



## Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

zwischen

**Sana Klinikum Hof**

Eppenreuther Str. 9

95032 Hof

- im Folgenden „**Auftraggeber**“ genannt -

und

[Auftragnehmer], [Adresse]

- im Folgenden „**Auftragnehmer**“ genannt -

Ergänzung zum Vertrag ..... (Hauptvertrag) vom .....

### § 1 Gegenstand und Dauer des Auftrags

(1) Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und Auftragnehmer im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag. Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Beschäftigte des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten verarbeiten. In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU-Datenschutzgrundverordnung (DSGVO) zu verstehen. Demnach ist der Auftragnehmer ein Auftragsverarbeiter i.S.d. Art. 4 Nr. 8 DSGVO und der Auftraggeber der Verantwortliche i.S.d. Art. 4 Nr. 7 DSGVO oder ein Auftragsverarbeiter, der mit in diesem Vertrag beschriebenen Verarbeitungen als Auftragsverarbeiter beauftragt wurde. Sofern der Auftraggeber nicht der Verantwortliche ist, sondern mit der in diesem Vertrag beschriebenen Verarbeitungen als Auftragsverarbeiter beauftragt wurde, nimmt der Auftraggeber die in diesem Vertrag beschriebenen Pflichten des Verantwortlichen wahr.

(2) Dieser Vertrag umfasst die Arbeiten und Dienstleistungen gemäß Anlage 1 Nr. 1. Dabei verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers nach Art. 28 DSGVO.

(3) Die Dauer des Auftrags ist ebenfalls in Anlage 1 Nr. 1 festgelegt. Dieser Vertrag gilt unbeschadet der Angaben in Anlage 1 Nr. 1 so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet. Der Auftraggeber kann diesen 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.



## **§ 2 Konkretisierung des Auftragsinhalts**

(1) Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind in Anlage 1 Nr. 2 beschrieben.

(2) Die Art der verwendeten Daten und die Kategorien der durch die Verarbeitung betroffenen Personen sind in Anlage 1 Nr. 3 beschrieben.

(3) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet grundsätzlich in einem Mitgliedsstaat der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Jede Verlagerung in ein Drittland darf nur erfolgen, wenn der Auftraggeber zugestimmt hat und die besonderen Voraussetzungen der Artt. 44 ff. DSGVO erfüllt sind. Eine mögliche Zustimmung des Auftraggebers ist in Anlage 1 Nr. 4 beschrieben. Liegt eine Zustimmung vor, so ist die Erfüllung der besonderen Voraussetzungen in Anlage 2 Nr. 5 beschrieben. Jede weitere Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers.

## **§ 3 Technische und organisatorische Maßnahmen**

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Die vereinbarten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer zukünftig gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Über wesentliche Änderungen, die durch den Auftragnehmer zu dokumentieren sind, ist der Auftraggeber unverzüglich in Kenntnis zu setzen.

(3) Ob die Verarbeitung von Daten, die diesem Vertrag unterliegen, in Privatwohnungen gestattet ist (Heim- und Telearbeit), ist durch diesen Vertrag (Anlage 1 Nr. 9) festgelegt.

(4) Das festgelegte Sicherheitsniveau ist abhängig vom Schutzbedarf der zu verarbeiteten personenbezogenen Daten. Unter Anlage 1 Nr. 3 ist der Schutzbedarf der personenbezogenen Daten festgelegt. Die Verarbeitung personenbezogener Daten, die diesem Vertrag unterliegen, haben mindestens einen normalen Schutzbedarf. Die sich daraus ergebenden Standard-Anforderungen für die technischen und organisatorischen Maßnahmen (Datenschutzniveau) sollten sich nach etablierten Standards orientieren (z.B. nach BSI IT-Grundschutz). Sollten gemäß Anlage 1 Nr. 3 auch personenbezogene Daten verarbeitet werden, die einem erhöhten Schutzbedarf haben, so wird der Auftragnehmer zusätzliche Maßnahmen umsetzen, die den entsprechenden Anforderungen, ggf. abhängig von den Schutzzielen, genügen. Der Auftragnehmer bestätigt unter Anlage 2 Nr. 6 die Einhaltung des geforderten Datenschutzniveaus.

