STANDARDVERTRAGSKLAUSELN

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

1. Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sichergestellt werden.
2. Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.
3. Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.
4. Die Anhänge I bis IV sind Bestandteil der Klauseln.
5. Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 unterliegt.
6. Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 erfüllt werden.

Klausel 2

Unabänderbarkeit der Klauseln

1. Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

2. Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.
3. Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 erfüllt werden.

Klausel 3

Auslegung

1. Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.
2. Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.
3. Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4

Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5

Kopplungsklausel

1. Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.
2. Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.
3. Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

ABSCHNITT II

PFLICHTEN DER PARTEIEN

Klausel 6

Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7

Pflichten der Parteien

7.1 Weisungen

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann

während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

2. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2 Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3 Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

7.4 Sicherheit der Verarbeitung

1. Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.
2. Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen

personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5 Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6 Dokumentation und Einhaltung der Klauseln

1. Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.
2. Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.
3. Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.
4. Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten

oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

5. Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7 Einsatz von Unterauftragsverarbeitern

1. ALLGEMEINE SCHRIFTLICHE GENEHMIGUNG: Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens vier Wochen im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

2. Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 unterliegt.

3. Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

4. Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.
5. Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8 Internationale Datenübermittlungen

1. Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.
2. Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8

Unterstützung des Verantwortlichen

1. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

2. Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

3. Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

   I. Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

   II. Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz- Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

   III. Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

4. Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.

5. Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei

der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9

Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1 Verletzung des Schutzes der vom Verantwortlichen verarbeitenden Daten

1. Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

2. bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

3. bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

    I. die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

II. die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

III. die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

4. Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

5. bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2 Verletzung des Schutzes der vom Auftragsverarbeiter verarbeitenden Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

I. eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

II. Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

III. die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

ABSCHNITT III

SCHLUSSBESTIMMUNGEN

Klausel 10

Verstöße gegen die Klauseln und Beendigung des Vertrags

1. Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.
2. Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn
    I. der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

II. der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 nicht erfüllt;

III. der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 zum Gegenstand hat, nicht nachkommt.

3. Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

4. Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

ANHANG I

LISTE DER PARTEIEN

Verantwortliche(r):

Gemäß Angebot/Auftragsbestätigung/Rechnung für das Produkt THERA-Trainer senso und die zugehörige Software.

Auftragsverarbeiter: [Name und Kontaktdaten des/der Auftragsverarbeiter/s und gegebenenfalls des Datenschutzbeauftragten des Auftragsverarbeiters]

Name: medica Medizintechnik GmbH

Anschrift: Blumenweg 8 88454 Hochdorf

Name, Funktion und Kontaktdaten der Kontaktperson:

Dr. Jonathan Kopf
CEO

Dr. Jonathan Kopf, CEO

ANHANG II

BESCHREIBUNG DER VERARBEITUNG

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden
☒ Kunden ☒ Patienten

Kategorien personenbezogener Daten, die verarbeitet werden
☒ Name
☒ E-Mailadresse
☒ IP-Adresse
☒ Geräteinformationen
☒ Geschlecht

Verarbeitete sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen

☒ Daten, Ergebnisse und Aufzeichnungen von Trainingseinheiten
☒ Daten, Ergebnisse und Aufzeichnungen von Leistungsevaluierungen

Art der Verarbeitung
Erfassung und Speicherung der Daten

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden
Erstellen von persönlichen Trainingsplänen, die auf die individuellen Leistungen und Fortschritte der Patienten abgestimmt ist.

Dauer der Verarbeitung
Gemäß Laufzeit vom Hauptvertrag.

