**Zusatzvereinbarung zur Auftragsdatenverarbeitung im Auftrag des Auftraggebers**

zwischen

_____

(„**Auftraggeber**“)

und

Brainlab Sales GmbH, Olof-Palme-Str. 9, 81829 München
(„**Auftragnehmer**”, zusammen die „**Parteien**”)

**Präambel**

Diese Vereinbarung findet Anwendung auf die Tätigkeiten des Auftragnehmers in Bezug auf die Installation von Hard- und Software, Wartung, Reparatur, Training, Fernzugriff, Fehlersuche und alle anderen Servicearbeiten für die Produkte des Auftragnehmers, die den Auftraggeber bei der Erbringung von Gesundheitsdienstleistungen unterstützen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit Personenbezogenen Daten des Auftraggebers in Berührung kommen können. Die zugrundeliegende Vereinbarung bezüglich dieser Tätigkeiten oder Dienstleistungen wird im folgenden als Hauptvertrag bezeichnet.

Diese Zusatzvereinbarung wird nach Maßgabe des Hauptvertrages geschlossen und richtet sich nach der Laufzeit des Hauptvertrages.

**1. Definitionen**

In dieser Vereinbarung haben die folgenden Begriffe folgende Bedeutung:

„**Drittland mit angemessenem Datenschutzniveau**“ ist jedes Land außerhalb des EWR, das von der Europäischen Kommission aufgrund seines innerstaatlichen Rechts oder der von ihm eingegangenen internationalen Verpflichtungen anerkannt ist, ein angemessenes Datenschutzniveau zu bieten;

„**DS-GVO**“ ist die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung);

„**Weisung**” ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers.

„**Personenbezogene Daten**”, „**Verantwortlicher**“, „**Auftragsverarbeiter**“, „**Verarbeitung/verarbeiten**“, „**betroffene Person**“, „**technische und organisatorische Maßnahmen**“, „**Aufsichtsbehörde**“ oder „**Verarbeitung im Auftrag eines Verantwortlichen**“ sind nach der DS-GVO auszulegen.

## 2. Gegenstand und Verantwortlichkeit

Der Auftragnehmer verarbeitet Personenbezogene Daten im Auftrag des Auftraggebers. Gegenstand des Auftrags sind Tätigkeiten, die im Hauptvertrag und seinen Anlagen, insbesondere der Leistungsbeschreibung, konkretisiert sind. Der Auftraggeber ist im Rahmen dieser Zusatzvereinbarung für die Einhaltung der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung durch den Auftragnehmer allein verantwortlich.

## 3. Konkretisierung des Auftragsinhalts

3.1 Zweck, Art und Umfang der Erhebung, Verarbeitung und/oder Nutzung Personenbezogener Daten im Rahmen des Auftrags sind im Hauptvertrag konkretisiert, auf den insoweit Bezug genommen wird.

3.2 Die Arten der Kategorien der erhobenen und/oder verwendeten Personenbezogenen Daten sowie die Kategorien der durch den Umgang mit Personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen sind in Anlage 1 und/oder im Hauptvertrag beschrieben, auf den insoweit Bezug genommen wird.

## 4. Weisungsrechte des Auftraggebers

4.1 Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Spezifikation ein Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

4.2 Der Auftragnehmer wird den Auftraggeber informieren, wenn er der Ansicht ist, eine Weisung verstoße gegen datenschutzrechtliche Vorgaben. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wurde.

## 5. Pflichten des Auftragnehmers

5.1 Der Auftragnehmer erhebt, verarbeitet oder nutzt Daten, soweit nicht gesetzlich oder anderweitig zulässig (z.B. Einwilligung der betroffenen Person), grundsätzlich nur im Auftrag des Auftraggebers und unter Beachtung der Weisungen des Auftraggebers, insbesondere aber nicht für eigene Zwecke. Der Auftragnehmer wird von ihm im Auftrag des Auftraggebers verarbeitete Personenbezogene Daten nur nach Weisung des Auftraggebers korrigieren, löschen, berichtigen oder sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen an den Auftraggeber weiterleiten.