## **§ 4 Weisungsbefugnis des Auftraggebers**

(1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn er ist nach dem Recht des Mitgliedstaats oder



nach Unionsrecht zu einer Verarbeitung verpflichtet. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Die weisungsberechtigten Personen des Auftraggebers sind in Anlage 1 Nr. 5 und die berechtigten Weisungsempfänger sind in Anlage 2 Nr. 3 benannt.

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(3) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

#### **§ 5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers**

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- a) Ist der Auftragnehmer zur Benennung eines Datenschutzbeauftragten, der die Tätigkeiten gemäß Artt. 38 und 39 DSGVO ausübt, verpflichtet, werden dessen Kontaktdaten dem Auftraggeber zum Zweck der direkten Kontaktaufnahme in Anlage 2 Nr. 1 aufgeführt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber zeitnah mitgeteilt.
- b) Ist der Auftragnehmer nicht zur Benennung eines Datenschutzbeauftragten verpflichtet, wird ein Ansprechpartner beim Auftragnehmer benannt, dessen Kontaktdaten in Anlage 2 Nr. 1 beschrieben sind. Ein Wechsel des Ansprechpartners wird dem Auftraggeber unverzüglich mitgeteilt.
- c) Hat der Auftragnehmer seinen Sitz außerhalb der Union, benennt er einen Vertreter in der Union nach Art. 27 Abs. 1 DSGVO unter Anlage 2 Nr. 2.
- d) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Die Vertraulichkeitspflicht besteht auch nach Beendigung des Auftrages fort. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- e) Werden gemäß Anlage 1 Nr. 7 dieses Vertrages durch den Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers verarbeitet, die gesetzlich geschützte Geheimnisse von Berufsheimnisträgern i.S.d. § 203 StGB sind, gilt die Verpflichtung von „sonst mitwirkenden Personen“ zur Geheimhaltung gemäß § 203 Abs. 4 StGB sowie die Einhaltung des Zeugnisverweigerungsrechts nach §§ 53 und 53a StPO und des Beschlagnahmeverbots nach § 97 StPO. In diesem Fall setzt der Auftragnehmer bei der Durchführung der Arbeiten nur solche Beschäftigte ein, die hinreichend und belastbar zur Geheimhaltung i.S.d. § 203 Abs. 4 Nr. 1 StGB verpflichtet sowie über die Strafbarkeit bei unbefugter Offenbarung dieser Geheimnisse nach § 203 StGB belehrt wurden. Des Weiteren werden diese Beschäftigten darauf hingewiesen, dass ihnen im



Hinblick auf Ihre Tätigkeit für den Berufsgeheimnisträger ein Zeugnisverweigerungsrecht nach § 53a StPO zusteht sowie in diesem Rahmen das Beschlagnahmeverbot nach § 97 StPO zu beachten ist. Über die Ausübung des Rechts dieser Personen, das Zeugnis zu verweigern, entscheiden gemäß § 53a Abs. 1 S. 2 StPO die Berufsgeheimnisträger, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann.

- f) Werden gemäß Anlage 1 Nr. 8 dieses Vertrages Gesundheitsdaten im Auftrag von Leistungserbringern i.S.d. § 393 Abs. 1 SGB V verarbeitet und handelt es sich bei der in diesem Vertrag beschriebenen Auftragsverarbeitung ganz oder teilweise um Verarbeitungen im Wege von Cloud-Computing-Diensten, so sind die Vorgaben nach § 393 SGB V zu beachten und einzuhalten.
- g) Die Umsetzung und Einhaltung aller für diesen Vertrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO (Einzelheiten in Anlage 2 Nr. 6).
- h) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- i) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Vertrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- j) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- k) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.
- l) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 8 dieses Vertrages.
- m) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beaskunften, portieren, berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Soweit vom Leistungsumfang umfasst, sind die Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung sowie Datenportabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.



Dieser Vertrag entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DSGVO.

