

Vereinbarung gem. Art. 28 DSGVO über die Auftragsverarbeitung personenbezogener Daten

Anlage 5 zum EVB-IT Cloudvertrag Vertrag über die Erstellung eines Gesamtsystems zum Betrieb eines KI-Raumassistenten zur Sturzprävention inkl. Bereitstellung im Rahmen einer Cloud-Infrastruktur

Zwischen

Asklepios Kliniken Langen-Seligenstadt GmbH

Asklepios Str. 1

63500 Seligenstadt

(nachfolgend „Auftraggeber“)

und

[...]

- als Auftragsverarbeiter -

(nachfolgend „Auftragnehmer“)

(Auftraggeber und Auftragnehmer zusammen: „Parteien“)

Präambel

Der Auftragnehmer erbringt auf Grundlage der bestehenden vertraglichen Vereinbarung gemäß Zuschlag für den Auftraggeber Leistungen zur Erstellung eines Gesamtsystems zum Betrieb eines KI-Raumassistenten zur Sturzprävention inkl. Bereitstellung im Rahmen einer Cloud-Infrastruktur Cloudleistungen. In diesem Zusammenhang hat der Auftragnehmer, soweit zur Leistungserbringung im Einzelfall erforderlich, ggf. die Zugriffsmöglichkeit auf personenbezogene Daten (nachfolgend „Hauptvertrag“). Hierbei verarbeitet der Auftragnehmer personenbezogene Daten, für die der Auftraggeber im Sinne der DSGVO bzw. der datenschutzrechtlichen Vorschriften verantwortlich ist.

Mit der vorliegenden Vereinbarung zur Auftragsverarbeitung (nachfolgend „AVV“), sollen die jeweils damit verbundenen datenschutzrechtlichen Verpflichtungen konkret geregelt werden. Diese AVV soll dabei Anlage und Bestandteil des Hauptvertrages sein.

1 Umfang der Beauftragung

- 1.1 Die Regelungen dieser AVV gelten immer dann, sobald der Auftragnehmer im Rahmen seiner hauptvertraglichen Leistungserbringung Zugang/Zugriff zu personenbezogenen Daten (nachfolgend „Daten“) erhält, für die der Auftraggeber im Sinne der datenschutzrechtlichen Vorschriften verantwortlich ist. In diesen Fällen verarbeitet der Auftragnehmer Daten im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber bleibt hierbei Verantwortlicher im datenschutzrechtlichen Sinn. Für die Einhaltung aller datenschutzrechtlicher Vorgaben, insbesondere der DSGVO, aber auch dafür, dass die gesetzlichen Betroffenenansprüche im Zusammenhang mit personenbezogenen Daten eingehalten werden, ist insofern der Auftraggeber verantwortlich.
- 1.2 Die Datenverarbeitung durch den Auftragnehmer erfolgt in der Art, dem Umfang und zu dem Zweck wie in **Appendix 1** zu diesem Vertrag spezifiziert; die Verarbeitung betrifft die darin bezeichneten Arten personenbezogener Daten und Kategorien betroffener Personen. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.
- 1.3 Die Datenverarbeitung durch den Auftragnehmer findet grundsätzlich nur innerhalb Deutschlands oder der Europäischen Union (EU) statt.

2 Verantwortlichkeit des Auftraggebers

- 2.1 Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Daten sowie für die Wahrung der Rechte der Betroffenen im Verhältnis der Parteien zueinander allein verantwortlich.
- 2.2 Dem Auftraggeber obliegt es, dem Auftragnehmer die Daten rechtzeitig zur Leistungserbringung nach dem Hauptvertrag zur Verfügung zu stellen, und er ist verantwortlich für die Qualität der Auftraggeberdaten. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.
- 2.3 Der Auftragnehmer wirkt als Dienstleister an der beruflichen Tätigkeit des Auftraggebers, der einer beruflichen Verschwiegenheitsverpflichtung unterliegt, mit. Er verarbeitet für den Auftraggeber u.a. Daten, die in den Anwendungsbereich von § 203 Strafgesetzbuch (StGB) fallen (im Folgenden „Berufsgeheimnisdaten“) und fällt somit in den Anwendungsbereich des § 203 StGB. Der Auftragnehmer verpflichtet sich, über Berufsgeheimnisdaten Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben unbedingt erforderlich ist.

