Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 DS-GVO

zwischen dem

Universitätsklinikum Frankfurt (Anstalt des öffentlichen Rechts),

vertreten durch den Vorstand

Theodor - Stern - Kai 7

60590 Frankfurt am Main

Ausführende Stellen, Verantwortliche nach Art. 4 DS-GVO

- Verantwortliche - nachstehend Auftraggeber genannt -

---

und dem/der

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

Präambel

Die Parteien sind sich über die Bedeutung des Schutzes des Persönlichkeitsrechts beim Umgang mit personenbezogenen Daten bewusst und ihnen sind die dazu bestehenden rechtlichen, insbesondere datenschutzrechtlichen Vorschriften bekannt. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien, die sich aus bestehenden oder künftigen Verträgen über Lieferungen und Leistungen ergeben, soweit diese eine Verarbeitung von personenbezogenen Daten des Auftraggebers oder seiner Patienten, insbesondere im Sinne der Datenschutzgrundverordnung (DS-GVO), durch den Auftragnehmer zum Gegenstand haben.

Inhalt

Präambel 2

1. Gegenstand und Dauer des Auftrags 3

2. Konkretisierung des Auftragsinhalts 3

3. Technisch-organisatorische Maßnahmen 4

4. Berichtigung, Einschränkung und Löschung von Daten 4

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers 5

6. Unterauftragsverhältnisse 6

7. Kontrollrechte des Auftraggebers 7

8. Mitteilung bei Verstößen des Auftragnehmers 7

9. Weisungsbefugnis des Auftraggebers 8

10. Löschung und Rückgabe von personenbezogenen Daten 8

11. Informationspflichten, Schriftformklausel 8

12. Verpflichtung zur Geheimhaltung von Berufsgeheimnissen (§ 203 StGB) 9

13. Haftung 10

14. Salvatorische Klausel 10

15. Rechtswahl, Gerichtsstand 10

Anlage 1 – Technisch-organisatorische Maßnahmen nach Art. 25 ..... **Error! Bookmark not defined.**

Anlage 2 – Kontaktdaten des Auftragnehmers 17

1. Datenschutzbeauftragte(r) 17

2. Ansprechpartner (wenn kein(e) Datenschutzbeauftragte(r) erforderlich ist) 17

3. ständiger Vertreter gemäß Art. 27 DS-GVO 17

Anlage 3 – Liste der Unterauftragnehmer des Auftragnehmers 18

Anlage 4 – Weisungsberechtigte Personen 19

1. beim Auftraggeber 19

2. beim Auftragnehmer 19

1. Gegenstand und Dauer des Auftrags

- (1) Gegenstand

- Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: ……für das Universitätsklinikum Frankfurt

- (2) Dauer

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist gemäß Hauptbeauftragung gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalts

- Auftragsinhalt ist die Durchführung von: …… für das Universitätsklinikum Frankfurt.

- (1) 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. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

(2) Art der Daten

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

- ☐ Patientendaten / Personenstammdaten
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Adressdaten
- ☐ Gesundheitsdaten
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Interessenten
- ☐ Besucher
- ☐ Bewerber
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☐ .....

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☐ Patienten
- ☐ Spender
- ☐ Interessenten
- ☐ Beschäftigte
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☐ Ansprechpartner
- ☐ Abonnenten
- ☐ .....

3. Technisch-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 Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO 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 DS-GVO zu berücksichtigen [**Anlage 1**].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(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. Der Auftragnehmer unterstützt angesichts der Art der Verarbeitung den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DS-GVO genannten Rechte der betroffenen Person nachzukommen.

(2) 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 Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) ☐ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt.

☐ Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

☐ Als Datenschutzbeauftragte(r) ist beim Auftragnehmer bestellt: [**Anlage 2**].
Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

☐ Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b) ☐ oder: Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird benannt:
[**Anlage 2**].

c) ☐ oder: Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DS-GVO in der Union: **[Anlage 2].**

d) ☐ Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. 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. 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) ☒ Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen ist gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO **[Anlage 1]** sicherzustellen.