## **§ 6 Unterauftragsverhältnisse**

(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) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. In Anlage 1 Nr. 6 bestimmt der Auftraggeber, ob eine Unterbeauftragung zulässig ist, oder nicht. Sollte eine Unterbeauftragung zulässig sein, stimmt der Auftraggeber der Beauftragung, der in Anlage 2 Nr. 4 benannten Unterauftragnehmer zu. Die Hinzuziehung oder Ersetzung von Unterauftragnehmern ist zulässig, soweit der Auftraggeber gemäß den Regelungen in der Anlage 1 Nr. 6 zugestimmt oder keinen Einspruch erhoben hat. Die Zustimmung des Auftraggebers erfolgt nur unter der Bedingung einer vertraglichen Vereinbarung zwischen Auftragnehmer und Unterauftragnehmer nach Maßgabe des Art. 28 Abs. 2 bis 4 DSGVO, bzw. dessen Inhalt diesem Vertrag entspricht.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die Einhaltung und Umsetzung der technischen und organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vorab der Verarbeitung personenbezogener Daten und sodann regelmäßig durch den Auftragnehmer kontrolliert. Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung. Der Auftragnehmer stellt ferner sicher, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann.

(4) Erbringt ein Unterauftragnehmer (unter zwingender Berücksichtigung gemäß § 2 Abs. 3 dieses Vertrages) die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(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.

## **§ 7 Rechte und Pflichten des Auftraggebers**

(1) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.



(2) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

(3) Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

(4) Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

(5) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(6) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

#### **§ 8 Kontrollrechte des Auftraggebers**

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Vertrag betreffen, kann in Abstimmung mit dem Auftraggeber z.B. erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

#### **§ 9 Mitteilung bei Verstößen und Unterstützung durch den Auftragnehmer**

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artt. 30, 32 bis 36 DSGVO genannten Pflichten zur Dokumentation von Verarbeitungstätigkeiten, Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

- a) im Zusammenhang mit der beauftragten Verarbeitung das Bereitstellen von Angaben zur Erstellung und Fortschreibung des Verzeichnisses von Verarbeitungstätigkeiten



- b) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
- c) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
- d) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber der betroffenen Person zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
- e) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
- f) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

#### **§ 10 Löschung und Rückgabe von personenbezogenen Daten**

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) 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.

#### **§ 11 Haftung**

(1) Auftraggeber und Auftragnehmer haften nach den gesetzlichen Vorschriften gemäß Art. 82 DSGVO.

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

#### **§ 12 Sonstiges**

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

(2) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(3) Für Nebenabreden ist die Schriftform erforderlich.



(4) Soweit sich aus anderen Vereinbarungen zwischen Auftraggeber und Auftragnehmer anderweitige Abreden zum Schutz personenbezogener Daten ergeben, soll dieser Vertrag zur Auftragsverarbeitung vorrangig gelten, es sei denn die Parteien vereinbaren ausdrücklich etwas anderes.

(4) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

<div></div>	<div></div>
Ort/Datum	Ort/Datum
<div></div>	<div></div>
Auftraggeber	Auftragnehmer

Mitgeltende Anlagen:

Anlage 1: Zusatzangaben vom Auftraggeber zur Auftragsverarbeitung

Anlage 2: Zusatzangaben vom Auftragnehmer zur Auftragsverarbeitung

**Kommentiert [A1]:** Soll die Anlage 2 schon mit dem Angebot eingereicht werden?





## Anlage 1

### Zusatzangaben vom Auftraggeber zur Auftragsverarbeitung

#### 1. Angaben zum Gegenstand und der Dauer des Auftrags

(gemäß § 1 Vertrag zur Auftragsverarbeitung)

☐ Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung/SLA/Vertrag (Teil oder Anlage zum Hauptvertrag)

\_\_\_\_\_ vom \_\_\_\_\_ (im folgenden Leistungsvereinbarung genannt), auf die hier verwiesen wird.

Konkreter Bezug in der Leistungsvereinbarung:

\_\_\_\_\_

☐ Gegenstand des Auftrags ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Dauer der Beauftragung:

☐ Die Dauer (Laufzeit) dieses Vertrags entspricht der Laufzeit der Leistungsvereinbarung.

Konkreter Bezug in der Leistungsvereinbarung: \_\_\_\_\_

☐ Der Vertrag beinhaltet eine einmalige Ausführung.