3 Weisungsbefugnisse des Auftraggebers

- 3.1 Dem Auftraggeber steht hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht gegenüber dem Auftragnehmer zu. Der Auftraggeber kann bei Bedarf in schriftlicher oder einer anderen dokumentierten Form Einzelweisungen erteilen. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

- 3.2 Autorisierte Mitarbeiter des Auftraggebers, die berechtigt sind Weisungen zu erteilen:

Steffen Printz, Pflegedienstleitung, Tel.: +49 (0) 6182 83 – 8204,

E-Mail: s.printz@asklepios.com

Michelle Ullrich, Klinikkoordinatorin, Tel.: +49 6182 83-62872,

E-Mail: mi.ullrich@asklepios.com

Autorisierte Mitarbeiter des Auftragnehmers, die berechtigt sind Weisungen entgegenzunehmen:

Name	Funktion	Telefonnummer	E-Mail:
------	----------	---------------	---------

Name	Funktion	Telefonnummer	E-Mail:
------	----------	---------------	---------

Ergeben sich Veränderungen bei den autorisierten Mitarbeitern, sind die Kontaktdaten zu aktualisieren.

- 3.3 Der Auftragnehmer verarbeitet die Daten entsprechend den Weisungen des Auftraggebers, sofern der Auftragnehmer nicht gesetzlich zu einer anderweitigen Verarbeitung verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung in Textform mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
- 3.4 Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, ist er verpflichtet, den Auftraggeber unverzüglich darauf hinzuweisen. Erfolgt eine entsprechende Mitteilung (z.B. per E-Mail oder über ein Ticketsystem) an den Auftraggeber, ist der Auftragnehmer berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen. Die Parteien stimmen darin überein, dass die alleinige Verantwortung für die weisungsgemäße Verarbeitung der Daten beim Auftraggeber liegt.

4 Anforderung an Personal des Auftragnehmers

- 4.1 Zur Erfüllung seiner Verpflichtungen wird der Auftragnehmer ausschließlich Personen einsetzen, die sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheit unterliegen.
- 4.2 Der Auftragnehmer verpflichtet sich, diejenigen seiner bei ihm beschäftigten Personen, die bestimmungsgemäß mit Berufsgeheimnisdaten des Auftraggebers in Berührung kommen oder bei denen dies nicht auszuschließen ist, zur Vertraulichkeit hinsichtlich der Berufsge-

heimnisdaten zu verpflichten und über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB zu belehren. Eine entsprechende Musterverpflichtungserklärung kann vom Auftraggeber zur Verfügung gestellt werden.

5 Einschaltung von Subunternehmern

- 5.1 Der Auftragnehmer wird Subunternehmer nur mit schriftlicher Zustimmung des Auftraggebers beauftragen. Der Auftraggeber wird seine Zustimmung erteilen, wenn keine berechtigten Interessen des Auftraggebers, insbesondere Gründe in der Person des Subunternehmers oder datenschutzrechtliche Gründe, gegen die Beauftragung des Subunternehmers sprechen.
- 5.2 Der Auftragnehmer wird Unterauftragsverarbeiter als Subunternehmer sodann nur beauftragen, soweit sichergestellt ist, dass diese die Voraussetzungen von Art. 28 DSGVO erfüllen. Er hat sicherzustellen, dass er alle ihm nach diesem Vertrag obliegenden (datenschutzrechtlichen) Pflichten auf den Subunternehmer überträgt. Sofern der Auftraggeber datenschutzrechtliche Gründe darlegen kann, kann er dem künftigen Einsatz von Subunternehmern widersprechen. Der Auftragnehmer wird in einem solchen Fall den betreffenden Subunternehmer nicht einsetzen. Dem Auftraggeber sind im Unterauftragsverarbeitungsvertrag gegenüber dem Subunternehmer unmittelbar sämtliche Kontrollrechte gemäß Ziffer 10 dieses Vertrags einzuräumen (echter Vertrag zugunsten Dritter). Der Auftragnehmer haftet für ein Verschulden eines Subunternehmers wie für eigenes Verschulden.
- 5.3 Zur Prüfung der Zustimmung hat der Auftragnehmer dem Auftraggeber den Entwurf des Unterauftragsverarbeitungsvertrags zwischen ihm und dem weiteren Auftragsverarbeiter ungekürzt in Kopie zur Verfügung zu stellen. Ferner muss der Auftragnehmer dem Auftraggeber schriftlich bestätigen, dass er den weiteren Auftragnehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt hat, er sich von der Einhaltung der beim weiteren Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt hat und dieser Erklärung eine Bestätigung der Ergebnisdokumentation dieser Überprüfung beizufügen.
- 5.4 Der Auftraggeber wird seine Zustimmung erteilen, wenn keine berechtigten Interessen des Auftraggebers, insbesondere Gründe in der Person des Subunternehmers oder datenschutzrechtliche Gründe, gegen die Beauftragung des Subunternehmers sprechen.
- 5.5 Der Zustimmungspflicht unterliegen auch Vertragsverhältnisse, die die Prüfung oder Wartung von Datenverarbeitungsverfahren oder -anlagen durch andere Stellen oder andere Nebenleistungen zum Gegenstand haben, sofern dabei ein Zugriff auf Auftraggeberdaten nicht ausgeschlossen werden kann.
- 5.6 Aktuell setzt der Auftragnehmer die in der **Appendix 2** „Subunternehmer“ aufgeführten Subunternehmer ein. Der Auftragnehmer bestätigt ausdrücklich, dass er die in **Appendix 2** aufgeführten Subunternehmer gemäß den Voraussetzungen von Art. 28 DSGVO verpflichtet hat und sämtliche datenschutzrechtlichen Pflichten aus diesem Vertrag auf die