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

g) ☒ Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag 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.

h) ☒ 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.

i) ☒ 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.

j) ☒ Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

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 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) wie folgt beauftragen:

☐ Eine Unterbeauftragung ist unzulässig

☒ nach vorheriger ausdrücklicher schriftlicher Zustimmung des Auftraggebers

☐ Der Auftraggeber stimmt der Beauftragung der Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO. [**Anlage 3**]

(3) Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers ist zulässig, soweit der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und der Auftraggeber nicht innerhalb einer Frist von 14 Tagen, gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(4) Die Weitergabe von personenbezogenen Daten des Auftragnehmers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(5) Erbringt der Unterauftragnehmer 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. Eine weitere Auslagerung durch den Unterauftragnehmer

☒ ist nicht gestattet;
☐ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);
☐ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennendem 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 DS-GVO 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 solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch (optional durch Auftragnehmer zu belegen):

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

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artt. 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige 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 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
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer wird Daten des Auftraggebers nur zur Erfüllung der vertraglich vereinbarten Leistungen und nach Weisung des Auftraggebers verarbeiten. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(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 so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Weisungsberechtigte Personen des Auftraggebers sind in der [**Anlage 4]** benannt und sind mit den weisungsberechtigten Personen des Auftragnehmers zu vervollständigen.

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 den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Informationspflichten, Schriftformklausel

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den Daten beim Auftraggeber liegt.

(2) Es gelten ausschließlich diese Bedingungen; Nebenabreden, Änderungen oder Ergänzungen dieser Bedingungen bedürfen für Ihre Wirksamkeit der Schriftform. Dieses gilt auch für die Abbedingung der Schriftformklausel.

12. Verpflichtung zur Geheimhaltung von Berufsgeheimnissen (§ 203 StGB)

(1) Im Rahmen dieses Auftrages werden auch Daten verarbeitet, die unter ein Berufsgeheimnis (im Sinne von § 203 StGB) fallen.
Der Auftragnehmer verpflichtet sich, über Berufsgeheimnisse Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben erforderlich ist.
Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich Personen, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken und unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist, strafbar machen nach § 203 Abs. 4 S. 1 StGB.
Zudem macht sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde.

(2) Der Auftragnehmer stellt sicher, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des Auftraggebers befassten Beschäftigten und andere für den Auftragnehmer tätigen Personen (z.B. Subunternehmer), die damit befasst sind, sich in Textform dazu verpflichtet haben, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren und sie über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB belehrt wurden. Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar macht, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und die mitwirkende Person nicht dafür Sorge getragen hat, dass die weitere mitwirkende Person zur Geheimhaltung verpflichtet wurde

(3) Der Auftragnehmer wird darauf hingewiesen, dass Daten, die er im Auftrag eines Berufsgeheimnisträgers verarbeitet u.U. dem Zeugnisverweigerungsrecht von sogenannten mitwirkenden Personen unterliegt (§ 53a Strafprozessordnung (StPO)). Entsprechend § 53a StPO entscheidet jedoch der Berufsgeheimnisträger über die Ausübung des Schweigerechts. Im Falle einer Befragung wird der Auftragnehmer unter Hinweis auf § 53a StPO dieser widersprechen und unverzüglich den Auftraggeber informieren, der daraufhin bzgl. der Wahrnehmung des Schweigerechts entscheidet.

(4) Der Auftragnehmer wird darauf hingewiesen, dass die sich in seinem Gewahrsam befindenden Geheimnisschutzdaten dem Beschlagnahmeverbot gemäß § 97 Abs. 2 StPO unterliegen. Die Daten dürfen nicht ohne das Einverständnis des Auftraggebers (Berufsgeheimnisträger) herausgegeben werden. Im Falle einer Beschlagnahme wird der Auftragnehmer dieser widersprechen und unverzüglich den Auftraggeber informieren.

13. Haftung

Die Haftung richtet sich nach den allgemeinen Gesetzen insbesondere nach Artikel 82 DS-GVO.

14. Salvatorische Klausel

Sollten einzelne Bestimmungen dieses Vertrages ganz oder teilweise unwirksam oder unanwendbar sein oder werden, oder sollte sich in dem Vertrag eine Lücke befinden, so soll hierdurch die Gültigkeit der übrigen Bestimmungen nicht berührt werden. Anstelle der unwirksamen oder unanwendbaren Bestimmung oder zur Ausfüllung der Lücke soll eine angemessene Regelung treten, die, soweit rechtlich möglich, dem am nächsten kommt, was die Vertragsparteien gewollt haben oder nach dem Sinn und Zweck dieses Vertrages gewollt haben würden, wenn sie den Punkt bedacht hätten.

15. Rechtswahl, Gerichtsstand

Für etwaige Streitigkeiten aus den Verträgen oder damit im Zusammenhang stehenden Rechtsbeziehungen wird Frankfurt als Gerichtsstand vereinbart.

