

Verbindliche Hinweise zur Bearbeitung des Formblatts

Den Vergabeunterlagen ist diese Auftragsverarbeitungsvereinbarung zur Information beigelegt. Er wird erst nach Zuschlag ausgefüllt, der Bieter hat mit Angebotsabgabe hier keine Angaben zu machen. Die Inhalte dieses Vertrages sind allerdings, wie auch die anderen Vergabeunterlagen, Vertragsbestandteile bei Zuschlag.

**Auftragsverarbeitungsvereinbarung gemäß Art. 28
Datenschutz-Grundverordnung (DSGVO)
zwischen**

Technische Universität München

als staatliche Einrichtung in Vertretung des Freistaates Bayern,

vertreten durch ihren Präsidenten

Arcisstr. 21

80333 München

hier handelnd:

Hochschulreferat 6 – Gesundheit, Sicherheit, Strahlenschutz

Dr. Andreas Bauer

Walther-Meißner-Straße 1

85748 Garching

- nachstehend auch „Auftraggeber“ genannt -

und

[Name des Auftragnehmers]

[Adresse]

vertreten durch [Name]

- im Folgenden „Auftragnehmer“ genannt –

Präambel

Diese Vereinbarung regelt die Verpflichtungen der Vertragsparteien nach Art. 28 Abs. 3 DSGVO und ergänzt insoweit die Verträge über die arbeitsmedizinische Betreuung an den Standorten Garching, München und Freising - im Folgenden „Auftrag“ genannt. Sie findet Anwendung auf alle Verarbeitungen personenbezogener Daten, die mit dem Auftrag in Zusammenhang stehen und bei denen der Auftragnehmer oder durch den Auftragnehmer beauftragte Dritte personenbezogene Daten für den Auftraggeber verarbeiten.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsvereinbarung

(1) Der Auftraggeber ist die Technische Universität München. Der Gegenstand des Auftrags ergibt sich im Einzelnen aus dem zwischen den Vertragsparteien abgeschlossenen Vertrag über die Betriebsärztliche Betreuung des Standorts Freising-Weihenstephan.

(2) Die Dauer dieser Vereinbarung (Laufzeit) entspricht der Laufzeit des Vertrages.

§ 2 Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von personenbezogenen oder personen-beziehbaren Daten (nachfolgend „Daten“):

Eine Verarbeitung von Daten erfolgt ausschließlich zum Zweck der Gesundheitsvorsorge oder der Arbeitsmedizin für die Mitglieder der TU-München entsprechend Art. 8 (3) BayDSG. Die Datenverarbeitung dient mithin der Abwicklung und Durchführung des Vertrags.

Der Auftragnehmer verpflichtet sich, die ihm im Verlauf der Vertragsanbahnung und -abwicklung oder anlässlich der Zusammenarbeit erhobenen Daten, bekannt gewordenen Geheimnisse oder sonstige ihrer Natur nach schutzwürdigen Angelegenheiten nur zur rechtmäßigen Aufgabenerfüllung im Sinn der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten sowie die Art der Daten und den Kreis der betroffenen Personen nur für vertragliche Zwecke zu verwenden und im Übrigen geheim zu halten. Die Geheimhaltungspflicht gilt über das Vertragsende hinaus.

Der Auftragnehmer verwendet Daten, die ihm im Rahmen der vertraglichen Erfüllung bekannt geworden sind, nur für die in dem Vertrag und dieser Vereinbarung vorgesehenen Zwecke. Kopien oder Duplikate dürfen ohne Wissen und Zustimmung des Auftraggebers nicht erstellt werden.

Auskünfte an Dritte darf der Auftragnehmer, außer in gesetzlich zwingend vorgesehenen Fällen, nicht erteilen.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

(2) Art der Daten:

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Personenstammdaten: Vor- und Nachname/Titel, ggf. Funktion beim Auftraggeber
- Kommunikationsdaten: Telefonnummern; E-Mail-Adressen
- Arbeitsmedizinische Daten: z.B. digitale Probandenakte, Labor- und Diagnosedaten, Berichte und Bescheinigungen
- Systemdaten: z. B. Datenbank-Indizes (enthalten Teile der Personenstammdaten), Zugriffs-Log

(3) Kategorien betroffener Personen:

Durch die Verarbeitung betroffene Personen sind sämtliche Mitglieder der Technischen Universität München, die aufgrund des Arbeitsschutzgesetzes (ArbSchG) in Verbindung mit der Verordnung zur Arbeitsmedizinischen Vorsorge (ArbMedVV) im Rahmen des Vertrags berechtigt oder verpflichtet sind, arbeitsmedizinische Vorsorge in Anspruch zu nehmen.