5.2 Der Auftragnehmer bleibt berechtigt, in Einzelfällen Daten, die er im Rahmen des Supports erhält, in der Form zu verwenden, dass es dem jeweiligen Mitarbeiter des Auftragnehmers nicht möglich ist, Rückschlüsse auf die Person des Betroffenen (z.B. eines Patienten, Arztes oder Mitarbeiter des Krankenhauses) zu ziehen. Die Nutzung erfolgt zum Zwecke (i) der Erfüllung gesetzlicher Pflichten (z.B. Produktbeobachtungs- und Berichtspflichten) oder (ii) zur Wahrung berechtigter Interessen des Auftragnehmers und des Auftraggebers, insbesondere zur Verbesserung der Qualität und Funktionalität der Produkte des Auftragnehmers durch die Verwendung ausgewählter Support-Daten (z.B. entpersonalisierter CT- oder MRT-Bilder) u.a. zum Test von neuen Produktversionen. Die weiteren, für die Verarbeitung Personenbezogener Daten im Auftrag in dieser Vereinbarung enthaltenen Restriktionen, finden keine Anwendung.

5.3 Die Verarbeitung erfolgt nur auf Weisung des Auftraggebers, es sei denn, der Auftragnehmer ist nach dem Recht der Europäischen Union oder des Mitgliedstaates, dem der Auftragnehmer unterliegt, dazu verpflichtet; in diesem Fall unterrichtet der Auftragnehmer den Auftraggeber vor der Verarbeitung über diese gesetzliche Verpflichtung, es sei denn, dieses Gesetz verbietet solche Informationen aus wichtigen Gründen des öffentlichen Interesses (vgl. Art. 28 Abs. 3 lit. a DS-GVO).

5.4 Sofern nicht durch geltendes Recht oder ein behördliches Ersuchen untersagt, hat der Auftragnehmer den Auftraggeber unverzüglich über alle Ersuchen von staatlichen Stellen, Datenschutzbehörden oder Strafverfolgungsbehörden um Zugang zu oder Beschlagnahme Personenbezogener Daten des Auftraggebers zu unterrichten.

5.5 Vor der Gewährung des Zugriffs auf Personenbezogene Daten wird der Auftragnehmer die mit der Verarbeitung der Personenbezogenen Daten befassten Personen auf das Datengeheimnis und die Vertraulichkeit verpflichten und sie mit den Bestimmungen der für den Auftragnehmer geltenden Datenschutzverpflichtungen vertraut machen. Dazu gehört, falls nötig, auch die Verpflichtung der betroffenen Personen auf ein ggf. bestehendes (abgeleitetes) Berufsgeheimnis (z.B. bei der Verarbeitung von Daten aus Krankenhäusern oder von niedergelassenen Ärzten) oder das Fernmeldegeheimnis, wenn und soweit im Hauptvertrag entsprechende Leistungen vereinbart sind. Soweit berufs- und standesrechtlich erforderlich, wird der Auftraggeber alle erforderlichen Maßnahmen vornehmen und den Auftragnehmer entsprechend informieren und instruieren.

5.6 Soweit gesetzlich vorgeschrieben, ernennt der Auftragnehmer einen Datenschutzbeauftragten und stellt dem Auftraggeber dessen Kontaktdaten während der Laufzeit des Hauptvertrags zur Verfügung.

5.7 Der Auftragnehmer wird den Auftraggeber über Verstöße gegen Weisungen oder Bestimmungen zum Schutz der Personenbezogenen Daten des Auftraggebers durch den Auftragnehmer oder eine vom Auftragnehmer angestellte Person informieren.

Wenn Personenbezogene Daten verloren gegangen sind, unrechtmäßig übertragen oder anderweitig gemäß Art. 33 und 34 der DS-GVO unrechtmäßig Dritten offengelegt wurden, ist der Auftraggeber über diese Vorfälle unverzüglich zu unterrichten. Der Auftragnehmer trifft in Absprache mit dem Auftraggeber geeignete Maßnahmen, um die Daten zu schützen und mögliche nachteilige Folgen für die betroffenen Personen abzumildern.

Außerdem wird der Auftragnehmer den Auftraggeber unverzüglich über schwerwiegende Störungen des normalen Betriebsablaufs und über den Verdacht auf Datenschutzverletzungen oder sonstige Unregelmäßigkeiten bei der Verarbeitung der Personenbezogenen Daten informieren.