☐ Die Dauer dieses Vertrags (Laufzeit) ist befristet bis zum \_\_\_\_\_

☐ Der Vertrag wird für unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von \_\_\_\_\_ zum \_\_\_\_\_ gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

#### 2. Art und Zweck der Verarbeitung

(gemäß § 2 Abs. 1 Vertrag zur Auftragsverarbeitung)

☐ Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret in der in Nr. 1 genannten Leistungsvereinbarung beschrieben.

Konkreter Bezug in der Leistungsvereinbarung: \_\_\_\_\_



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

---

---

---

---

---

---

### 3. Kategorien betroffener Personen und Art der Daten

(gemäß § 2 Abs. 2 Vertrag zur Auftragsverarbeitung)

☐ Die Kategorien der durch die Verarbeitung betroffenen Personen sowie die Art der Daten sind in der in Nr. 1 genannten Leistungsvereinbarung konkret beschrieben unter:

Konkreter Bezug in der Leistungsvereinbarung: \_\_\_\_\_

☐ Die Kategorien der durch die Verarbeitung betroffenen Personen und die Art der Daten umfassen (Art der Daten in Abhängigkeit der Kategorien betroffener Personen):

---

---

---

---

☐ Die aufgeführten personenbezogene Daten haben einen normalen Schutzbedarf.

☐ Bei den aufgeführten Daten handelt es sich (teilweise) um personenbezogene Daten mit erhöhten Schutzbedarf (Beschreibung der Kategorien der Art der Daten):

---

---

---

---

Diese Daten haben einen erhöhten Schutzbedarf, insbesondere hinsichtlich folgender Schutzziele:

- ☐ Vertraulichkeit
- ☐ Integrität (inkl. Authentizität)
- ☐ Verfügbarkeit



#### 4. Verlagerung der Verarbeitung in Drittländer (außerhalb EU/EWR) (gemäß § 2 Abs. 3 Vertrag zur Auftragsverarbeitung)

- ☐ Eine Verlagerung der Verarbeitung in ein Drittland ist nicht gestattet.
- ☐ Eine Verlagerung der Verarbeitung in ein Drittland ist gestattet und zwar unter folgenden Bedingungen:
- ☐ Erfüllung der besonderen Voraussetzungen der Artt. 44 ff. DSGVO
  - ☐ Es handelt sich um die Schweiz (Angemessenheitsbeschluss der Kommission)
  - ☐ \_\_\_\_\_

#### 5. Weisungsberechtigte Personen (gemäß § 4 Abs. 1 Vertrag zur Auftragsverarbeitung)

Weisungsberechtigte Personen des Auftraggebers sind:  
(Vorname, Name, Organisationseinheit, Telefon)

---

---

---

#### 6. Unterauftragsverhältnisse (gemäß § 6 Vertrag zur Auftragsverarbeitung)

- ☐ Eine Unterbeauftragung ist unzulässig.
- ☐ Der Auftraggeber stimmt der Beauftragung in Nr. 4 Anlage 2 genannten Unterauftragnehmer unter den Bedingungen gemäß § 6 Abs. 2 des Vertrages zur Auftragsverarbeitung zu.
- ☐ Die Hinzuziehung oder Ersetzung von Unterauftragnehmern ist zulässig, soweit der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich anzeigt und der Auftraggeber dieser Änderung zustimmt.
- ☐ Die Hinzuziehung oder Ersetzung von Unterauftragnehmern ist zulässig, soweit der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich anzeigt, um dem Auftraggeber die Möglichkeit zu geben, gegen diese Änderungen begründet Einspruch zu erheben.
- ☐ Sollte der Auftraggeber diesen Änderungen nicht zustimmen oder Einspruch erheben,

---

---

#### 7. Geheimnisse von Berufsheimnisträgern (gemäß § 5 lit. e Vertrag zur Auftragsverarbeitung)

- ☐ Es werden keine personenbezogenen Daten durch den Auftragnehmer verarbeitet, die gesetzlich geschützte Geheimnisse von Berufsheimnisträgern i.S.d. § 203 StGB sind.