Bei der Verarbeitung durch (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben.
Bereitstellung der SaaS Software zur Verarbeitung der Daten zu den oben genannten für die Dauer der Laufzeit des Hauptvertrags

ANHANG III

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN, EINSCHLIEßLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATE

medica Medizintechnik GmbH

Datenschutz-Konzept

Technische und organisatorische Maßnahmen im Sinne des Art. 32 Abs. 1 DSGVO

Stand:
Juni 2018

Autor:
Stefan Fischerkeller – Deutsche Datenschutzkanzlei

Inhaltsverzeichnis

1 Einleitung

Die EU-Datenschutzgrundverordnung (DSGVO) enthält Vorgaben darüber, wie in technischer und organisatorischer Hinsicht mit personenbezogenen Daten umgegangen werden soll. Dies dient dem Ziel der Datensicherheit. Die Datensicherheit stellt damit einen weiteren und ergänzenden Aspekt des Datenschutzes dar.

Gesetzlich geregelt ist die Datensicherheit in Art. 32 Abs. 1 DSGVO. Diese Vorschriften fordern, dass solche technischen und organisatorischen Maßnahmen zu treffen sind, die erforderlich sind, um den Schutz personenbezogener Daten zu gewährleisten.

Das Gesetz nennt verschiedene Kontrollbereiche, die jeweils noch verschiedene Unterpunkte beinhalten:

(1) Vertraulichkeit

(2) Integrität

(3) Verfügbarkeit und Belastbarkeit

(4) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(5) Pseudonymisierung und Verschlüsselung

Diese Maßnahmen stellen wir in der Folge vor, um unseren Informationspflichten aus Art. 28 Abs. 3 lit. c) DSGVO nachzukommen.

2 Organisatorisches

Die medica Medizintechnik GmbH gewährleistet die schriftliche Dokumentation des aktuellen Datenschutzniveaus, sowie der schriftlichen Arbeitsanweisungen, Richtlinien und Merkblätter für Mitarbeiter. Die bei der Datenverarbeitung eingesetzten Mitarbeiter sind auf das Datengeheimnis bzw. auf die Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. B, 29, 32 Abs. 4 DSGVO verpflichtet.

Einige diesen Bereich betreffenden Sicherungsmaßnahmen der folgenden Prüfliste sind nicht gesondert ausgewiesen, da sie in die Verantwortung der Unterbeauftragten fallen oder aus Gründen der Aufrechterhaltung der Sicherheit durch Vertraulichkeit nicht detailliert veröffentlich werden.

3 Sicherungsmaßnahmen

Die folgenden Punkte beschreiben die technischen und organisatorischen Maßnahmen, die von der medica Medizintechnik GmbH betrieben werden:

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

3.1.1 Zutrittskontrolle

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

- Pförtner/Personenkontrolle
- Zentrale Abteilung ist besetzt
- Nur Personen mit Berechtigungsausweis können das Gebäude (außerhalb der Besetzungszeiten der Zentralen Abteilung) betreten
- Die Verwaltung und Wartung der maschinellen Zutrittskontrollsysteme ist geregelt und wird dokumentiert
- Die Verteilerräume oder -bereiche (Gebäudetechnik) sind gegen unbefugten Zutritt gesichert
- Räume sind verschlossen; dazugehörige Schlüssel nur für Berechtigte verfügbar
- Einsatz einbruchshemmender Maßnahmen (Alarmanlage mit Fernschaltung zu einem Sicherheitsdienst)
- Unternehmensserver werden in einem abgeschlossenen und zutrittsgesicherten Raum betrieben. Nur Befugte haben Zutritt zum Serverraum
- Die Netzwerkkomponenten befinden sich in dafür vorgesehenen zutrittskontrollierten Räumen (zutrittsgesichert durch abgeschlossene Serverschränke oder abgeschlossene Räume)

3.1.2 Zugangskontrolle

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

- Es ist über die Rechteverwaltung bzw. bei individuellem Bedarf (in Überwachung mit der IT) sichergestellt, dass Benutzer nur Zugang zu den Netzdiensten bekommen, zu deren Nutzung sie ausdrücklich befugt sind
- Nur berechtigte Personen haben logischen Zugang zu den Netzwerkkomponenten
- Der (Fern-)Wartungsvorgang wird überwacht. Die Überwachung erfolgt über ein Protokoll der Firewall
- Verbindungsaufbau auf das Netzwerk von außerhalb über eine SSTP Verschlüsselung