Dem Auftragnehmer ist bekannt, dass der Auftraggeber verpflichtet ist, Verletzungen des Schutzes Personenbezogener Daten zu dokumentieren und, falls erforderlich, die Aufsichtsbehörde bzw. die betroffene Person über eine solche Verletzung zu informieren. Falls und soweit es zu solchen Verletzungen gekommen ist, unterstützt der Auftragnehmer den Auftraggeber gemäß Art. 28 Abs. 3 lit. f DS-GVO bei Einhaltung seiner Pflichten in angemessener Weise, damit der Auftraggeber seinen Verpflichtungen fristgerecht nachkommen kann. Der Auftragnehmer wird dem Auftraggeber die Verletzung mitteilen und mindestens folgende Angaben machen, soweit ihm entsprechende Informationen vorliegen:

a) eine Beschreibung der Art der Verletzung des Schutzes Personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes Personenbezogener Daten;

d) eine Beschreibung der von dem Auftraggeber ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes Personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

5.8 Der Auftragnehmer informiert den Auftraggeber unverzüglich über alle Überwachungstätigkeiten und Maßnahmen, die von der Aufsichtsbehörde in Bezug auf die Verarbeitung Personenbezogener Daten des Auftraggebers ergriffen werden.

5.9 Ist der Auftraggeber gemäß den geltenden gesetzlichen Datenschutzbestimmungen verpflichtet, Auskunft über die Erhebung, Verarbeitung oder Nutzung von Daten zu erteilen, so hat der Auftragnehmer dem Auftraggeber alle entsprechenden Informationen zur Verfügung zu stellen.

5.10 Der Auftragnehmer überwacht die Einhaltung der oben genannten Verpflichtungen während der Durchführung der beauftragten Datenverarbeitung.

5.11 Der Auftragnehmer führt ein schriftliches Verzeichnis über alle Kategorien von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 der DS-GVO, die im Auftrag des Auftraggebers erfolgen.

5.12 Gegebenenfalls unterstützt der Auftragnehmer gemäß Art. 28 Abs. 3 lit. f DS-GVO bei der Erstellung einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO und unterstützt, wo zweckdienlich, bei der vorherigen Konsultation der Aufsichtsbehörde nach Art. 36 DS-GVO. Auf Verlangen des Auftraggebers hat der Auftragnehmer ihm die erforderlichen Informationen und Unterlagen zur Verfügung zu stellen. Die zusätzlichen Kosten, die durch diese Leistungen entstehen, sind dem Auftragnehmer zu erstatten.

5.13 Der Auftragnehmer ergreift geeignete Maßnahmen in Bezug auf Datenmissbrauch, Datenverlust und Wiederherstellbarkeit von Daten (z.B. durch Erstellung von Backups gemäß Industriestandard), soweit dies im Hauptvertrag vorgesehen ist.

## 6. Sicherheit der Datenverarbeitung

6.1 Im Rahmen seiner Zuständigkeit richtet der Auftragnehmer seine interne Organisation nach allen geltenden Datenschutz- und Datensicherheitsanforderungen ein. Der Auftragnehmer trifft, pflegt und kontrolliert technische und organisatorische Maßnahmen, um einen angemessenen Schutz der Daten des Auftraggebers vor Missbrauch und Verlust in Übereinstimmung mit den Anforderungen der geltenden Gesetze zu gewährleisten.

6.2 Der Auftragnehmer trifft alle geeigneten technischen und organisatorischen Maßnahmen, die den Anforderungen des Art. 32 DS-GVO entsprechen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und den Auftraggeber dabei zu unterstützen, die Verpflichtungen aus Art. 32 DS-GVO einzuhalten (Art. 28 Abs. 3 lit. c, f DS-GVO).

6.3 In diesem Zusammenhang berücksichtigt der Auftragnehmer den Stand der Technik, die Implementierungskosten und die Art, den Umfang, die Umstände und Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen. Dazu gehören geeignete Maßnahmen, z.B. zur Eingangskontrolle, Benutzerkontrolle, Zugangskontrolle, Übertragungskontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle sowie die Trennung nach Zweck sowie

a) Pseudonymisierung und Verschlüsselung Personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der Personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

6.4 Anlage 2 enthält eine Beschreibung und Spezifikation der erforderlichen technischen und organisatorischen Maßnahmen, die der Auftragnehmer im Rahmen dieser Vereinbarung durchführen wird. Diese können durch weitere Unterlagen ergänzt werden.

6.5 Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt und der Entwicklung. Der Auftragnehmer kann geeignete alternative Maßnahmen ergreifen. Diese dürfen jedoch das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschreiten. Wesentliche Änderungen müssen dokumentiert werden.

6.6 Der Auftragnehmer unterstützt den Auftraggeber gemäß Art. 28 Abs. 3 lit. e DS-GVO durch geeignete technische und organisatorische Maßnahmen, soweit dies möglich und zumutbar ist, zur Erfüllung der Verpflichtung des Auftraggebers gemäß Abschnitt 3 der DS-GVO gegenüber den betroffenen Personen, z.B. bei der Information und dem Auskunftsrecht der betroffenen Personen, Berichtigung und Löschung der Daten, Einschränkung der Verarbeitung oder des Rechts auf Datenübertragbarkeit und Widerspruchsrecht. Die zusätzlichen Kosten, die durch diese Leistungen entstehen, sind dem Auftragnehmer zu erstatten.