§ 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/ein Audit des Auftraggeber einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO und Art. 32 BayDSG insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen. Einzelheiten ergeben sich aus dem Anhang 1 „Technische und organisatorische Maßnahmen“ zu dieser Auftragsverarbeitungsvereinbarung.

(3) Die in Anhang 1 zu dieser Auftragsverarbeitungsvereinbarung festgehaltenen vereinbarten technischen und organisatorischen Maßnahmen berücksichtigen zum Zeitpunkt des Abschlusses dieser Vereinbarung den Stand der Technik und unterliegen während der Laufzeit der Vereinbarung dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in Anhang 1 festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind von dem Auftraggeber zu genehmigen und im Anschluss zu dokumentieren.

§ 4 Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer darf die personenbezogenen Daten nur auf dokumentierte Weisung des Auftraggebers verarbeiten (vergl. Art. 28 Abs. 3 S. 2 lit. a DSGVO), sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, zu einer anderweitigen Verarbeitung verpflichtet ist. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Eine „Weisung“ ist jede an den Normadressaten gerichtete Anordnung, die sich auf den Gegenstand und die Art des Umgangs mit Daten und der darauf bezogenen technischen und organisatorischen Maßnahmen bezieht.

(3) Mündlich erteilte Weisungen bestätigt der Auftraggeber schriftlich (mind. Textform).

(4) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Auffassung 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.

§ 5 Berichtigung, Löschung und Einschränkung der Auftragsverarbeitung

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers 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.

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

§ 6 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat einen Datenschutzbeauftragten schriftlich bestellt, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr/Frau [Name, Funktion, Telefon, Email-Adresse] bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

ODER

Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr/Frau [Name, Funktion, Telefon, Email-Adresse] benannt.

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

a) Die Wahrung der Vertraulichkeit bzw. der angemessenen Verschwiegenheitspflicht gemäß Art. 28 Abs. 3 S. 2 lit. b), 29 DS GVO, Art. 32 Abs. 1 BayDSG ist herzustellen. Der Auftragnehmer wird darauf hingewiesen, dass die Verletzung personenbezogener Daten eine Ordnungswidrigkeit oder Straftat nach §§ 41, 42 des Bundesdatenschutzgesetzes (BDSG) bedeuten kann. Er ist verpflichtet, hierüber ebenfalls die von ihm Beschäftigten oder sonst vertraglich Verpflichteten zu belehren. Der Auftragnehmer setzt bei der Durchführung des Auftrags nur Beschäftigte ein, die auf die Vertraulichkeit bzw. Verschwiegenheit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz betraut gemacht wurden. Sie sind über die sich aus dieser Vereinbarung ergebenden besonderen Datenschutzpflichten zu informieren sowie über die bestehende Weisungs- bzw. Zweckbindung zu belehren. Dies ist schriftlich zu dokumentieren und dem Auftraggeber auf Verlangen durch Vorlage der unterzeichneten Vertraulichkeitsverpflichtungserklärungen nachzuweisen.

b) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit c), 32 DSGVO und Art. 32 BayDSG ist zu gewährleisten. Dies insbesondere, damit der Auftraggeber die Rechte der betroffenen Personen nach Kapitel III der DSGVO innerhalb der gesetzlichen Fristen jederzeit erfüllen kann (vergl. Art. 28 Abs. 3 S. 2 lit e DSGVO).

c) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

d) Der Auftragnehmer hat die Pflicht, den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde zu informieren, soweit sie sich auf diesen Auftrag beziehen (vergl. Art. 31, 51 ff. DSGVO). 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 (vgl. Art. 83, 84 DSGVO).

e) 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 (vergl. Art. 28 Abs. 3 S. 2 lit f DSGVO).

f) 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 Person gewährleistet wird.

g) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 3 und 8 dieser Vereinbarung.

h) Der Auftragnehmer hat den bzw. die für die Nutzung der Daten des Auftraggebers im Rahmen dieser Vereinbarung vorgesehenen Standort/Standorte seiner Geschäftsräume bzw. der genutzten Rechenzentren, dem Auftraggeber vor Vertragsschluss schriftlich zu benennen, angefügt als Anhang 2 zu dieser Vereinbarung. Eine Änderung des Standortes/der Standorte, in dem/ in denen Daten des Auftraggebers verarbeitet und/oder genutzt werden, bedarf der schriftlichen Zustimmung des Auftraggebers. Der Auftragnehmer stellt sicher, dass ein Zugriff auf die Daten des Auftraggebers, die an dem/ den in Anhang 2 zur Vereinbarung genannten Standort/Standorten des Auftragnehmers verarbeitet werden, durch Dritte ausgeschlossen ist.