Für den Auftraggeber:	**Für den Auftragnehmer:**
_____	_____
Name, Funktion:	Name, Funktion: *(mindestens ppa.)*
_____	_____
Ort, Datum, Unterschrift:	Ort, Datum, Unterschrift:

Universitätsklinikum Frankfurt

Anlage 1 – Technisch-organisatorische Maßnahmen nach Art. 32 DSGVO

Bereitgestellt durch:

Firma:
Straße, Nr.:
PLZ, Ort:

Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle

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

	Technische Maßnahmen		Organisatorische Maßnahmen
	Alarmanlage		Personenkontrolle beim Pförtner / Empfang
	Absicherung von Gebäudeschächten		Protokollierung der Besucher *(ev. Besucherbuch)*
	Automatisches Zutrittskontrollsystem		Schlüsselregelung / Schlüsselbuch
	Biometrische Zugangssperren		Tragepflicht von Berechtigungsausweisen
	Chipkarten- / Transponder-Schließsystem		Sorgfältige Auswahl von Sicherheitspersonal
	Lichtschranken / Bewegungsmelder		Sorgfältige Auswahl von Reinigungspersonal
	Manuelles Schließsystem		
	Schließsystem mit Codesperre		
	Sicherheitsschlösser		
	Videoüberwachung der Zugänge		

Zugangskontrolle

Verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

	Technische Maßnahmen		Organisatorische Maßnahmen
	Authentifikation mit Benutzernamen + Passwort		Benutzerberechtigungen verwalten
	Authentifikation mit biometrischen Daten		Erstellen von Benutzerprofilen
	Einsatz von Anti-Viren-Software		Passwortvergabe / Passwortregeln
	Einsatz von Firewalls		Richtlinie „sicheres Passwort“
	Einsatz von Mobile Device Management		Richtlinie „clean Desk“
	Einsatz von VPN-Technologie		Richtlinie „Löschen / Vernichten“

	Intrusion Detection Systeme		allg. Richtlinie „Datenschutz und Sicherheit“
	Gehäuseverriegelungen		Mobile Device Policy
	Sperren von externen Schnittstellen *(z.B. USB-Anschlüsse)*		Anleitung „Manuelle Desktopsperre“
	Verschlüsselung von Datenträgern		
	Verschlüsselung von Smartphones		

Zugriffskontrolle

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

	Technische Maßnahmen		Organisatorische Maßnahmen
	Einsatz von Aktenvernichtern		Anzahl der Administratoren auf das »Notwendigste« reduzieren
	Ordnungsgemäße Vernichtung von Datenträgern *(DIN 32757)*		Einsatz von Dienstleistern zur Akten- und Datenvernichtung (nach Möglichkeit mit Zertifikat)
	Physische Löschung von Datenträgern vor deren Wiederverwendung		Erstellen eines Berechtigungskonzepts
	Protokollierung der Vernichtung von Daten		Sichere Aufbewahrung von Datenträgern
	Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten		Verwaltung der Benutzerrechte durch Systemadministratoren

Trennungskontrolle

Gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

	Technische Maßnahmen		Organisatorische Maßnahmen
	Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern		Erstellung eines Berechtigungskonzepts
	Trennung von Produktiv- und Testsystem		Festlegung von Datenbankrechten
	Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden		Logische Mandantentrennung (softwareseitig)
			Versehen der Datensätze mit Zweckattributen/ Datenfeldern

Pseudonymisierung

Verarbeitung personenbezogener Daten in einer Weise, dass diese 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.

	Technische Maßnahmen		Organisatorische Maßnahmen
	Im Falle der Pseudonymisierung: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System *(mögl. verschlüsselt)*		Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren
	Es erfolgt keine Pseudonymisierung		

Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle

Gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und das überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

	Technische Maßnahmen		Organisatorische Maßnahmen
	Einrichtungen von VPN-Tunneln		Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
	E-Mail-Verschlüsselung		Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
	Sichere Transportbehälter/-verpackungen		Sorgfältige Auswahl von Transportpersonal und -fahrzeugen
			Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

Eingabekontrolle

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

	Technische Maßnahmen		Organisatorische Maßnahmen
	Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern		Erstellung eines Berechtigungskonzepts
	Trennung von Produktiv- und Testsystem		Festlegung von Datenbankrechten
	Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden		Logische Mandantentrennung *(softwareseitig)*
			Versehen der Datensätze mit Zweckattributen / Datenfeldern

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle

Gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

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

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

Gewährleisten, dass nach einer Unterbrechung schnellstmöglich der Datenzugriff wiederhergestellt wird.

