

Auftragsverarbeitung

Zwischen dem

Universitätsklinikum Würzburg
Anstalt des öffentlichen Rechts
Josef-Schneider-Str.2, 97080 Würzburg
(Verantwortlicher im Sinne der DSGVO, im folgenden Auftraggeber genannt)

und

(Auftragsverarbeiter im Sinne der DSGVO, im folgenden Auftragnehmer genannt)

wird folgendes vereinbart:

Präambel

Dieser Auftragsverarbeitungs-Vertrag (AV-Vertrag) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der Erbringung der in § 1 dargestellten Leistungen ergeben.

Sämtliche in diesem Vertrag beschriebenen Verpflichtungen finden Anwendung auf alle Tätigkeiten, die mit den in § 1 dargestellten Leistungen 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 des Auftrags

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers zur Erbringung folgender Leistungen:

- ☒ (Dienst-)Leistungen gemäß Vertrag vom
- ☐ Einrichtung
- ☒ Wartung und Aktualisierung
- ☒ Support
- ☒ Funktionserweiterung
- ☐ sonstiges:

(2) Die Auftragsverarbeitung umfasst folgende Datenarten / -kategorien

- ☒ Personenstammdaten (z. B. Mitarbeiter, Kooperationspartner, nicht med. Patientendaten)
- ☐ Gesundheitsdaten im Sinne von Art. 4 Nr. 15 DSGVO (Medizinische Patientendaten, Befunde, Diagnosen, ...)
- ☐ genetische Daten (Art. 4 Nr. 13 DSGVO)

- ☐ biometrische Daten (Art. 4 Nr. 14 DSGVO)
 - ☒ 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. Auskunftsteilen, oder aus öffentlichen Verzeichnissen)
 - ☐ sonstige:
- (3) Der Kreis der von der Auftragsverarbeitung Betroffenen umfasst folgende Personenkategorien:
- ☒ Patienten
 - ☐ Angehörige von Patienten
 - ☒ Beschäftigte
 - ☐ Kunden
 - ☒ Lieferanten
 - ☐ Bewerber
 - ☐ Ansprechpartner
 - ☐ sonstige:

§ 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 Art. 4 Ziff. 7 DSGVO).
- (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) 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) Der Vertrag wird mit Unterzeichnung wirksam und läuft auf unbestimmte Zeit. Jede Partei ist berechtigt, den Vertrag mit einer Frist von sechs Wochen zum Ende eines Quartals 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) Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.
- (4) Kündigungen bedürfen zu ihrer Wirksamkeit der Schriftform.

§ 4 Weisungsbefugnis des Auftraggebers

- (1) Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch diesen AV-Vertrag festgelegt und können vom Auftraggeber danach durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).
- (2) 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.

- (3) Die Weisungen des Auftraggebers werden vom Auftraggeber dokumentiert und dem Auftragnehmer unmittelbar nach erfolgter Dokumentation als unterschriebene Kopie zur Verfügung gestellt.
- (4) 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.
- (5) 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 erteilt sowie den Grund, warum keine schriftliche Beauftragung erfolgen konnte.
- (6) Weisungsberechtigte Personen des Auftraggebers sind der Ärztliche und der Kaufmännische Direktor des Auftraggebers, die Leitung des Servicezentrums Medizininformatik sowie von diesen beauftragte Personen.

§ 5 Leistungsort

- (1) Der Auftragnehmer wird die vertraglichen Leistungen in Deutschland erbringen. Etwaige Unterauftragnehmer erbringen die sie betreffenden Leistungen in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) oder in einem Drittland. Erfolgt eine Leistungserbringung durch einen Unterauftragnehmer in einem Drittland, garantiert der Auftragnehmer die Einhaltung der diesbezüglichen Vorgaben der DSGVO und weist dies auf Verlangen nach.
- (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) 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.
- (7) 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.

§ 6 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

(2) Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

(3) 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 DSGVO 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.