## 7 Fern- und Supportzugriff

7.1 Für die Durchführung von Fern- und Supportzugriffen gelten ergänzend folgende Regelungen, wenn und soweit die Verarbeitungsaktivitäten besondere Kategorien Personenbezogener Daten betreffen oder der Auftraggeber einem Berufsgeheimnis unterliegt.

7.2 Fernzugriffe werden, sofern und soweit hierbei ein Zugriff auf Personenbezogene Daten nicht ausgeschlossen werden kann, ausschließlich mit Einwilligung der zuständigen Mitarbeiter des Auftraggebers ausgeführt.

7.3 Die Mitarbeiter des Auftragnehmers verwenden angemessene Identifizierungs- und Verschlüsselungsverfahren.

7.4 Fernzugriffe werden dokumentiert und protokolliert. Der Auftraggeber ist berechtigt, Prüfungs- und Wartungsarbeiten vor, bei und nach Durchführung zu kontrollieren. Dabei hat er die in Abschnitt 9 aufgeführten Bestimmungen zu beachten. Bei Fernzugriffen ist der Auftraggeber - soweit technisch möglich und im Hinblick auf die Art der erbrachten Leistungen realisierbar - berechtigt, diese von einem Kontrollbildschirm aus zu verfolgen und jederzeit abzubrechen.

7.5 Fernzugriffe zu den relevanten Systemen erfolgen nur nach dem Need-to-know-Prinzip.

7.6 Tätigkeiten zur Fehleranalyse, bei denen ein Zugang zu Personenbezogenen Daten erforderlich ist, bedürfen der vorherigen Einwilligung der zuständigen Mitarbeiter des Auftraggebers. Wenn für diese Zwecke Kopien angefertigt werden, wird der Auftragnehmer diese nach Bereinigung des Fehlers so ändern, dass der Auftragnehmer keinen Personenbezug mehr herstellen kann, oder löschen, es sei denn, dass die (unveränderte) Aufbewahrung entsprechender Daten aus anderen Gründen (z.B. Nachweis der vorgenommenen Arbeiten und deren Ordnungsgemäßheit) erforderlich ist. Personenbezogene Daten dürfen nur zum Zweck der Fehleranalyse verwendet werden und dürfen zudem nicht ohne angemessene Verschlüsselung auf mobile Speichermedien (PDAs, USB-Speichersticks oder ähnliche Geräte) kopiert werden. Ziffer 5.2 bleibt hiervon unberührt.

7.7 In Einzelfällen kann es sein, dass Arbeiten zur Fehleranalyse ohne vorherige Einholung einer Einwilligung erfolgen, wenn dies zur Erbringung der vertragsgemäßen Leistungen (insbesondere zum Zweck der Instandsetzung) erforderlich ist. Der Auftraggeber erteilt hiermit eine generelle Einwilligung für entsprechende Handlungen.

7.8 Fernzugriffe sowie sämtliche in diesem Zusammenhang erforderlichen Tätigkeiten, insbesondere Tätigkeiten wie Löschen, Datentransfer oder eine Fehleranalyse, werden unter Berücksichtigung von technischen und organisatorischen Maßnahmen zum Schutz Personenbezogener Daten durchgeführt.

## 8. Rechte und Pflichten des Auftraggebers

8.1 Der Auftraggeber und der Auftragnehmer sind bezüglich der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

8.2 Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung des Auftrages fest. Soweit keine derartigen Festlegungen erfolgen, sind die Daten dem Auftraggeber auszuhändigen oder zu löschen. Soweit auf Grund besonderer Festlegungen die Löschung der Daten erfolgt, ist diese vom Auftragnehmer dem Auftraggeber mit Datumsangabe zu bestätigen. Eine Rückgabe oder Löschung der gespeicherten Daten ist nur möglich, sofern keine gesetzlichen oder regulatorischen Pflichten, denen der Auftragnehmer unterliegt, zur Aufbewahrung bestehen. Ziffer 5.2 bleibt hiervon unberührt.

## 9. Kontrollrechte

9.1 Der Auftragnehmer stellt dem Auftraggeber auf Anfrage Nachweise der Umsetzung technischer und organisatorischer Maßnahmen und der weiteren Verpflichtungen gemäß Art. 28 DS-GVO zur Verfügung.