	Technische Maßnahmen		Organisatorische Maßnahmen
	Spiegelung der Daten auf dem Gelände		Vorhandenes Backup & Recoverykonzept
	Spiegelung der Daten an 2 Orten mit mehr als 10 km Abstand		

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Datenschutz-Management

Gewährleisten, dass die Anforderung der DS-GVO nachprüfbar umgesetzt wurden.

	Technische Maßnahmen		Organisatorische Maßnahmen
	Software-Lösungen für Datenschutz-Management im Einsatz		Interner / externer Datenschutzbeauftragter
	Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter bei Bedarf/Berechtigung (Intranet …)		Regelmäßige Sensibilisierung der Mitarbeiter, mindestens jährlich
	Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt		Mitarbeiter geschult und auf Vertraulichkeit verpflichtet
			Informationspflichten werden eingehalten (Art. 13 und 14 DS-GVO)
			Interne Revision
			Externe Testierung / Prüfung / Zertifizierungen
			DSMS vorhanden

Incident-Response-Management

Gewährleisten, dass nach einer Störung der Auftraggeber eine Information über die Störung erhält, sofern dessen Daten betroffen waren.

	Technische Maßnahmen		Organisatorische Maßnahmen
	Monitoring von Datenzugriffen		Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen
	Alarmsysteme bei Dateneinbruch		Eskalations-Management vorhanden
	Einsatz von Intrusion Detection System (IDS)		Einbindung des DSB / ISB bei Sicherheitsvorfällen / Datenpannen
	Einsatz von Intrusion Prevention System (IPS)		Testierung des Meldeprozesses

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

Gewährleisten, dass nach einer zeitlichen Vorgabe personenbezogene Daten gelöscht werden.

	Technische Maßnahmen		Organisatorische Maßnahmen
	Manuelle Softwareunterstützung		Manuelle Löschung nach gesetzlicher Vorgabe
	Automatische Softwareunterstützung		Manuelle Löschung auf Anforderung
	Eigenentwicklungen		Sonstiges:

Auftragskontrolle

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

	Technische Maßnahmen		Organisatorische Maßnahmen
			Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten *(insbesondere hinsichtlich Datensicherheit)*
			Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
			Schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag) i.S.d. Art. 28 DS-GVO)
			Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
			Verpflichtung der Mitarbeiter des Auftragnehmers auf die Vertraulichkeit und den Datenschutz
			Vertragsstrafen bei Verstößen
			Vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen und entsprechender Dokumentation

			Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
			Auftragnehmer hat Datenschutzbeauftragten bestellt

Sonstige technische oder organisatorische Maßnahmen zum Auftrag

Auftragsbezogene Maßnahmen hier angegeben. (optional oder ergänzend)

Technische Maßnahmen	Organisatorische Maßnahmen

_____ _____

Datum Name in Druckbuchstaben, Funktion, Unterschrift

Anlage 2 – Kontaktdaten des Auftragnehmers

1. Datenschutzbeauftragte(r)

Herr / Frau	
Name, Vorname	
Straße	
PLZ, Ort	
Telefon	
E-Mail-Adresse	

oder

2. Ansprechpartner (wenn kein(e) Datenschutzbeauftragte(r) erforderlich ist)

Herr / Frau	
Name, Vorname	
Straße	
PLZ, Ort	
Telefon	
E-Mail-Adresse	

oder

3. ständiger Vertreter gemäß Art. 27 DS-GVO

Herr / Frau	
Name, Vorname	
Straße	
PLZ, Ort	
Telefon	
E-Mail-Adresse	

Anlage 3 – Liste der Unterauftragnehmer des Auftragnehmers

Alternativ in freier Form zur Verfügung stellen.
Sollten keine Unterauftragnehmer im Einsatz sein, bitte diese Seite entwerten.

Firma Unterauftragnehmer	Anschrift/Land	Leistung

Anlage 4 – Weisungsberechtigte Personen

1. beim Auftraggeber

Als weisungsberechtigte Personen im Sinne dieser Vereinbarung gelten die jeweiligen hauptverantwortlichen Fachbereichsleiter*innen am Universitätsklinikum Frankfurt oder deren stellvertretenden Personen. Das Weisungsrecht beschränkt sich auf die Hauptvereinbarung oder SLA des jeweils verantwortlichen Fachbereichs am Universitätsklinikum Frankfurt im Sinne der DS-GVO mit dem Auftragnehmer.

2. beim Auftragnehmer

Herr / Frau	
Name, Vorname	
Straße	
PLZ, Ort	
Telefon	
E-Mail-Adresse	