☐ Es werden personenbezogene Daten durch den Auftragnehmer verarbeitet, die gesetzlich geschützte Geheimnisse von Berufsgeheimnisträgern i.S.d. § 203 StGB sind. Die Einhaltung der Regelungen gemäß § 5 lit. e des Vertrages zur Auftragsverarbeitung sind demnach erforderlich und durch den Auftragnehmer zu gewährleisten.

#### **8. Cloud-Einsatz im Gesundheitswesen**

*(gemäß § 5 lit. f Vertrag zur Auftragsverarbeitung)*

☐ Es werden keine Gesundheitsdaten von Leistungserbringern im Rahmen der Auftragsverarbeitung verarbeitet.

☐ Es werden Gesundheitsdaten von Leistungserbringern im Rahmen der Auftragsverarbeitung verarbeitet. Findet diese Verarbeitung ganz oder teilweise im Wege von Cloud-Computing-Diensten i.S.d § 393 SGB V statt, so sind durch den Auftragsverarbeiter die Vorgaben nach § 393 SGB V zu beachten und einzuhalten.

#### **9. Verarbeitung in Privatwohnungen**

*(gemäß § 3 Abs. 3 Vertrag zur Auftragsverarbeitung)*

☐ Die Verarbeitung von Daten, die diesem Vertrag unterliegen, ist in Privatwohnungen gestattet (Heim- und Telearbeit).

☐ Die Verarbeitung von Daten, die diesem Vertrag unterliegen, ist in Privatwohnungen nicht gestattet (Heim- und Telearbeit).



## Anlage 2

### Zusatzangaben vom Auftragnehmer zur Auftragsverarbeitung

#### 1. Datenschutzbeauftragter beim Auftragnehmer

(gemäß § 5 a) und b) Vertrag zur Auftragsverarbeitung)

☐ Datenschutzbeauftragter (Vorname, Name, Organisationseinheit, Telefon, E-Mail):

---

---

---

---

☐ Es besteht keine Pflicht zur Benennung eines Datenschutzbeauftragten. Ansprechpartner beim Auftragnehmer (Vorname, Name, Organisationseinheit, Telefon, E-Mail):

---

---

---

---

#### 2. Auftragnehmer in einem Drittland

(gemäß § 5 c) Vertrag zur Auftragsverarbeitung)

☐ Der Auftragnehmer hat seinen Sitz innerhalb der Europäischen Union (EU).

☐ Der Auftragnehmer hat seinen Sitz außerhalb der Europäischen Union (EU) und benennt folgende Person als Vertreter nach Art. 27 Abs. 1 DSGVO (Vorname, Name, Organisationseinheit, Telefon, E-Mail):

---

---

---

---

#### 3. Weisungsempfänger

(gemäß § 4 Abs. 2 Vertrag zur Auftragsverarbeitung)

Weisungsempfänger beim Auftragnehmer sind (Vorname, Name, Organisationseinheit, Telefon):

---

---



#### 4. Beauftragung von Unterauftragnehmern durch den Auftragnehmer

(gemäß § 6 Vertrag zur Auftragsverarbeitung)

☐ Es werden keine Unterauftragnehmer beauftragt.

☐ Es werden folgende Unterauftragnehmer im Rahmen dieser Auftragsverarbeitung beauftragt (Name des Subunternehmers, Anschrift, Land, Tätigkeit im Rahmen des Unterauftragsverhältnisses):

---

---

---

---

---

☐ Es ist sichergestellt, dass die beauftragten Unterauftragnehmer im Rahmen des Unterauftragsverhältnisses ihrerseits keine weiteren Unterauftragnehmer beauftragen.

☐ Es ist sichergestellt, dass die beauftragten Unterauftragnehmer nur innerhalb der EU / des EWR tätig werden.

☐ Es werden regelmäßig Kontrollen wie folgt bei den Unterauftragnehmern durchgeführt:

---

---

---

#### 5. Verlagerung der Datenverarbeitung in ein Drittland

(gemäß § 2 Abs. 3 Vertrag zur Auftragsverarbeitung)

☐ Es findet keine Verlagerung in ein Drittland statt. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt.

☐ Es findet eine Verlagerung in das Drittland \_\_\_\_\_ statt.