Subunternehmer übertragen hat. Der Auftraggeber erklärt hiermit ausdrücklich seine Zustimmung zu diesen Subunternehmern.

6 Sicherheit der Verarbeitung (technisch-organisatorische Maßnahmen)

- 6.1 Der Auftragnehmer wird gemäß Art. 32 DSGVO erforderliche, geeignete technische und organisatorische Maßnahmen ergreifen, die unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Datenverarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeberdaten zu gewährleisten.
- 6.2 Die aktuellen technisch organisatorischen Maßnahmen sind in der **Appendix 3** zu dieser AVV dargestellt.
- 6.3 Dem Auftragnehmer ist es nach vorheriger schriftlicher Zustimmung gestattet, adäquate alternative technische und organisatorische Maßnahmen während der Laufzeit des Vertrages umzusetzen, sofern das Sicherheitsniveau der in **Appendix 3** festgelegten Maßnahmen nicht unterschritten wird.
- 6.4 Der Auftragnehmer wird auf Weisung des Auftraggebers darüber hinausgehende wirksame technische und organisatorische Maßnahmen umsetzen, wenn sich die in **Appendix 3** bestimmten Maßnahmen als nicht ausreichend erwiesen haben oder wenn der technische Fortschritt dies erfordert. Der Auftragnehmer hat den Auftraggeber unverzüglich schriftlich zu informieren, wenn er Grund zu der Annahme hat, dass die Maßnahmen gemäß **Appendix 3** nicht (mehr) ausreichend sind oder der technische Fortschritt weitere Maßnahmen erfordert.

7 Betroffenenrechte

- 7.1 Der Auftragnehmer wird den Auftraggeber mit technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte betroffener Personen nachzukommen.
- 7.2 Auskünfte an Dritte oder den Betroffenen wird der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an den Auftragnehmer gerichtete Anfragen werden unverzüglich an den Auftraggeber weitergeleitet.
- 7.3 Der Auftragnehmer wird dem Auftraggeber Informationen über die gespeicherten Daten, die Empfänger von Daten, an die der Auftragnehmer sie auftragsgemäß weitergibt, und den Zweck der Speicherung mitteilen, sofern dem Auftraggeber diese Informationen nicht selbst vorliegen oder er sie sich selbst beschaffen kann.
- 7.4 Der Auftragnehmer wird es dem Auftraggeber ermöglichen, im Rahmen des Zumutbaren und Erforderlichen, Auftraggeberdaten zu berichtigen, zu löschen oder ihre weitere Verarbeitung einzuschränken oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung

oder Einschränkung der weiteren Verarbeitung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.

- 7.5 Der Auftragnehmer stellt sicher, dass er auf Einzelweisung des Auftraggebers den gesamten zu einer betroffenen Person gespeicherten Datensatz in einem vom Auftraggeber im Einzelfall festzulegenden, strukturierten, gängigen und maschinenlesbaren Format an den Auftraggeber übergeben kann.