(4) Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein aussagekräftiges und aktuelles Datenschutz- und Sicherheitskonzept für diese Auftragsverarbeitung zur Verfügung. Als Vorlage dient Anlage 1.

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

(6) Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

(7) Die Wahrung des Fernmeldegeheimnisses entsprechend § 3 TDDDG muss vom Auftragnehmer gewährleistet werden. Dazu muss der Auftragnehmer alle Mitarbeiter, 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.

(8) Weiterhin sind alle Mitarbeiter des Auftragnehmers bzgl. der Pflichten zur Wahrung von Geschäfts- und Betriebsgeheimnissen des Auftraggebers zu verpflichten und müssen auf § 23 GeschGehG hingewiesen werden.

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

(10) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DS-GVO). Er hat die dazu erforderlichen Angaben nach schriftlicher Anforderung dem Auftraggeber unverzüglich zur Verfügung zu stellen.

(11) Als Datenschutzbeauftragter ist beim Auftragnehmer derzeit

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 DSGVO erfüllt werden. Sofern kein Datenschutzbeauftragter beim Auftragnehmer benannt ist, benennt der Auftragnehmer dem Auftraggeber einen Ansprechpartner.

(12) 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 und 34 DSGVO.

(13) 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. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

(14) 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.

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

(16) 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.

(17) 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 DSGVO liegen.

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

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

§ 7 Fernzugriff zu Wartungs-, Reparatur- und ähnlichen Zwecken

Für die Durchführung von Fernzugriffen zu Wartungs-, Reparatur- und ähnlichen Zwecken (nachfolgend Fernservice) auf automatisierte Verfahren, Datenverarbeitungsanlagen oder sonstige elektronische Geräte (nachfolgend Fernserviceobjekte) oder bei Fernzugriffen für andere Dienstleistungen gelten ergänzend folgende Rechte/Pflichten des Auftraggebers/Auftragnehmers:

(1) Fernservice an Arbeitsplatzsystemen werden erst nach Freigabe durch den jeweiligen Berechtigten / zuständigen Mitarbeiter des Auftraggebers durchgeführt.

(2) Fernservice 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 des Fernservice werden sich Auftraggeber und Auftragnehmer über etwaig notwendige Datensicherheitsmaßnahmen in ihren jeweiligen Verantwortungsbereichen verständigen.
- (5) Der Auftragnehmer hat ein Serviceprotokoll über alle Fernzugriffe einschließlich der Freischaltungen zu führen. Es beinhaltet Datum, Uhrzeit, Dauer, Name Servicemitarbeiter/in, Name beauftragende/r Mitarbeiter/in des Auftraggebers bzw. der beauftragenden Stelle (nachvollziehbare Darstellung der Aktivitäten). Das Serviceprotokoll ist mindestens ein Jahr aufzubewahren. Der Auftraggeber erhält auf Verlangen Einblick bzw. Auszüge. Zu jedem Fernzugriff erfolgt ein Eintrag im Serviceprotokoll.
- (6) Bei Fernservicemaßnahmen ist der Auftraggeber - soweit technisch möglich - berechtigt, diese von einem Kontrollbildschirm aus zu verfolgen und jederzeit abzurechnen.
- (7) Der Auftragnehmer wird von den ihm eingeräumten Zugriffsrechten auf Fernserviceobjekte 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. Eine Nutzung des Fernzugangs durch den Auftragnehmer nach dem Ende dieser Vereinbarung ist unzulässig, auch wenn der Zugang technisch noch nicht gesperrt sein sollte.
- (8) Der Auftragnehmer wird im Rahmen des Fernservices nur in zwingend notwendigen Fällen und nur im unbedingt erforderlichen Ausmaß auf Wirkdaten (Produktions-/Echtdaten), insbesondere Patientendaten, zugreifen. Ist dies erforderlich, wird der Auftragnehmer dies dem Auftraggeber rechtzeitig vorher schriftlich oder in Textform mitteilen. Der Auftragnehmer wird in diesen Fällen mit dem Fernservice erst nach Freigabe durch einen befugten Mitarbeiter des Auftraggebers beginnen.
- (9) Tätigkeiten zur Fehleranalyse, bei denen ein Datenabzug der Wirkdaten erforderlich ist, bedürfen der vorherigen Einwilligung des Auftraggebers; ein Datenabzug von personenbezogenen Patientendaten ist nicht zulässig. Bei Datenabzug der Wirkdaten 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.
- (10) Der Fernservice und 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.
- (11) Der Fernservice hat so zu erfolgen, dass am Fernservice nicht beteiligte Dritte keine Kenntnis von personenbezogenen Daten erhalten können. Dies schließt die Verarbeitung von personenbezogenen Daten in Privatwohnungen oder im öffentlichen Raum grundsätzlich aus. Diese ist nur mit vorheriger Zustimmung des Auftraggebers im Einzelfall gestattet. Eine aufgrund Eilbedürftigkeit erteilte mündliche Zustimmung ist schriftlich oder in Textform zu bestätigen.
- (12) Leistungen, die zu ihrer Durchführung ein Auslösen von Röntgenstrahlung und-/oder die mechanische Bewegung der Fernserviceobjekte erfordern, dürfen nicht über Fernservice erbracht werden.
- (13) Soweit dem Fernservice kein Vertrag zugrunde liegt, in dem die Vergütung für die zu erbringenden Leistungen geregelt ist, richtet sich die Vergütung für die Leistungen, die der Auftragnehmer im Rahmen des Fernservice erbringt, zunächst nach der zuletzt abgestimmten Vergütung. Ist eine solche nicht vereinbart, etwa, weil der Antragsteller erstmals Dienstleistungen dieser Art erbringt, richtet sich die Vergütung nach § 612 BGB unter Berücksichtigung von § 242 BGB.