Das angemessene Schutzniveau

☐ ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DSGVO);

☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften (Artt. 46 Abs. 2 lit. b i.V.m. 47 DSGVO);

☐ wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c und d DSGVO);

☐ wird hergestellt durch genehmigte Verhaltensregeln (Artt. 46 Abs. 2 lit. e i.V.m. 40 DSGVO);

☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Artt. 46 Abs. 2 lit. f i.V.m. 42 DSGVO).



☐ wird hergestellt durch sonstige Maßnahmen (Art. 46 Abs 2 lit. a, Abs. 3 litt. a und b DSGVO):

---

---

---

## 6. Technische und organisatorische Maßnahmen

(gemäß § 3 Vertrag zur Auftragsverarbeitung)

☐ Die umgesetzten technischen und organisatorischen Maßnahmen entsprechen den Anforderungen, die einem normalen Schutzbedarf genügen.

☐ Es werden die Basis- und Standard-Anforderungen gemäß BSI IT-Grundschutz erfüllt. (standardisierte Sicherheitsanforderungen)

☐ Die umgesetzten technischen und organisatorischen Maßnahmen entsprechen den Anforderungen, die einem erhöhten Schutzbedarf (z.B. gemäß BSI IT-Grundschutz) in den folgenden Schutzzielen genügen.

☐ Vertraulichkeit

☐ Integrität (inkl. Authentizität)

☐ Verfügbarkeit

☐ Es wird ein Datenschutzkonzept mit den technischen und organisatorischen Maßnahmen als Anlage beigelegt.

☐ Es wurde der Prüfkatalog des Sana Bereichs Informationssicherheit unter Berücksichtigung der Schutzbedarfe ausgefüllt, die Angaben durch den Sana Bereich Informationssicherheit bewertet und die Ergebnisse durch beide Parteien als angemessene Maßnahmen festgelegt. Die Ergebnisse (Anhang aus dem Prüfkatalog) werden als zusätzlicher Anhang dieses Vertrags zur Auftragsverarbeitung Teil des Vertrags.

☐ Es werden folgende beschriebene technische und organisatorische Maßnahmen umgesetzt (wenn kein Datenschutzkonzept vorliegt):

### 1. Pseudonymisierung und Verschlüsselung personenbezogener Daten

---

---

---

---

### 2. Gewährleistung einer kontinuierlichen Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung



---

---

---

---

3. Gewährleistung der Verfügbarkeit personenbezogener Daten und des raschen Zugangs zu Daten im Falle eines physischen oder technischen Zwischenfalls

---

---

---

---

4. Gewährleistung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

---

---

---

---

5. Identifizierung und Authentifizierung von Nutzern

---

---

---

---

6. Schutz personenbezogener Daten bei der Übertragung

---

---

---

---





7. Schutz personenbezogener Daten bei der Speicherung

---

---

---

---

8. Gewährleistung einer physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden

---

---

---

---

9. Beschreibung von Maßnahmen zum Schutz personenbezogener Daten bei der Heim- oder Telearbeit

*(Nicht zu beschreiben, wenn die Heim- und Telearbeit gem. § 3 Abs. 3 Vertrag zur Auftragsverarbeitung i.V.m. Nr. 8 der Anlage 1 untersagt wurde.)*

---

---

---

---

10. Anforderungen an die Ereignisprotokollierung (z.B. bei der Nutzerauthentifizierung oder der Dateneingabe, -veränderung oder -löschung)

---

---

---

---

11. Maßnahmen im Rahmen der Unterstützungspflichten des Auftragnehmers (z.B. bei den Betroffenenrechten)



---

---

---

---

#### 12. Zusätzliche Maßnahmen

Werden weitere Maßnahmen durchgeführt, die nicht den obigen Bereichen zugeordnet werden können, so sind diese hier aufzuführen.

Zusätzliche technische und organisatorische Maßnahmen:

---

---

---

---

☐ Es liegt ein Testat einer unabhängigen Instanz (nach § 8 Abs. 2 und 3 Vertrag zur Auftragsverarbeitung) vor, dass die Umsetzung der Maßnahmen bestätigt. Dieses Testat wird dem Auftraggeber als Anlage zur Verfügung gestellt.