8 Mitteilungs- und Unterstützungspflichten des Auftragnehmers

- 8.1 Trifft den Auftraggeber eine gesetzliche Melde- oder Benachrichtigungspflicht (insbesondere nach Art. 33, 34 DSGVO), wird der Auftragnehmer den Auftraggeber unverzüglich über etwaige meldepflichtige Ereignisse in seinem Verantwortungsbereich informieren. Der Auftragnehmer wird den Auftraggeber bei der Erfüllung der Melde- und Benachrichtigungspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen unterstützen. Der Auftragnehmer wird insbesondere unverzüglich sämtliche zumutbaren Maßnahmen ergreifen, um die entstandenen Gefährdungen für die Integrität, Verfügbarkeit oder Vertraulichkeit der Auftraggeberdaten zu minimieren und zu beseitigen, die Auftraggeberdaten zu sichern und mögliche nachteilige Folgen für Betroffene zu verhindern oder in ihren Auswirkungen so weit wie möglich zu begrenzen. Der Auftragnehmer wird bei allen Verletzungen des Schutzes personenbezogener Daten dem Auftraggeber zumindest folgende Informationen mitteilen:

- Eine Beschreibung der Art der Verletzung, der Kategorien und ungefähre Anzahl der betroffenen Personen und Datensätze
- Name und Kontaktdaten eines Ansprechpartners für weitere Informationen;
- Eine Beschreibung der wahrscheinlichen Folgen der Verletzung für den Betroffenen;
- Eine Beschreibung der ergriffenen und zu ergreifenden Maßnahmen zur Behebung oder Abmilderung der Verletzung.

- 8.2 In dem Fall, dass der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen ist oder ihm betroffene Personen gegenüber Rechten geltend machen, wird der Auftragnehmer den Auftraggeber im erforderlichen Umfang unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

- 8.3 Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen bei etwa vom Auftraggeber durchzuführenden **Datenschutz-Folgenabschätzungen** und sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DSGVO unterstützen.

- 8.4 Ist der Auftraggeber gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von Auftraggeberdaten zu erteilen oder mit diesen Stellen anderweitig zusammenzuarbeiten, so ist der Auftragnehmer verpflichtet, den Auftraggeber

auf erstes Anfordern bei der Erteilung solcher Auskünfte bzw. der Erfüllung anderweitiger Verpflichtungen zur Zusammenarbeit zu unterstützen.

- 8.5 Sofern der Zugriff auf die Daten, die der Auftraggeber dem Auftragsnehmer zur Datenverarbeitung übermittelt hat, durch Maßnahmen Dritter (z.B. Maßnahmen eines Insolvenzverwalters, Beschlagnahme durch Finanzbehörden, Pfändung, etc.) gefährdet wird, hat der Auftragsnehmer den Auftraggeber unverzüglich hierüber zu benachrichtigen.

9 Datenlöschung

- 9.1 Der Auftragsnehmer wird die Daten nach Beendigung dieses Vertrages löschen, sofern nicht gesetzlich eine Verpflichtung des Auftragsnehmers zur weiteren Speicherung dieser Daten besteht.
- 9.2 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung von Auftraggeberdaten dienen, dürfen durch den Auftragsnehmer auch nach Vertragsende aufbewahrt werden.

10 Nachweise und Überprüfungen

- 10.1 Der Auftragsnehmer wird dem Auftraggeber auf dessen Anforderung alle erforderlichen und beim Auftragsnehmer vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem Vertrag zur Verfügung stellen.
- 10.2 Der Auftraggeber ist berechtigt, den Auftragsnehmer bezüglich der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen, zu überprüfen; einschließlich durch Inspektionen. Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragsnehmer Überprüfungen selbst durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen.
- 10.3 Zur Durchführung von Kontrollen ist der Auftraggeber berechtigt, jederzeit sämtliche Geschäftsräume des Auftragsnehmers zu betreten und dort Vor-Ort-Kontrollen durchzuführen. Soweit möglich, wird der Auftraggeber dem Auftragsnehmer solche Vor-Ort-Kontrollen rechtzeitig vorher ankündigen. Der Auftragsnehmer gewährt dem Auftraggeber sämtliche für die Durchführung der Kontrolle benötigten Zugangs-, Auskunfts- und Einsichtsrechte. Der Auftragsnehmer verpflichtet sich insbesondere, dem Auftraggeber Zugang zu den Datenverarbeitungseinrichtungen, Dateien und anderen Dokumenten zu gewähren, um die Kontrolle und Überprüfung der relevanten Datenverarbeitungseinrichtungen, Dateien und anderer Dokumentationen zu ermöglichen, die mit der Verarbeitung von Auftraggeberdaten im Zusammenhang stehen. Der Auftraggeber nimmt hierbei angemessene Rücksicht auf die Betriebsabläufe und berechtigte Geheimhaltungsinteressen des Auftragsnehmers.
- 10.4 Der Auftragsnehmer ermöglicht solche Überprüfungen und trägt durch alle zweckmäßigen und zumutbaren Maßnahmen zu solchen Überprüfungen bei, unter anderem durch die Bereitstellung aller notwendigen Informationen einschließlich aller Zertifikate, Auditberichte und sonstigen Ergebnisse von Überprüfungen im Hinblick auf die Verarbeitung von Auftraggeberdaten.