§ 8 Technisch – organisatorischer Ablauf für den Fernservice

- (1) Für die technische und organisatorische Betreuung des Fernzuganges auf Seiten des Auftraggebers ist das Servicezentrum für Medizin-Informatik (Fernzugang@ukw.de) zuständig.
- (2) Für Mitarbeiter des Auftragnehmers muss grundsätzlich eine persönliche Fernzugangskennung eingerichtet werden. Dazu muss das als **Anlage 3 beigefügte Formular „Antrag auf Zugang zum Kliniknetz für Fernservicezwecke“** vollständig ausgefüllt und unterschrieben werden. Die Aufgaben des Mitarbeiters müssen in dem Antrag spezifiziert werden. Der Auftragnehmer ist verpflichtet, Änderungen durch Übersendung eines aktualisierten Antrages umgehend mitzuteilen.

§ 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 Art. 33 und 34 DSGVO 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 DSGVO 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 Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DSGVO). Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.
- (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) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

§ 11 Berichtigung, Beschränkungen 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

- a. sämtliche im Rahmen des Auftrags in seinen Besitz gelangte Unterlagen oder Datenträger,
 - b. erstellte Verarbeitungsergebnisse,
- 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.

§ 12 Unterauftragnehmer

- (1) Unterauftragnehmer ist ein vom Auftragnehmer beauftragter Leistungserbringer, dessen Dienstleistung und/oder Werk der Auftragnehmer zur Erbringung der in diesem AV-Vertrag beschriebenen Leistungen gegenüber dem Auftraggeber benötigt. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind nur 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-/Transportleistungen, 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 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.
- (3) Die nachfolgenden Regelungen finden sowohl für den Unterauftragnehmer als auch für alle in der Folge eingesetzten weiteren Unterauftragnehmer entsprechende Anwendung.
- (4) 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 Unterauftrag-

nehmern, 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.

(5) 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.

(6) Zum Zeitpunkt des Abschlusses dieser Vereinbarung sind die in der Anlage 2 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.

(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 DSGVO 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.

§ 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 DSGVO 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 DSGVO 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 DSGVO 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 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.