9.2 Der Auftraggeber kann in Absprache mit dem Auftragnehmer eine Auftragskontrolle durchführen oder Prüfer damit beauftragen, dies vor Beginn der Datenverarbeitung und in zumutbarer Weise während der gesamten Laufzeit des Auftrags zu tun. Der Auftragnehmer kann diesen Aufforderungen jederzeit vor Beginn und während der Laufzeit der Verarbeitung durch entsprechende Selbstauskünfte, aktuelle Bescheinigungen, Berichte oder Auszüge von unabhängigen Stellen (z.B. durch externe Prüfer, interne Audits, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutz- oder Qualitätsprüfer) oder durch eine geeignete Zertifizierung im Rahmen eines IT-Sicherheits- oder Datenschutzaudits nachkommen.

9.3 Sofern der Auftraggeber dem Auftragnehmer darzulegende begründete Zweifel an der von dem Auftragnehmer vorgelegten Selbstauskunft oder Beurteilung hat, ist der Auftraggeber dazu berechtigt, auf eigene Kosten selbst eine angemessene Prüfung in den Geschäftsräumen des Auftragnehmers durchzuführen, um die Einhaltung der technisch-organisatorischen Maßnahmen und der sonstigen Verpflichtungen nach Art. 28 DS-GVO zu überprüfen. Eine entsprechende Prüfung ist mindestens zwei Wochen im Voraus anzukündigen, darf nur während der regulären Geschäftszeiten durchgeführt werden und darf den internen Betrieb nicht stören. Der Auftraggeber hat alle zusätzlichen Kosten zu erstatten, die dem Auftragnehmer durch eine entsprechende Prüfung entstehen.

9.4 Auf schriftliche Anfrage des Auftraggebers hat der Auftragnehmer dem Auftraggeber innerhalb einer angemessenen Frist die für die Prüfung erforderlichen Informationen und Unterlagen zur Verfügung zu stellen.

## 10. Unterauftragnehmer

10.1 Dem Auftragnehmer ist es gestattet, Unterauftragnehmer und andere Unternehmen für die Erfüllung ihrer vertraglichen Verpflichtungen zu beauftragen.

10.2 Der Auftragnehmer stellt durch den Abschluss von Vereinbarungen mit Unterauftragnehmern sicher, dass den Unterauftragnehmern zumindest im Wesentlichen die gleichen Verpflichtungen auferlegt werden, die der Auftragnehmer gemäß dieser Zusatzvereinbarung übernommen hat, bevor dem Unterauftragnehmer der Zugang zu den Personenbezogenen Daten des Auftraggebers während der Ausführung gewährt wird.

Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/EWR und einem Drittland mit angemessenem Datenschutzniveau, sorgt der Auftragnehmer durch geeignete Maßnahmen für die Einhaltung der EU-Datenschutzbestimmungen.

10.3 Auf Nachfrage stellt der Auftragnehmer eine Liste der an den hierunter ausgeführten Datenverarbeitungsaktivitäten beteiligten Unterauftragnehmern zur Verfügung. Der Auftragnehmer unterrichtet den Auftraggeber über alle beabsichtigten Änderungen, die das Hinzufügen oder Ersetzen anderer Unterauftragnehmer betreffen, und gibt ihm damit die Möglichkeit, diesen Änderungen zu widersprechen, wobei der Auftraggeber begründeten Einwand vorzubringen hat. Wenn der Auftraggeber einen neuen Unterauftragnehmer nicht genehmigt, können der Auftraggeber und/oder der Auftragnehmer die von der jeweiligen Verarbeitung betroffenen Dienste, zu der ein Subunternehmer hinzugezogen werden soll, fristlos d.h. ohne Einhaltung einer Kündigungsfrist, und sonstige Pflicht zur Leistung von Schadens- oder Aufwendungsersatz schriftlich kündigen.

10.4 Der Auftraggeber ist berechtigt, die Unterauftragnehmer des Auftragnehmers gemäß Ziffer 9 und nach vorheriger Absprache und Vereinbarung mit dem Auftragnehmer zu prüfen, wobei der Auftraggeber hiermit den Auftragnehmer mit der Prüfung in seinem Namen beauftragt und damit einverstanden ist, dass eine solche Prüfung nur von dem Auftragnehmer durchgeführt werden darf und auch durch Vorlage aktueller Bescheinigungen, Berichte oder Auszüge von unabhängigen Stellen (z.B. externe Prüfer, interne Audits, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutz- oder Qualitätsprüfer) oder durch eine geeignete Zertifizierung im Rahmen eines IT-Sicherheits- oder Datenschutzaudits erfüllt werden kann. Der Auftraggeber hat vor der Weitergabe von entsprechenden Unterlagen und Informationen des Unterauftragsnehmers ggf. eine oder mehrere Geheimhaltungsvereinbarungen mit dem Unterauftragnehmer und/oder dem Auftragnehmer hierzu abzuschließen.