- 10.5 Der Auftraggeber hat den Auftragnehmer rechtzeitig über alle mit der Durchführung der Überprüfung zusammenhängenden Umstände zu informieren. Der Auftraggeber darf eine Überprüfung pro Kalenderjahr durchführen. Weitere Überprüfungen erfolgen nach Abstimmung mit dem Auftragnehmer.
- 10.6 Der Auftragsverarbeiter kann die Erfüllung der datenschutzrechtlichen Anforderungen insbesondere durch Nachweise nach Art. 40 DSGVO oder Art. 42 DSGVO belegen. Anerkannt werden insbesondere Zertifizierungen wie ein aktuelles C5- Testat).

11 Vertragsdauer und Kündigung

Die Laufzeit und Kündigung dieses Vertrags richten sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

12 Haftung

- 12.1 Für Schäden des Auftraggebers durch schuldhafte Verstöße des Auftragnehmers gegen diesen Vertrag sowie gegen die ihn unmittelbar treffenden gesetzlichen Datenschutzverpflichtungen haftet der Auftragnehmer entsprechend den gesetzlichen Haftungsregelungen. Etwaige anderweitig zwischen den Parteien vereinbarte Haftungsbegrenzungen (z.B. aus dem Hauptvertrag) finden diesbezüglich keine Anwendung. Soweit Dritte Ansprüche gegen den Auftraggeber geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftragnehmers gegen diesen Vertrag oder gegen eine ihn unmittelbar treffende gesetzliche Datenschutzverpflichtung haben, stellt der Auftragnehmer den Auftraggeber von diesen Ansprüchen auf erstes Anfordern frei.
- 12.2 Der Auftragnehmer trägt die Beweislast dafür, dass etwaige Schäden und Geldbußen nicht auf einem von ihm zu vertretenden Umstand beruhen, soweit die jeweilige Ursache in der Verarbeitung von Auftraggeberdaten in der Zuständigkeitssphäre des Auftragnehmers liegt.

13 Schlussbestimmungen

- 13.1 Die Einrede des Zurückbehaltungsrechts gemäß § 273 BGB wird hinsichtlich der verarbeiteten Daten und der dazugehörigen Datenträger ausgeschlossen.
- 13.2 Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und dabei den Anforderungen des Art. 28 DSGVO genügt.
- 13.3 Nebenabreden bedürfen der Schriftform.

- 13.4 Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Vertrags vor.

Der Vertrag kommt durch Zuschlag zu Stande und wird durch den Auftraggeber nicht unterschrieben.

Datum, Ort, Unterschrift Auftragnehmer

Appendix 1

Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen

Art und Zweck der beabsichtigten Verarbeitung

Gegenstand der Datenverarbeitung ist die Bereitstellung eines Gesamtsystems zum Betrieb eines KI-Raumassistenten zur Sturzprävention inkl. Bereitstellung im Rahmen einer Cloud-Infrastruktur Cloudleistungen durch den Auftragnehmer. In diesem Zusammenhang kann der Auftragnehmer, soweit zur Leistungserbringung im Einzelfall erforderlich, ggf. die Zugriffsmöglichkeit auf personenbezogenen Daten des Auftragnehmers erhalten und diese verarbeiten.

Zweck der Datenverarbeitung ist der Schutz und die Versorgung von Patienten durch Gewährleistung ihrer Privatsphäre, Sicherstellung der jederzeitigen Erreichbarkeit von Pflegepersonal im Notfall, Prävention von Gefahrensituationen (z. B. beim unbeaufsichtigten Verlassen der Einrichtung) sowie effizienter Einsatz personeller Ressourcen zur bestmöglichen Patientenversorgung.

