11) Überlassene personenbezogene Daten und 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.

(12) 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.

(13) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden bzw. laufende Ermittlungen einer Aufsichtsbehörde beim Auftragnehmer.

(14) 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.

(15) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahmung, 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 KDR-OG liegen.

(16) 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.

(17) Der Auftragnehmer speichert keine Patientendaten auf Systemen, die außerhalb der Verfügungsgewalt des Auftraggebers liegen bzw. die nicht dem Beschlagnahmenschutz unterliegen.

(18) 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.

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

§ 7 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 §§. 33, 34 KDR-OG 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 § 26 KDR-OG resultierenden Anforderungen bzgl. der Sicherheit der Verarbeitung seinerseits eingehalten werden. Insbesondere gilt dies für Fernzugriffe des Auftragnehmers auf die Datenbestände des Auftraggebers.

§ 8 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 KDR-OG 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.

§ 9 Berichtigung und Beschränkung bei Verarbeitung, Löschung und Rückgabe von Datenträgern

(1) Während der laufenden Beauftragung berichtigt, löscht oder sperrt der Auftragnehmer die vertragsgegenständlichen Daten nur auf dokumentierte Anweisung des Auftraggebers. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäÙen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(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) Nach Abschluss der Erbringung der Verarbeitungsleistungen muss der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers entweder löschen oder diesem zu-rückgeben, sofern nicht nach dem Unionsrecht oder dem für den Auftragnehmer geltendem nationalen Recht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

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

§ 10 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 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. Der Auftraggeber stimmt der Beauftragung der in Anlage 2 aufgeführten Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des § 29 KDR-OG.

(3) Im Fall einer bestehenden 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) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform). Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

(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 KDR-OG erfolgt.

(8) 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.

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

§ 11 Zurückbehaltungsrecht

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

§ 12 Haftung

(1) Auftraggeber und Auftragnehmer haften für den Schaden, der durch eine nicht der KDR-OG entsprechenden 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

1. er den aus der KDR-OG resultierenden und speziell für Auftragsverarbeiter auferlegten Pflichten nicht nachgekommen ist oder
2. er unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers handelte oder
3. 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

1. seinen ihm speziell durch die KDR-OG auferlegten Pflichten nicht nachgekommen ist oder
2. unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers oder gegen diese Anweisungen gehandelt hat

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

§ 13 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.

§ 14 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 § 14 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.

§ 15 Rechtswahl, Gerichtsstand

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

Ort, Datum

Ort, Datum

Auftraggeber

Auftragnehmer

Anlage 1 zum AV-Vertrag – Nachweis der allgemeinen technischen und organisatorischen Maßnahmen

1. Wahrung der Vertraulichkeit

- a) Die vom Auftragnehmer konkret ergriffenen technischen und organisatorischen Maßnahmen zur Wahrung der Vertraulichkeit werden an folgender Stelle ausführlich beschrieben:

.....
.....

- b) Folgende technischen und organisatorischen Maßnahmen werden vom Auftragnehmer zur Wahrung der Vertraulichkeit ergriffen:

1. Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen (z. B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pfortner, Alarmanlagen, Videoanlagen):

.....
.....
.....
.....
.....

(Konkret ergriffene Maßnahmen ausführlich beschreiben)

2. Zugangskontrolle

Keine unbefugte Systembenutzung (z. B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern):

.....
.....
.....
.....
.....

(Konkret ergriffene Maßnahmen ausführlich beschreiben)

3. Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems (z. B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen)

.....
.....
.....
.....
.....

(Konkret ergriffene Maßnahmen ausführlich beschreiben)

4. Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden (z. B. Mandantenfähigkeit, Sandboxing)

.....
.....
.....
.....
.....

(Konkret ergriffene Maßnahmen ausführlich beschreiben)

Pseudonymisierung Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen:

.....
.....
.....
.....
.....

(Konkret ergriffene Maßnahmen ausführlich beschreiben)

2. Integrität

- a) Die vom Auftragnehmer konkret ergriffenen technischen und organisatorischen Maßnahmen zur Wahrung der Integrität werden an folgender Stelle ausführlich beschrieben:

.....
.....

- b) Folgende technischen und organisatorischen Maßnahmen werden vom Auftragnehmer zur Wahrung der Integrität ergriffen:

1. Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport (z. B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur)

.....
.....
.....
.....
.....

(Konkret ergriffene Maßnahmen ausführlich beschreiben)

2. Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (z. B.: Protokollierung, Dokumentenmanagement)

.....
.....
.....
.....
.....

(Konkret ergriffene Maßnahmen ausführlich beschreiben)

3. Verfügbarkeit und Belastbarkeit

a) Die vom Auftragnehmer konkret ergriffenen technischen und organisatorischen Maßnahmen zur Gewährleistung von Verfügbarkeit und Belastbarkeit werden an folgender Stelle ausführlich beschrieben:

.....
.....

b) Folgende technischen und organisatorischen Maßnahmen werden vom Auftragnehmer zur Gewährleistung von Verfügbarkeit und Belastbarkeit ergriffen:

1. Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust (z. B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne):

.....
.....
.....
.....
.....

(Konkret ergriffene Maßnahmen ausführlich beschreiben)

2. Rasche Wiederherstellbarkeit

.....
.....
.....
.....
.....

(Konkret ergriffene Maßnahmen ausführlich beschreiben)

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

a) Die vom Auftragnehmer konkret ergriffenen technischen und organisatorischen Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung werden an folgender Stelle ausführlich beschrieben:

.....
.....

b) Folgende technischen und organisatorischen Maßnahmen werden vom Auftragnehmer zur Gewährleistung von Verfügbarkeit und Belastbarkeit ergriffen:

1. Datenschutz-Management

.....
.....
.....
.....
.....
(Konkret ergriffene Maßnahmen ausführlich beschreiben)

2. Incident-Response-Management

.....
.....
.....
.....
.....
(Konkret ergriffene Maßnahmen ausführlich beschreiben)

3. Datenschutzfreundliche Voreinstellungen

.....
.....
.....
.....
.....
(Konkret ergriffene Maßnahmen ausführlich beschreiben)

4. Auftragskontrolle

Keine Auftragsdatenverarbeitung ohne entsprechende Weisung des Auftraggebers (z. B.:
eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des
Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen)
.....
.....
.....
.....
.....
(Konkret ergriffene Maßnahmen ausführlich beschreiben)

Anlage 2 zum AV-Vertrag – Unterauftragsverhältnis beim Auftragnehmer zum Zeitpunkt der Auftragsvergabe (zu § 11/12 Opt. (2))

Name und Anschrift des Unterauftragnehmers	Beschreibung der Teilleistungen	Ort der Leistungserbringung