Zusätzlich werden folgende Maßnahmen eingesetzt:

- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie
- Sicherheitsschlösser
- Authentifikation mit Benutzername und Passwort
- Verschlüsselung von Smartphone-Inhalten
- Einsatz von Anti-Viren-Software
- Verbindliches Verfahren zur Rechtevergabe
- Abschaltung von überflüssigen Diensten
- Netzwerkmonitoring mit Alarmierung

- Einsatz von Hardware-Firewall
- Funktionelle Beschränkung der Nutzung von Clientsystemen und Bildschirmarbeitsplätzen (restriktive Rechtevergabe)

3.1.3 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.

Die Einschränkung der Zugriffsmöglichkeiten wird gewährleistet durch:

- Datenträgerverwaltung-/Management
- Softwareseitigen Ausschluss (Berechtigungskonzept)
- Einschränkung Zugriffsmöglichkeiten der Benutzer
- Restriktive Zugriffsberechtigung/projektbezogene Zugänge
- Konzept zur Laufwerksnutzung/-zuordnung
- Berechtigungsvergabeverfahren
- Abgestufte Zugriffsrechte mit Logging/Protokollierung
- IT-Sicherheitsrichtlinien/Policies
- Personenbezogene Daten werden in der Regel nicht auf externen Datenträgern abgespeichert
- Es existiert eine Anweisung darüber, wie mit nicht mehr benötigten Datenträgern umzugehen ist (dazu gehört auch beschriebenes oder bedrucktes Papier)
    - Arbeitsanweisung Datenschutz und Datensicherheit
    - Teilprozessbeschreibung über alle Vorgänge in der IT
- Es existiert eine Anweisung darüber, wie bei der Entsorgung oder Weiterverwendung von Geräten vorzugehen ist, die mit Speichermedien ausgerüstet sind
    - Teilprozessbeschreibung über alle Vorgänge in der IT

3.1.4 Trennungsgebot

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

- Personenbezogene Daten auf den Systemen werden physisch voneinander getrennt (Verarbeitung unterschiedlicher Datensätze auf getrennten Systemen)
- Auf den Systemen werden personenbezogene Daten logisch voneinander getrennt (unterschiedliche Datensätze in einer einheitlichen Datenbank werden je nach Zweck markiert (softwareseitige Unterscheidbarkeit)
- Es besteht ein entsprechendes Berechtigungskonzept

- Es existieren Datenbankrechte
- Die Mandantenfähigkeit ist für die davon betroffenen Verfahren durchgängig realisiert
- Office-, Entwicklungs-, Test- und Wirksysteme bzw. Test- und Produktivdaten befinden sich auf unterschiedlichen Servern und im gleichen Netzwerk
- Es ist sichergestellt, dass im Entwicklungs- und Testsystem nur Testdaten verarbeitet werden

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

3.2.1 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.

- Alle Personen (auch neu Beschäftigte), die mit der Verarbeitung/Nutzung personenbezogener Daten beschäftigt sind, sind zur Einhaltung der Vertraulichkeit verpflichtet
    - Arbeitsanweisung zum Datenschutz
    - Datenschutz-Verpflichtungserklärung für Administratoren
    - Betriebsvereinbarung
- Es werden insbesondere neuen Beschäftigten Informationen zum Datenschutz ausgehändigt und von diesen gegengezeichnet (im Rahmen der Arbeitsanweisung)
- Mitarbeiter, die personenbezogene Daten verarbeiten/nutzen, werden durch Datenschutzschulungen - Awarenessmaßnahmen auf datenschutzgerechtes Verhalten am Arbeitsplatz geschult
- Anwendung der Regelungen zum On-/Off-Boarding-Prozess
- Für den physischen Transport von Datenträgern werden Sicherheitsmaßnahmen wie VPN und Verschlüsselungen umgesetzt

Zusätzliche Maßnahmen werden eingesetzt:

- Aufbau Transportverbindung nur zwischen definierten und durch Zertifikate gesicherten Systemen
- VPN-Zugänge für mobile Arbeitsplätze/Heimarbeitsplätze
- Kontrollierte Vernichtung von Datenträgern und Papierdokumenten nach DIN 66399

3.2.2 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.