Arten der personenbezogenen Daten

Verarbeitungsgegenstand personenbezogener Daten können danach folgende Datenarten/-kategorien sein:

1. Zugangsdaten / Nutzerverwaltung

- Name, E-Mail, Passwort-Hash, Funktion (Administratoren)
- Geräte-ID + Zimmer-/Standortzuordnung (Gerätezuordnung)
- Name, E-Mail, Rolle, Zugriffsrechte (Nutzungskonten Pflegepersonal, Ärzte)

2. Ereignis- und Alarmdaten

- Gesundheitsdaten Art. 9 Abs. 1 DSGVO:
 - Bei Sturzereignissen: Zeitstempel, Raumnummer, Alarmstatus
 - Bei Hilferuf-Ereignissen: Zeitstempel, Raumnummer, Dauer
 - Bewegungsmuster/-aktivität: Tages- und Nachtaktivität pro Raum, Laufwege
- Mitarbeiterdaten
 - Reaktionszeiten Personal
 - Alarmquittierungen (Nutzer-ID + Zeitstempel)

3. Video-/Bilddaten, Stimmdatei von Betroffenen

Kategorien der betroffenen Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Mitarbeiter des Auftraggebers
- Patienten des Auftraggebers
- ggf. mittelbar Angehörige von Patienten

Appendix 2

Subunternehmer

Für die Datenverarbeitung im Auftrag des Auftraggebers setzt der Auftragnehmer die Leistungen von Dritten ein, die in seinem Auftrag Daten verarbeiten („Subunternehmer“).

Unternehmen	Anschrift	Zweck der Datenver- arbeitung	Ort der Datenverar- beitung

Appendix 3

Technische und organisatorische Maßnahmen des Auftragnehmers

Diese Anlage beschreibt die vom Auftragsverarbeiter ergriffenen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten, die im Rahmen der Auftragsverarbeitung verarbeitet werden.

Ziel ist die Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste.

[Bitte ausfüllen und Maßnahmen darstellen, soweit einschlägig, die Maßnahmen sind nur als Muster eingefügt]

A. Vertraulichkeit

Zutrittskontrolle

Mit welchen Maßnahmen wird der Zutritt zur Datenverarbeitungsanlage gegenüber unberechtigten Dritten gesichert?

- ☐ Gebäude und Zu- und Ausgangssicherung
 - ☐ Alarmanlage
 - ☐ Bewegungsmelder
 - ☐ Einbruchmeldeanlagen (EMA)
 - ☐ Schließanlage
 - ☐ Sicherheitsschlösser
 - ☐ biometrische Zutrittskontrolle
 - ☐ Magnet- oder Chipkarten
 - ☐ Schlüsselkonzept (Schlüsselliste)
 - ☐ Werkschutz/Wachpersonal
 - ☐ Pförtner
 - ☐ elektrische Türöffner
 - ☐ abgesicherte Gebäudeschächte
- ☐ Videoüberwachungsanlage
- ☐ funktions- und rollenbasierte Zutrittsberechtigung
- ☐ unterteilte Bereiche in verschiedene Sicherheitszonen
- ☐ Firmenausweis
- ☐ Besucherregelung
 - ☐ Besucherprotokollierung
 - ☐ persönliche Besucherführung
 - ☐ Besucherausweis ☐ Besucherbuch
- ☐ Beaufsichtigung von Fremdpersonal
- ☐ Anwesenheitsaufzeichnungen, in welcher Form: Klicken oder tippen Sie hier, um Text einzugeben.

weitere Maßnahmen: [Klicken oder tippen Sie hier, um Text einzugeben.](#)

Zugangskontrolle

Wie erfolgt der Zugang zur Systembenutzung bzw. zu den personenbezogenen Daten/ wie wird eine unbefugte Systembenutzung verhindert?