(3) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO sowie Art. 13, 14, 32, 33, 36 BayDSG Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherigen Konsultationen. Hierzu gehören u.a.

a) 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,

b) die Verpflichtung, Verletzungen von Vorschriften zum Schutz personenbezogener Daten unverzüglich an den Auftraggeber zu melden,

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen,

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung sowie

e) die Unterstützung des Auftraggebers bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Personen,

f) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

§ 7 Unterauftragsverhältnisse

(1) Die Einschaltung von Unterauftragnehmern, die für den Auftragnehmer unmittelbar Daten des Auftraggebers nutzen, ist dem Auftragnehmer nur nach schriftlicher Zustimmung des Auftraggebers gestattet. Für die im Angebot des Auftragnehmers benannten Unterauftragnehmer gilt die Zustimmung des Auftraggebers als erteilt.

(2) Der Auftragnehmer ist verpflichtet, eine Liste mit allen Unterauftragnehmern zu führen, deren Einschaltung der Auftraggeber zugestimmt hat. Der Auftragnehmer hat diese Liste fortlaufend zu aktualisieren.

(3) Die Auslagerung auf Unterauftragnehmer oder der Wechsel eines bestehenden Unterauftragnehmers sind zulässig, soweit:

- a) der Auftragnehmer die Auslagerung bzw. den Wechsel auf den Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- b) der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- c) eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

(4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die Einhaltung der Voraussetzungen durch den Unterauftragnehmer wird vom Auftragnehmer regelmäßig überprüft.

(5) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher und weist dies dem Auftraggeber auf dessen Aufforderung hin nach.

(6) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Auftraggebers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

(7) Bezüglich der Unterauftragnehmer sind dem Auftraggeber erforderliche Kontroll- und Überprüfungsrechte entsprechend Ziffer 8 dieser Vereinbarung einzuräumen.

§ 8 Kontrollrechte des Auftraggebers

(1) Der Auftragnehmer räumt dem Auftraggeber Kontrollrechte nach Art. 28 Abs. 3 lit. S. 2 h DSGVO nach Maßgabe dieser Ziffer 8 ein.

(2) Der Auftragnehmer wird dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte geben und die entsprechenden Nachweise verfügbar machen. Hierzu wird der Auftragnehmer dem Auftraggeber alle erforderlichen Informationen, insbesondere gegebenenfalls erstellte Protokolle, zum Nachweis der Einhaltung der Pflichten zur Verfügung stellen.

(3) Aufgrund der Kontrollverpflichtung des Auftraggebers vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann.

(4) Der Auftraggeber kann sich zu Prüfzwecken in den Betriebsstätten des Auftragnehmers zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsdatenverarbeitung einschlägigen Datenschutzgesetze überzeugen.

(5) Der Auftraggeber ist berechtigt, die vorgenannten Kontrollen auch unter Hinzuziehung Dritter durchzuführen (insbesondere solcher, die gegenüber dem Auftraggeber zur Kontrolle berechtigt sind, wie z.B. Auftraggeber des Auftraggebers und Aufsichtsbehörden).

(6) Der Auftragnehmer ist verpflichtet, die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO und Art. 32 BayDSG sowie die

Durchführung der regelmäßig durchgeführten Risikobewertung nachzuweisen. Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann dabei auch durch Vorlage eines aktuellen Testats oder von Berichten unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditor) oder einer geeigneten Zertifizierung gemäß Art. 42 DSGVO durch IT-Sicherheits- oder Datenschutzaudit erbracht werden.

§ 9 Löschung und Rückgabe personenbezogener 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 des Vertrages – 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, sofern keine gesetzlichen Speicherfristen vorliegen. 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.

§ 10 Kündigung

Ergänzend zum Vertrag wird geregelt, dass die Verletzung von gesetzlichen oder vertraglichen Datenschutzbestimmungen durch den Auftragnehmer stets ein wichtiger Grund für den Auftraggeber ist, das im Vertrag vorbehaltene Recht zur außerordentlichen Kündigung auszuüben. In diesem Zusammenhang kann der Auftraggeber den Vertrag aus wichtigem Grunde ohne Einhaltung einer Frist kündigen.

§ 11 Haftung

(1) Die Vertragsparteien haften entsprechend den einschlägigen gesetzlichen Bestimmungen bzw. gegenüber betroffenen Personen gemäß Art. 82 DSGVO.