- In einem Ordner mit Versionsverwaltung ist dokumentiert, welche benutzer- oder verfahrensbezogene Auswertemöglichkeiten im unserem Unternehmen eingesetzt werden (in der Zeiterfassung sind es 30 Tage)

- Es kann nachträglich überprüft werden, ob und vom wem Daten verarbeitet werden:

    - Benutzerprofile
    - Berechtigungskonzepte
    - Protokollierung der Eingabe, Änderung und Löschung von Daten
    - Firewall-Protokollierung (TCP/IP)
    - Protokollierung über Active Directory

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

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

Zufällige Zerstörung/Verlust von personenbezogenen Daten wird durch adäquate Maßnahmen verhindert:

- Einsatz unterbrechungsfreie Stromversorgung inkl. Überspannungsschutz und Notstromaggregat
- Löschanlage/Feuer-/Rauchmeldeanlage
- Blitzschutzeinrichtungen
- Einsatz Klimaanlage inkl. Dokumentation Klimatechnik
- Verteilung Netzwerkkomponenten zum Zweck der Risiko-/Ausfallminimierung auf mehrere geschützte Bereiche
- Überwachung Raumtemperatur/Luftfeuchtigkeit etc.
- Überspannungsschutz
- Alarmanlage inkl. Weiterleitung an Leitstelle, Werkschutz, Feuerwehr, Wachdienst etc.
- Es wird eine Risiko- und Schwachstellenanalyse durchgeführt, die von der IT bewertet wird. Es werden dabei die Risikofaktoren gegen die Aufrechterhaltung des DV-Betriebs untersucht.
- Es existiert ein Backup-/Recoverykonzept sowie ein Backup-Rechenzentrum. Die Anforderungen an das Backup sind in diesem Konzept dokumentiert
- Es existiert ein Notfallhandbuch, welches laufend aktualisiert wird
- Für den DV-Anlauf gibt es eine schriftliche Unterlage
- Es existiert ein Sicherheitsarchiv in den privaten Wohnräumen des Gesellschafters/Geschäftsführers, Herrn Otto Höbel, mit restriktivem Zutrittsberechtigungskonzept

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

3.3.1 Datenschutz-Management

Die medica Medizintechnik GmbH wird von der Deutschen Datenschutzkanzlei (externer Datenschutzbeauftragter stellt Herr Stefan Fischerkeller) betreut. Die Deutsche Datenschutzkanzlei nutzt ein eigens erstelltes Datenschutzmanagement-System (DSMS), in dem alle Maßnahmen, Verfahren sowie Tätigkeiten im Bereich des Datenschutzes abgebildet werden. Das DSMS beinhaltet die wichtigsten datenschutzrechtlichen Vorgaben und eine umfassende Struktur zur Abbildung der Datenschutzmaßnahmen und beinhaltet darüber hinaus einen Maßnahmenplan zur rechtskonformen Umsetzung der EU-Datenschutzgrundverordnung (Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO).

3.3.2 Incident-Response-Management

Ein prozessualisierter Umgang mit Sicherheitsvorfällen ist implementiert. Im Falle eines Vorfalls informieren die Mitarbeiter die IT bzw. ihren Vorgesetzten unverzüglich. Im Anschluss erfolgt die Abstimmung mit dem Datenschutzbeauftragten. Die Bearbeitung durch diesen ist durch entsprechende Vertretungsregelungen sichergestellt.