- ☐ biometrischen Authentifizierung
- ☐ Zwei-Faktor-Authentifizierung
- ☐ Authentifizierung mit Benutzername und Passwort
 - ☐ Passwortvergabe
 - ☐ Passwortrichtlinie zur Gewährleistung eines sicheren und vertraulichen Passworts
 - ☐ zeitgesteuerte passwortgeschützte Pausenschaltung
 - ☐ automatische Sperrmechanismen, z.B. Passwortwiederholungssperre nach Fehlversuchen
 - ☐ Verschlüsselung von abgelegten Passwörtern
- ☐ Anti-Viren-Software
- ☐ Anti-Spam-Gateway
- ☐ Hardware-Firewall (IDS/IPS)
- ☐ Software-Firewall
- ☐ Verschlüsselung von Datenträgern und/oder externen Schnittstellen (USB, HDMI etc.)
- ☐ Verschlüsselung von mobilen Endgeräten
- ☐ Virtual Private Networks (VPN)
- ☐ Mobile Device Policy
- ☐ Gerätepasswörter auf „Hardware-Ebene“ (z.B. BIOS, Drucker, etc.)
- ☐ Absicherung WLAN
- ☐ Netzwerksegmentierung
- ☐ Richtlinien Löschen/Vernichten von Daten
- ☐ Allgemeine Mitarbeiterrichtlinien zum Datenschutz und zur IT-Sicherheit (z. B. manuelle Desktopsperre, „Clean Desk“, ... gesunder Menschenverstand)

weitere Maßnahmen: [Klicken oder tippen Sie hier, um Text einzugeben.](#)

Zugriffskontrolle

Wie wird der Zugriff auf die Daten geschützt, so dass kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems möglich ist?

- ☐ Begrenzung der Administratoren auf das erforderliche Minimum
- ☐ Funktions- und rollenbasiertes Berechtigungskonzept
 - ☐ Leseberechtigung
 - ☐ Schreibberechtigung
 - ☐ Regelung zur Rechtegestaltung bei Urlaubsvertretung

- ☐ Verwaltung der Zugriffsberechtigung unter Beachtung der Funktionstrennung und des 4-Augenprinzips
- ☐ bedarfsgerechte Zugriffsrechte
- ☐ Protokollierung von Zugriffen
- ☐ Maßnahmen zur Speicherbegrenzung
- ☐ Protokollierte Datenvernichtung
 - ☐ ordnungsgemäße Vernichtung von Datenträgern (DIN 66399);
 - ☐ ordnungsgemäße Vernichtung von Papier (DIN 66399 – 2)
 - ☐ Richtlinie zum Homeoffice/Telearbeit

weitere Maßnahmen: [Klicken oder tippen Sie hier, um Text einzugeben.](#)

Trennungskontrolle

Gewährleisten Sie, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden getrennt verarbeitet werden?

- ☐ Festlegung von Datenbankrechten
- ☐ Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☐ Logische Mandantentrennung
- ☐ Trennung von Produktiv- und Testsystem

weitere Maßnahmen: [Klicken oder tippen Sie hier, um Text einzugeben.](#)

☐ **Pseudonymisierung**¹ (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO), d.h. die Verarbeitung personenbezogener Daten erfolgt 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.

- ☐ Auswahl eines Verfahrens zur Pseudonymisierung;
- ☐ interne Anweisung, dass personenbezogene Daten bei Weitergabe zu pseudonymisieren oder nach Ablauf der Löschfrist zu anonymisieren sind

weitere Maßnahmen: [Klicken oder tippen Sie hier, um Text einzugeben.](#)

B. Integrität

Weitergabekontrolle

Wie gewährleisten Sie, dass ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei einer elektronischen Übertragung oder einem Transport verhindert wird?

- ☐ Verschlüsselung
 - ☐ Einsatz eines kryptographischen Verfahrens nach dem Stand der Technik
 - ☐ E-Mail- Verschlüsselung
 - ☐ Verschlüsselung von Datenträgern und Laptops/Notebooks
 - ☐ Verschlüsselung von Inhalten auf Smartphones
 - ☐ Verschlüsselung von mobilen Datenträgern (USB-Sticks, DVD etc.)
 - ☐ Verschlüsselung von Passwörtern
- ☐ Datenaustausch über eine gesicherte Downloadplattform, Anbieter: [Klicken oder tippen Sie hier, um Text einzugeben.](#)
- ☐ Virtual Private Networks (VPN)
- ☐ elektronische Signatur
- ☐ Richtlinie zum Homeoffice/Telearbeit
- ☐ Verpflichtung der Mitarbeiter zur Verschwiegenheit
- ☐ Verpflichtung der Mitarbeiter auf das Fernmeldegeheimnis (§ 88 TKG)
- ☐ Verpflichtung der Mitarbeiter auf das Sozialgeheimnis (§ 35 SGB I)

weitere Maßnahmen: [Klicken oder tippen Sie hier, um Text einzugeben.](#)

Eingabekontrolle

Können Sie feststellen, ob und von wem personenbezogene Daten in Ihr Datenverarbeitungssystem eingegeben, verändert oder entfernt worden sind?