(2) Im Innenverhältnis haften die Parteien einander nur für ihren Anteil an der haftungsauslösenden Ursache.

§ 12 Anfragen betroffener Personen

Macht eine betroffene Person ihre Rechte gemäß Art. 15 ff. DSGVO gegenüber dem Auftragnehmer geltend, wird dieser die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber auf Basis der Angaben der betroffenen Person möglich ist. Gemäß Nr. 2.4 dieser Vereinbarung unterstützt der Auftragnehmer den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen.

§ 13 Schlussbestimmungen

- (1) Diese Vereinbarung tritt mit Unterzeichnung der Vertragsparteien in Kraft.
- (2) Wenn eine Bestimmung dieser Vereinbarung unwirksam sein oder werden sollte, wird dadurch die Geltung der Vereinbarung im Übrigen nicht berührt. Es gilt dann eine der unwirksamen Bestimmung dem Sinn und der wirtschaftlichen Bedeutung nach möglichst nahekommende andere Bestimmung zwischen den Parteien als vereinbart.
- (2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- (3) Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
- (4) Die Rechtsbeziehungen der Partner unterliegen dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts und unter Ausschluss derjenigen Regeln des deutschen Rechtes, die auf eine andere als die deutsche Rechtsordnung verweisen.
- (5) Als ausschließlicher Gerichtsstand wird München vereinbart.
- (6) Reicht der Regelungsgehalt einzelner Vorschriften dieser Vereinbarung über die Vertragslaufzeit hinaus, bleiben diese Vorschriften insoweit auch nach Ende der Vertragslaufzeit wirksam.
- (7) Die dieser Vereinbarung angefügten Anhänge sind wesentlicher Bestandteil derselben.

Für den Auftraggeber:

Hochschulreferat 6 – Gesundheit, Sicherheit, Strahlenschutz

Garching,

Ort, Datum

[Name]

Für den Auftragnehmer:

Ort, Datum

[Name]

Anhang 1: „Technische und organisatorische Maßnahmen“ gemäß Art. 32 DSGVO und Art. 32 BayDSG

Anhang 2: „Datenschutz- und Verschlüsselungskonzept Vertinex Software“

Anhang 3: „Orte der Datenverarbeitung durch den Auftragnehmer“

Anhang 1 zur Auftragsverarbeitungsvereinbarung – „Technische und organisatorische Maßnahmen“ gemäß Art. 32 DSGVO und Art. 32 BayDSG

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Zutrittskontrolle

Server-seitig: Standard-TOM seitens LRZ.

Client-seitig: Der Auftragnehmer betreibt [Zahl und Art der Endgeräte] im Betriebsarzt-Zimmer am Standort Freising-Weihenstephan. Der Raum ist mittels Transponderschließung vor unbefugtem Zutritt geschützt.

- Zugangskontrolle

Der Zugang zu den Systemen (Login Betriebssystem) ist auf die jeweiligen persönlichen Accounts der Benutzer eingeschränkt. Der Zugang zum MWN erfolgt ausschließlich durch TUM-Zugänge (LAN, WLAN plus VPN); deren Mindest-Passwortstärke, das Verfahren zur Passwortneuvergabe u. ä. wird dabei durch TUM-Online geregelt. Der Zugang zur Datenbank ist durch die Infrastruktur auf die jeweiligen Netzbereiche der in den Betriebsarztbüros aufliegenden Kabel-gebundenen Netzzugänge beschränkt. Ein Zugriff über WLAN (bei mobilem Einsatz mit Laptop) ist nur über ein Instituts-VPN des Leibniz-Rechenzentrums (cust-fw110) möglich. Ein anderweitiger Zugriff aus dem MWN (z. B. eduroam) oder aus öffentlichen Netzwerken ist nicht möglich. Das Programm (Fabiola der Fa. Vertinex) selbst fordert beim Start zur Eingabe eines Benutzernamens und Passwort auf.

- Zugriffskontrolle

Für den Einsatz an der TU-München werden im Programm Fabiola der Fa. Vertinex 5 Rollen konfiguriert:

Systemadministrator: Starten und beenden des Server-Dienstes, Installation von Updates, Auslösen von Datenbank-Dumps – KEIN Zugriff auf die Datenbankinhalte

Programmadministrator: Rechte- und Rollenverwaltung, Zuweisung der Zugriffsrechte (welche Einrichtung wird von welchem Betriebsarzt betreut), Einrichten der Aufbauorganisation, Konfiguration der gesetzlichen Löschfristen – KEIN Zugriff auf die medizinischen Daten.