3.3.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Grundsätzlich werden nur Daten erhoben und verarbeitet, die für die Geschäftszwecke zweckmäßig und erforderlich sind. Verfahren der automatisierten Datenerfassung- und -verarbeitung sind so gestaltet, dass nur die erforderlichen Daten erhoben werden können. Die Daten der Kunden werden teilweise verschlüsselt vorgehalten.

3.3.4 Auftragskontrolle

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

Mitarbeiter, die als Administratoren Zugriff auf die Systeme haben, sind alle hinsichtlich des Datenschutzes belehrt, auf das Datengeheimnis verpflichtet und haben als Bestandteil ihres Arbeitsvertrags entsprechende Verschwiegenheits- und Geheimhaltungsvereinbarungen akzeptiert.

Sollte die medica Medizintechnik GmbH bei der Datenverarbeitung Unterauftragnehmer einsetzen, werden bestimmte Vorgaben umgesetzt. Hierzu zählt die Sicherstellung der technisch-organisatorischen Maßnahmen der Unterauftragnehmer im Sinne des Art. 28 DSGVO i. V. m. Art. 32 Abs. 1 DSGVO.

Voraussetzungen für das Eingehen eines Unterauftragsverhältnisses:

- Vertrag zur Auftragsdatenverarbeitung nach Vorgabe des Art. 28 Abs. 3 DSGVO.
- Deutsche Dienstleister haben einen betrieblichen Datenschutzbeauftragten bestellt und sorgen durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse.
- Beschreibung Prüfungen und Audits.
- Vergabe von Einzelaufträgen. Bestätigung von mündlichen Aufträgen.

- Für die Übermittlung von personenbezogenen Daten an externe Dienstleister steht eine Vertragsvorlage zur Auftragsdatenverarbeitung zur Verfügung, die entsprechende Regelungen zur Kontrolle enthält.

3.4 Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

Sofern eine direkte Personenbeziehbarkeit nicht erforderlich ist, wird von der Möglichkeit der Pseudonymisierung Gebrauch gemacht, wenn dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht (Datensparsamkeit). Die Datenübertragung von der Website erfolgt über die SSL Verschlüsselung.

3.5 Kooperation mit der Deutschen Datenschutzkanzlei

Zur Einhaltung der datenschutzrechtlichen Vorgaben nach der geltenden EU-Datenschutzgrundverordnung, arbeitet die medica Medizintechnik GmbH mit der Deutschen Datenschutzkanzlei zusammen. Neben der Erstellung von Richtlinien und Handlungshilfen, berät die Deutsche Datenschutzkanzlei die medica Medizintechnik GmbH in allen Fragen rund um den Datenschutz und stellt mit Herrn Stefan Fischerkeller den externen Datenschutzbeauftragten nach Art. 37 DSGVO des Unternehmens.

Ansprechpartner der Deutschen Datenschutzkanzlei sind:

Stefan Fischerkeller

Diplomverwaltungswirt (FH), geprüfter fachkundiger Datenschutzbeauftragter (DESAG)

E-Mail: fischerkeller@ddsk.de

Tel.: 07544 / 904 96 91

Maximilian Musch

Magister Artium, geprüfter fachkundiger Datenschutzbeauftragter (udis)

E-Mail: musch@ddsk.de

Tel.: 07544 / 904 96 92

Deutsche Datenschutzkanzlei

Büro Bodensee

Richard-Wagner-Straße 2, 88094 Oberteuringen

www.deutsche-datenschutzkanzlei.de

ANHANG IV

LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

Unterauftragsnehmer	**Land**	**Adresse**	**Kurzbeschreibung der Leistung**
Dividat AG	Schweiz	Neuhofstrasse 3, 8834 Schindellegi	Bereitstellung von Softwareanwendungen (SaaS) im Bereich der Pflege und Gesundheitsförderung