10.5 Die Vorgaben dieser Ziffer 10 gelten nicht, wenn der Auftragnehmer Nebendienstleistungen an Dritte vergibt; diese Nebendienstleistungen umfassen unter anderem Post-, Versand- und Facility-Dienstleistungen.

## 11. Datentransfer außerhalb des EWR

11.1 Die Verarbeitung erfolgt in der Regel in einem Mitgliedstaat der Europäischen Union, in einem Land des Europäischen Wirtschaftsraums oder in einem Drittland mit angemessenem Datenschutzniveau (einschließlich der USA, soweit eine entsprechende Privacy-Shield Zertifizierung vorliegt). Verarbeitungen in einem anderen Land ("**Drittland**") sind zulässig, wenn die geltenden Anforderungen für die internationale Übermittlung Personenbezogener Daten gemäß Art. 44 ff. DS-GVO eingehalten werden.

11.2 Wenn und soweit sich (i) der Auftraggeber und Auftragnehmer innerhalb des Europäischen Wirtschaftsraums ("**EWR**") befinden, während sich der Unterauftragnehmer des Auftragnehmers in einem Drittland befindet, und (ii) der Auftragnehmer Vereinbarungen mit Unterauftragnehmern auf der Grundlage der EU-Standard-Vertragsklauseln für Auftragnehmer ("**SCC**") schließt, ermächtigt der Auftraggeber hiermit den Auftragnehmer, solche Unterauftragsverarbeitungsvereinbarungen mit Unterauftragnehmern, soweit dies dem Auftragnehmer möglich ist, auch im Namen und im Auftrag des Auftraggebers abzuschließen. Auf Verlangen hat der Auftragnehmer den Auftraggeber über das Bestehen und den Stand der unter den vorgenannten Umständen geschlossenen Standardvertragsklauselverträgen sowie die beteiligten Parteien zu informieren. Dabei steht es im Ermessen des Auftragnehmers, ob entsprechende Verträge abgeschlossen werden.

## 12. Haftung

12.1 Der Auftraggeber stellt den Auftragnehmer von jeglichen Ansprüchen Dritter oder anderen Schäden und Verbindlichkeiten frei, die sich aus (i) der Verletzung der Pflichten des

Auftraggebers aus dieser Vereinbarung und/oder anderen Verstößen gegen geltende Datenschutzgesetze, und/oder (ii) Verstößen des Auftragnehmers gegen geltende Datenschutzgesetze, soweit diese auf der Ausführung der Festlegungen dieser Vereinbarung oder sonstigen Weisungen des Auftraggebers beruhen, ergeben. Dies gilt nicht, soweit der Auftraggeber für die haftungsbegründenden Umstände nicht verantwortlich ist. Art. 82 (5) DS-GVO bleibt unberührt.

12.2 Soweit der Hauptvertrag eine Beschränkung oder einen Ausschluss der Haftung oder Freistellungsverpflichtung des Auftragnehmers vorsieht, gelten diese Beschränkungen oder Ausschlüsse auch für Ansprüche, die im Zusammenhang mit dieser Zusatzvereinbarung gegen den Auftragnehmer geltend gemacht werden.

12.3 Die Regelungen zur Haftung oder Freistellung im Hauptvertrag bleiben im Übrigen unberührt.

## 13. Geheimhaltung

Die Parteien verpflichten sich, sämtliche im Rahmen des Vertragsverhältnisses erhaltenen Kenntnisse über Geschäfts- und Betriebsgeheimnisse vertraulich zu behandeln. Dies findet auch über das Ende der Einzelaufträge und/oder der Geschäftsbeziehung hinaus Anwendung.

## 14. Informationspflichten, Schriftformklausel, Rechtswahl

14.1 Sollten die Personenbezogenen 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 Beteiligten darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber liegen.

14.2 Änderungen und Ergänzungen dieser Zusatzvereinbarung bedürfen der Schriftform und eines ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Zusatzvereinbarung handelt. Die Änderung dieser Formanforderung bedarf ihrerseits der Schriftform.