Betriebsarzt: Voller lesender, schreibender und löschender Zugriff bei den zugewiesenen Einrichtungen – KEIN Zugriff auf andere Einrichtungen, stark eingeschränkter Zugriff auf „versiegelte“ Akten.¹

Weiterbildungsassistent (i. d. R. Facharzt i. A.): Lesender und schreibender Zugriff auf die digitalen Probandenakten – KEIN löschender Zugriff, kein Zugriff auf „versiegelte“ Akten.

Assistenzzugang: Lesender und schreibender Zugriff auf Personenstammdaten, eingeschränkter Zugriff auf die medizinischen Daten.

¹ Unter versiegelten Akten versteht Vertinex Patientenakten, die auch für den lesenden Zugriff gesperrt wurden (z. B. beim Wechsel eines Betriebsarztes) und nur mit schriftlicher Einwilligung des Probanden wiedereröffnet werden dürfen.

- Trennungskontrolle

Eine getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, entfällt, da der Zweck ausschließlich die arbeitsmedizinische Betreuung im Sinne des ArbSchG in Verbindung mit der ArbMedVV ist. Die Trennung zwischen verschiedenen Betriebsärzten wird durch Zugriffsrechte gesteuert (Vergeben vom Programmadministrator). Die Wahrung der ärztlichen Schweigepflicht wird durch den Mechanismus der Aktenversiegelung¹ gewährleistet.

- Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Dokumentationspflichten, die sich aus den verschiedenen gesetzlichen Anforderungen an eine teils sehr langfristige (z. B. Strahlenschutz beruflich exponierter Personen: 30 Jahre, Dokumentation beim Umgang mit Cancerogenen der Kategorien 1A und 1B: 40 Jahre) Aufbewahrung ergeben, schließen eine Pseudonymisierung aus. Die Daten werden elektronisch jedoch ausschließlich in verschlüsselter Form aufbewahrt.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- Weitergabekontrolle

Es werden keine Daten aus dem System an andere Systeme übertragen. Die in Anlage 2 genannten Verfahren zur Datenreplikation (unter mehreren Servern, mit Satelliten²) kommen in der geplanten Umsetzung nicht zum Einsatz.

- Eingabekontrolle

Die Datenbanklogs der Software erlauben es festzustellen, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme gelesen, eingegeben, verändert oder entfernt worden sind.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, sichergestellt durch: Auf den Clients, die z. B. durch Diebstahl verloren gehen könnten, liegen keine Daten. Die Datenträger sind verschlüsselt. Beim Server handelt es sich um einen virtuellen Server (siehe Wiederherstellbarkeit).

- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO).

Der virtuelle Server wird mit Hilfe von Snapshots gesichert. Diese erlauben die schnelle Wiederherstellung eines betriebsfähigen Zustands. Zusätzlich werden die verschlüsselten Datenbanksicherungen außerhalb der virtuellen Maschine gesichert, um im Falle eines vollständigen Ausfalls einen max. 24 Stunden alten Zustand wiederherstellen zu können.

² Unter einem Satelliten versteht Vertinex einen *offline* lauffähigen Client, der einen umfassenden Cache der Daten bereitstellen muss. Die Notwendigkeit dieses Verfahrens soll mit der Anbindung der mobilen Clients über ein Instituts-VPN (siehe TOM „Zugangskontrolle“) vermieden werden.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Updates des Betriebssystems und des Softwareherstellers Vertinex werden nach Veröffentlichung zeitnah installiert. Im Fall des Betriebssystems erfolgt dies durch das LRZ (Managed Server). Liegen Anlässe vor, die einen Austausch des Schlüssels erforderlich machen (Software unterstützt größere Schlüssellänge, Wechsel des medizinischen Dienstleisters, Schlüssel möglicherweise kompromittiert) unterstützt das System ein entschlüsseln der Datenbank mit nachfolgender Verschlüsselung unter Verwendung eines neuen Schlüssels.

Anhang 3 zur Auftragsverarbeitungsvereinbarung – „Orte der Datenverarbeitung durch den Auftragnehmer“

Beschreibung der Orte der Datenverarbeitung durch den Auftragnehmer

- Campus München: Raum 0149, Arcisstraße 21, 80333 München
- Campus Weihenstephan: Raum HU40, Maximus-von-Imhof-Forum 6, 85354 Freising
- Campus Garching: Raum E07, Walther-Meißner-Straße 1, 85748 Garching
- Mobile Einsätze (Laptop) – z. B. am Campus Straubing