_____, den _____
Ort Datum

_____, den _____
Ort Datum

- Auftraggeber -

- Auftragnehmer -

Anlage 1

Technische und organisatorische Maßnahmen des Auftragnehmers

Hinweis (kann nach vollständiger Angabe der Maßnahmen gelöscht werden): Bitte geben Sie nachfolgend jeweils die getroffenen technischen und organisatorischen Maßnahmen an. Als Unterstützung sind hier bestimmte typische Begriffe als Hilfe und Veranschaulichung angeführt.

Bei einzelnen Maßnahmen kann eine stichwortartige Benennung oder auch nur ein Wort (z.B. „Alarmanlage“) ausreichend sein. Bei anderen Maßnahmen sollte jedoch regelmäßig eine kurze Beschreibung erfolgen, die eine Bewertung durch den Auftraggeber ermöglicht (Beispiel: Im Falle einer Videoüberwachung als Maßnahme der Zutrittskontrolle wäre es erforderlich, zu beschreiben, ob z.B. nur die Eingangstür oder auch andere Gebäudeteile überwacht werden und ob eine Aufzeichnung der Aufnahmen erfolgt). Auch bei einer Maßnahme wie einer „Passwortvergabe“ ist konkret aufzuführen, ob es eine Mindestpasswortlänge und -komplexität gibt und wie Passwortlänge und Komplexität ausgestaltet sind. Außerdem wäre zudem anzugeben, ob die Mindestpasswortlänge und -komplexität technisch erzwungen wird.

1) Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Typische Maßnahmen (nur Stichworte) sind z.B.:

- Alarmanlage
- Absicherung von Gebäudeschächten
- Automatisches Zugangskontrollsystem
- Chipkarten-/Transponder-Schließsystem
- Schließsystem mit Codesperre
- Manuelles Schließsystem
- Biometrische Zugangssperren
- Videoüberwachung der Zugänge
- Lichtschranken / Bewegungsmelder
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Personenkontrolle beim Pförtner / Empfang
- Protokollierung der Besucher
- Sorgfältige Auswahl von Reinigungspersonal
- Sorgfältige Auswahl von Wachpersonal
- Tragepflicht von Berechtigungsausweisen

- ☐ Es sind keine Maßnahmen zur Zutrittskontrolle erforderlich, weil ...
- ☐ Es existieren keine Maßnahmen zur Zutrittskontrolle, weil ...
- ☐ Es existieren folgende Maßnahmen zur Zutrittskontrolle:
 - 1) ...
 - 2) ...
 - 3) ...

2) Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Typische Maßnahmen (nur Stichworte) sind z.B.:

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Authentifikation mit biometrischen Verfahren
- Authentifikation mit Benutzername / Passwort
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Gehäuseverriegelungen
- Einsatz von VPN-Technologie
- Sperren von externen Schnittstellen (USB etc.)
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Personenkontrolle beim Pfortner / Empfang
- Protokollierung der Besucher
- Sorgfältige Auswahl von Reinigungspersonal
- Sorgfältige Auswahl von Wachpersonal
- Tragepflicht von Berechtigungsausweisen
- Einsatz von Intrusion-Detection-Systemen
- Verschlüsselung von mobilen Datenträgern
- Verschlüsselung von Smartphone-Inhalten
- Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
- Einsatz von Anti-Viren-Software
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall

- ☐ Es sind keine Maßnahmen zur Zugangskontrolle erforderlich, weil ...
- ☐ Es existieren keine Maßnahmen zur Zugangskontrolle, weil ...
- ☐ Es existieren folgende Maßnahmen zur Zugangskontrolle:
 - 1) ...
 - 2) ...
 - 3) ...

3) Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Typische Maßnahmen (nur Stichworte) sind z.B.:

- Erstellen eines Berechtigungskonzepts
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Sichere Aufbewahrung von Datenträgern
- physische Löschung von Datenträgern vor Wiederverwendung
- ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- Protokollierung der Vernichtung
- Verschlüsselung von Datenträgern

- ☐ Es sind keine Maßnahmen zur Zugriffskontrolle erforderlich, weil ...
- ☐ Es existieren keine Maßnahmen zur Zugriffskontrolle, weil ...