- ☐ Protokollierung der Eingabe, Veränderung und Löschung von Daten
- ☐ Funktions- und rollenbasiertes Berechtigungskonzept
 - ☐ Schreibberechtigung
- ☐ Dokumentenmanagement
- ☐ Nachvollziehbarkeit von Eingaben
- ☐ Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) à Benutzeridentifikation
- ☐ Klare Zuständigkeiten für Löschungen

weitere Maßnahmen: [Klicken oder tippen Sie hier, um Text einzugeben.](#)

C. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Gewährleisten Sie den Schutz der Daten gegen mutwillige oder zufällige Zerstörung?

- ☐ Backup-Strategie (online/offline; on-site/off-site) [Bsp. NAS- System: verschlüsseltes Back UP Auslagerung bei einem externen Anbieter]
- ☐ Verschlüsselte Backupdatenträger
- ☐ unterbrechungsfreie Stromversorgung (USV)

- ☐ Virenschutz, eingesetzte(s) System(e): Klicken oder tippen Sie hier, um Text einzugeben.
- ☐ Firewall, eingesetzte(s) System(e): Klicken oder tippen Sie hier, um Text einzugeben.
- ☐ Festplatten im RAID-Verbund
- ☐ Redundantes Netzteil
- ☐ Cluster
- ☐ Verteilte Standorte
- ☐ Überwachung Zustand/Funktionen relevanter Systeme (Monitoring)
- ☐ Regelmäßige Updates / Patchmanagement
- ☐ Meldewege und Notfallpläne (z.B. BSI IT-Grundschutz 100-4²)
- ☐ Feuer- und Rauchmelder
- ☐ Feuerlöschgeräte vor Serverraum
- ☐ Schutzsteckdosenleisten Serverraum

- ☐ Alarmmeldung bei unberechtigtem Zutritt zum Serverraum
- ☐ Überwachung Temperatur und Feuchtigkeit in Serverraum
- ☐ Datenschutztresor

weitere Maßnahmen: Klicken oder tippen Sie hier, um Text einzugeben.

Rasche Wiederherstellbarkeit

Setzen Sie Maßnahmen ein, welche die **Verfügbarkeit** der personenbezogenen Daten und den **Zugang** zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen?

- ☐ dokumentiertes Notfallkonzept

weitere Maßnahmen: Klicken oder tippen Sie hier, um Text einzugeben.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Welche Prozesse und Abläufe haben Sie auf organisatorischer Ebene im Unternehmen umgesetzt, um die Sicherheit der Datenverarbeitung zu gewährleisten?

- ☐ Datenschutz-Management
 - ☐ Bestellung eines Datenschutzbeauftragten
 - ☐ Datenschutzteam
 - ☐ Bestellung von Datenschutzkoordinatoren
 - ☐ zentrale Dokumentation aller Verarbeitungstätigkeiten
 - ☐ Richtlinie für Mitarbeiter zum Umgang mit Datenpannen
 - ☐ Richtlinie für Mitarbeiter zum Umgang mit Betroffenenrechten
 - ☐ Schulungskonzept zum Datenschutz
- ☐ IT-Sicherheitsbeauftragter

☐ Datenschutzinformationen gemäß Art 13, 14 DSGVO (Datenschutzerklärung),

☐ Zertifizierung

☐ Unterstützung bei Reaktionen auf Sicherheitsverletzungen

☐ Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);

z.B. keine vorangeklickten Checkboxen in Onlineformularen

☐ Auftragskontrolle, d.h.

Keine Auftragsdatenverarbeitung im Sinne von Art. 28, 29 DS-GVO ohne entsprechende Weisung des Auftraggebers

☐ eindeutige Vertragsgestaltung

☐ formalisiertes Auftragsmanagement

☐ strenge Auswahl des Dienstleisters

☐ Vorabüberzeugungspflicht, z.B. durch Zertifikate

☐ Nachkontrollen

weitere Maßnahmen: [Klicken oder tippen Sie hier, um Text einzugeben.](#)