14.3 Diese Zusatzvereinbarung und alle Streitigkeiten im Zusammenhang mit ihrem Zustandekommen und ihrer Durchführung unterliegen ausschließlich dem Recht der Bundesrepublik Deutschland, unter Ausschluss des Wiener Übereinkommens der Vereinten Nationen über den Internationalen Warenkauf vom 11.04.1980. Gerichtsstand für Streitigkeiten zwischen den Parteien im Zusammenhang mit dieser Zusatzvereinbarung ist das Landgericht München I.

| **Für den Auftragnehmer:** | **Für den Auftraggeber:** |
|---|---|
| [*Name*]<br>[*Position*]<br>[*Ort, Datum*] | [*Name]*<br>[*Position*]<br>[*Ort, Datum*] |
| _____ | _____ |

**<u>Anlage 1</u>: Arten von Datenkategorien und Kategorien von betroffenen Personen im Rahmen der Erhebung, Verarbeitung und/oder Nutzung Personenbezogener Daten**

## 1. Arten von erhobenen und/oder genutzten Personenbezogenen Daten

- Personenstammdaten (z.B. Vor- und Nachname, Geburtsdatum, Geschlecht, Patienten-ID)
- Kontaktdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (z.B. vertragliche Beziehung, Interesse an Produkten oder Verträgen)
- Kundenhistorie
- Rechnungs- und Zahlungsdaten (z.B. Bankkontonummer)
- Planungs- und Verwaltungsdaten (z.B. Informationen zur Kundeninfrastruktur)
- Bewertungsdaten (von Dritten, z.B. Bewertungsagenturen, oder von öffentlichen Verzeichnissen)
- Medizinische Informationen und Bilder der Patienten

## 2. Kategorien von Personen, die der Verarbeitung Personenbezogener Daten unterliegen

- Kunden
- Potentielle Kunden
- Abonnenten
- Patienten des Kunden

**<u>Anlage 2</u>: Sicherheit der Datenverarbeitung**

Diese Anlage beschreibt die TOMs und Verfahren, die der Auftragnehmer mindestens einhalten muss, um die Sicherheit der erstellten, erhobenen, empfangenen oder anderweitig erhaltenen Personenbezogenen Daten zu schützen und die laufende Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme und -dienste zu gewährleisten.

## Technische und organisatorische Maßnahmen

## I. Vertraulichkeit, Art. 32 Abs. 1 lit. b) DSGVO

### 1. Zutrittskontrolle

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

- ☒ Definition eines begrenzten zugangsberechtigten Personenkreises
- ☒ Sicherheitsschlösser
- ☒ Manuelles Schließsystem (z.B. abschließbarer Raum, Schrank) – speziell zutreffend bei Heimarbeit
- ☒ Chipkarten-/Transponder-Schließsystem
- ☒ Videoüberwachung der Zugänge

### 2. Zugangskontrolle

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

- ☒ Funktionelle und/oder zeitlich limitierte Vergabe von Benutzerberechtigungen
- ☒ Passwortrichtlinie inkl. Passwortlänge, -vergabe und -wechsel
- ☒ Authentifikation mit Benutzername / Passwort
- ☒ Einsatz von Intrustion-Detection und Intrusion-Prevention-Systemen
- ☒ Einsatz von Anti-Viren-Software
- ☒ Einsatz einer Hardware-Firewall
- ☒ Einsatz von E-Mail-Spam-Filtern
- ☒ Erstellen von Benutzerprofilen
- ☒ Zuordnung von Benutzerprofilen zu IT-Systemen
- ☒ Einsatz von VPN-Technologie
- ☒ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
- ☒ Einsatz einer Software-Firewall
- ☒ Laptop Festplattenverschlüsselung
- ☒ Zusätzliches Loginsystem für verschiedene Anwendungen

## 3. Zugriffskontrolle

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

- ☒ Festlegung der Zugriffsberechtigungen
- ☒ Verwaltung der Rechte durch Systemadministrator
- ☒ Restriktive Vergabe von Administratoren-Berechtigungen
- ☒ Erfordernis Passwortidentifikation
- ☒ physische Löschung von Datenträgern vor Wiederverwendung
- ☒ Sichere Aufbewahrung von Datenträgern
- ☒ Protokollierung von Datenübertragungen
- ☒ Protokollierung von Zugriffen auf verschiedene Anwendungen
- ☒ Sichere Vernichtung von Datenträgern
- ☒ Festgelegte Abläufe zur Genehmigungserteilung, Kontrolle und Entzug von Berechtigungen