☐ Es existieren folgende Maßnahmen zur Zugriffskontrolle:

- 1) ...
- 2) ...
- 3) ...

4) Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger 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.

Typische Maßnahmen (nur Stichworte) sind z.B.:

- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- E-Mail-Verschlüsselung
- Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschrufen
- Beim physischen Transport: sichere Transportbehälter/-verpackungen
- Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen

☐ Es sind keine Maßnahmen zur Weitergabekontrolle erforderlich, weil ...

☐ Es existieren keine Maßnahmen zur Weitergabekontrolle, weil ...

☐ Es existieren folgende Maßnahmen zur Weitergabekontrolle:

- 1) ...
- 2) ...
- 3) ...

5) Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Typische Maßnahmen (nur Stichworte) sind z.B.:

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

☐ Es sind keine Maßnahmen zur Eingabekontrolle erforderlich, weil ...

☐ Es existieren keine Maßnahmen zur Eingabekontrolle, weil ...

☐ Es existieren folgende Maßnahmen zur Eingabekontrolle:

- 1) ...
- 2) ...
- 3) ...

▪

6) Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Typische Maßnahmen (nur Stichworte) sind z.B.:

- *Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)*
- *vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen*
- *schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag)*
- *Auftragnehmer hat Datenschutzbeauftragten bestellt*
- *Sicherstellung der Rückgabe/Vernichtung von Daten nach Beendigung des Auftrags*
- *Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart*
- *laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten*
- *Vertragsstrafen bei Verstößen*

- ☐ Es sind keine Maßnahmen zur Auftragskontrolle erforderlich, weil ...
- ☐ Es existieren keine Maßnahmen zur Auftragskontrolle, weil ...
- ☐ Es existieren folgende Maßnahmen zur Auftragskontrolle:
 - 1) ...
 - 2) ...
 - 3) ...

7) Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Typische Maßnahmen (nur Stichworte) sind z.B.:

- *Unterbrechungsfreie Stromversorgung (USV)*
- *Klimaanlage in Serverräumen*
- *Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen*
- *Schutzsteckdosenleisten in Serverräumen*
- *Feuer- und Rauchmeldeanlagen*
- *Feuerlöschgeräte in Serverräumen*
- *Alarmmeldung bei unberechtigten Zutritten zu Serverräumen*
- *Erstellen eines Backup- & Recoverykonzepts*
- *Testen von Datenwiederherstellung*
- *Erstellen eines Notfallplans*
- *Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort*
- *Serverräume nicht unter sanitären Anlagen*
- *In Hochwassergebieten: Serverräume über der Wassergrenze*

- ☐ Es sind keine Maßnahmen zur Verfügbarkeitskontrolle erforderlich, weil ...
- ☐ Es existieren keine Maßnahmen zur Verfügbarkeitskontrolle, weil ...
- ☐ Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle:
 - 1) ...
 - 2) ...
 - 3) ...

8) Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Typische Maßnahmen (nur Stichworte) sind z.B.:

- *physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern*
- *Logische Mandantentrennung (softwareseitig)*
- *Erstellung eines Berechtigungskonzepts*
- *Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden*
- *Versehen der Datensätze mit Zweckattributen/Datenfeldern*

- *Beipseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System*
- *Festlegung von Datenbankrechten*
- *Trennung von Produktiv- und Testsystem*

- ☐ Es sind keine Maßnahmen zur Trennungskontrolle erforderlich, weil ...
- ☐ Es existieren keine Maßnahmen zur Trennungskontrolle, weil ...
- ☐ Es existieren folgende Maßnahmen zur Trennungskontrolle:
 - 1) ...
 - 2) ...
 - 3) ...

Anlage 2

Unterauftragnehmer

Der *Auftragnehmer* nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende Unternehmen:

(Hier sind alle Unternehmen mit Namen, Rechtsform, Kontaktdaten und ladungsfähiger Anschrift vom Auftragnehmer anzugeben)