## 4. Trennungskontrolle

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

- ☒ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☒ Logische Mandantentrennung (softwareseitig)
- ☒ Erstellung eines Berechtigungskonzepts
- ☒ Trennung von Produktiv- und Testsystem

# II. Pseudonymisierung und Verschlüsselung, Art. 32 Abs. 1 lit. a DSGVO

*Maßnahmen, zur Pseudonymisierung und Verschlüsselung der personenbezogenen Daten (sofern nicht schon unter Ziffer I).*

- ☒ Einsatz von Pseudonymisierungs- und Anonymisierungstechniken u.a. im Bereich R&D
- ☒ Standardmäßige Verschlüsselung besonders sensibler Daten (at rest) in einzelnen Diensten
- ☒ Bestehen von Regelwerken für Verschlüsselung von Daten

## III. Integrität, Art. 32 Abs. 1 lit. b) DSGVO

### 1. Weitergabekontrolle

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

- ☒ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☒ Schulung von Mitarbeitern zum Datenschutz
- ☒ Dokumentation der Empfänger von Daten
- ☒ In einer Richtlinie ist klar geregelt wie zu reagieren ist, wenn Datenträger abhandengekommen ist
- ☒ Laptop Festplattenverschlüsselung

### 2. Eingabekontrolle

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

- ☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- ☒ Protokollierung der Eingabe, Änderung und Löschung von Daten, soweit Systeme dies zulassen

## IV. Verfügbarkeit und Belastbarkeit, Art. 32 Abs. 1 lit b) und c) DSGVO

### 1. Verfügbarkeitskontrolle

*Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind, einschließlich Maßnahmen zur Wiederherstellung bei physischen oder technischen Zwischenfällen.*

- ☒ Unterbrechungsfreie Stromversorgung (USV)
- ☒ Klimakontrolle in Serverräumen
- ☒ Feuer- und Rauchmeldeanlagen
- ☒ Backup- & Recoverykonzept
- ☒ Bestehen eines Notfallplans
- ☒ Einsatz von Firewalls und Virenscannern
- ☒ Patchmanagement
- ☒ Angemessenes Feuerlöschsystem in Serverräumen
- ☒ Testen von Datenwiederherstellung
- ☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

## V. Verfahren zur regelmäßigen Überprüfung und Evaluierung, Art. 32 Abs. 1 lit. d) DSGVO

### 1. Datenschutz Management

*Sonstige Maßnahmen, vor allem organisatorische Maßnahmen zum Schutz personenbezogener Daten.*

- ☒ Beschreibung geltender Datenschutzvorgaben in verbindlichen Richtlinien und Handlungsanweisungen
- ☒ Beschaffung von aktuellen Informationen zur IT-Sicherheit und IT-Schwachstellen
- ☒ Regelmäßige Überprüfungen der Vorkehrungen zum Datenschutz und bestehender Regelwerke
- ☒ Ggf. Einbeziehung des Datenschutzbeauftragten in relevante neue Datenverarbeitungsverfahren

### 2. Incident Response Management

*Sonstige Maßnahmen zum Umgang mit Datenschutzzwischenfällen.*

- ☒ Regelwerk zum Verhalten bei Datenschutz- und IT-Sicherheitsvorfällen
- ☒ Business Continuity Management Prozesse
- ☒ Prozess zur Meldung für auftretende Vorfälle

### 3. Datenschutzfreundliche Voreinstellungen, Art. 25 Abs. 2 DSGVO

*Maßnahmen, die gewährleisten, dass Voreinstellungen den Interessen der Betroffenen gerecht werden (privacy by default).*

- ☒ Umsetzung datenschutzfreundlicher Voreinstellungen
- ☒ Einsatz von Pseudo- oder Anonymisierung personenbezogener Daten u.a. im Bereich R&D
- ☒ Beschränkung der Datenerhebung

### 4. Auftragskontrolle

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

- ☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- ☒ Vorabkontrolle des Auftragsverarbeiter, insbesondere vorherige Prüfung der Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- ☒ dokumentierte Weisungen an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag)
- ☒ Verpflichtung des Auftragsverarbeiters zur Verpflichtung seiner Mitarbeiter auf die Vetraulichkeit von Daten
- ☒ Auftragnehmer hat ggf. Datenschutzbeauftragten bestellt
- ☒ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- ☒ Schulung der Mitarbeiter
- ☒ Verzeichnis der Auftragsverarbeitungstätigkeiten