Version 09/2025

Vereinbarung zur Auftragsverarbeitung (AVV) inkl. Standardvertragsklauseln (SCC) (Art. 28, 29 DSGVO)

- Stand: 15.08.2025 -

Präambel:

Dieser Auftragsverarbeitungsvertrag regelt die Rechte und Pflichten der Vertragsparteien im Zusammenhang mit der Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO. Der vorliegende Vertrag basiert inhaltlich im Wesentlichen auf den **Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer** gemäß dem **Durchführungsbeschluss (EU) 2021/914 der Europäischen Kommission vom 4. Juni 2021**.

Die Standardvertragsklauseln bilden den Hauptbestandteil dieses Vertrags und wurden im Einklang mit den Vorgaben der Europäischen Kommission durch spezifische, vertraglich notwendige Ergänzungen vervollständigt – insbesondere durch Angaben zu den technischen und organisatorischen Maßnahmen, zur Art der verarbeiteten Daten, zu den Zwecken der Verarbeitung sowie zu den beteiligten Parteien und Unterauftragsverarbeitern.

Dieser Vertrag findet Anwendung auf alle Verarbeitungstätigkeiten im Zusammenhang mit dem zwischen den Parteien geschlossenen Dienstleistungsvertrag, bei denen Mitarbeiter des Auftragnehmers oder von ihm beauftragte Unterauftragnehmer personenbezogene Daten („Daten“) des Auftraggebers im Auftrag verarbeiten.

Die in diesem Vertrag verwendeten Begriffe sind im Sinne der Definitionen der EU-Datenschutz-Grundverordnung („DSGVO“) zu verstehen.

1. Zweck und Anwendungsbereich

1.1. 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 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sichergestellt werden.

1.2. Die in Anlage 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 Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.

1.3. Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anlage I.

1.4. Die Anhänge I bis IV sind Bestandteil der Klauseln.

1.5. Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 unterliegt.

1.6. 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.

2. Unabänderbarkeit der Klauseln

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

2.2. 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. Auslegung

3.1. 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.

3.2. Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.

3.3. 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.

4. Vorrang

4.1. 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.

5. Kopplungsklausel

5.1. 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 Anlage I unterzeichnet.

5.2. Nach Ausfüllen und Unterzeichnen der unter Ziffer 5.1. 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 Anlage II.

5.3. Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

6. Gegenstand und Dauer des Auftrags

6.1. Der Auftrag umfasst Folgendes: Therapiedatenverarbeitung

6.2. Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für die in Anlage I genannten spezifischen Zwecke, sofern er keine weiteren Weisungen des Verantwortlichen erhält.

6.3. Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO.

6.4. Die Daten werden vom Auftragsverarbeiter nur für die in Anlage I angegebene Dauer verarbeitet.

6.5. Vorbehaltlich der Regelungen eines gegebenenfalls bestehenden Hauptvertrags ist für jede Kündigung die Schriftform erforderlich.

7. Verarbeitungsrahmen / Art und Zweck der Verarbeitung

7.1. Der Auftragnehmer verarbeitet personenbezogene Daten wie folgt und zu folgendem Zweck:

a) Speichern und Visualisieren von gerätespezifischen und geräteunspezifischen Therapiedaten, die einem Benutzer (Patienten) zugeordnet sind

7.2. Art der personenbezogenen Daten und Kategorien betroffener Personen

a) Die Art der Daten und die Kategorien betroffener Personen, die Gegenstand dieser Vereinbarung sind, sind definiert in Anlage I: Art der Daten und Kategorien betroffener Personen.

8. Technische und organisatorische Maßnahmen

8.1. 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 die Dokumentation zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

8.2. Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c) und Art. 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen und zu gewährleisten. Insgesamt

handelt es sich bei den dabei zu treffenden technischen und organisatorischen Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

8.3. Die Einzelheiten der technischen und organisatorischen Maßnahmen (TOMs) des Auftragnehmers sind in Anlage IV geregelt.

8.4. 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.

9. Ort der Verarbeitung

9.1. Die Verarbeitung der Daten findet in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

9.2. Jede Verlagerung der Daten in einen anderen Staat (sogenanntes „*Drittland*“) bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

10. Weisungen und Weisungsbefugnis des Auftragnehmers

10.1. 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.

10.2. 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.

11. Sicherheit der Verarbeitung

11.1. Der Auftragsverarbeiter ergreift mindestens die in Anlage IV 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.

11.2. 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

12. Sensible Daten

12.1. 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 zusätzlichen Garantien an.

13. Dokumentation und Einhaltung der Klauseln

13.1. Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

13.2. Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

13.3. 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.

13.4. 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.

13.5. Die Parteien stellen den zuständigen Aufsichtsbehörden die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

14. Einsatz von Unterauftragsverarbeitern

14.1. 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.

14.2. 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.

14.3. 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.

14.4. 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.

14.5. 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.

15. Internationale Datenübermittlungen

15.1. 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.

15.2. Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Punkt 14 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.

16. Unterstützung des Verantwortlichen

16.1. Der Auftragsverarbeiter (Auftragnehmer) unterrichtet den Verantwortlichen (Auftraggeber) unverzüglich über jeden Antrag einer betroffenen Person. Eine Beantwortung erfolgt nur, wenn er dazu vom Auftraggeber ermächtigt wurde.

16.2. Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragnehmer den Auftraggeber bei der Beantwortung von Anträgen betroffener Personen auf Ausübung ihrer Rechte und befolgt dabei dessen Weisungen.

16.3. Geeignete technische und organisatorische Maßnahmen zur Unterstützung des Auftraggebers sowie deren Anwendungsbereich und Umfang werden in Anlage IV festgelegt.

16.4. Zusätzlich unterstützt der Auftragnehmer den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung folgender Pflichten:

a) Durchführung einer Datenschutz-Folgenabschätzung (DSFA), wenn eine Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt.
b) Konsultation der zuständigen Aufsichtsbehörde vor der Verarbeitung, wenn die DSFA ein hohes Risiko ergibt und keine Maßnahmen zur Risikominderung getroffen wurden.
c) Sicherstellung der Richtigkeit und Aktualität personenbezogener Daten durch unverzügliche Information an den Auftraggeber, wenn unrichtige oder veraltete Daten festgestellt werden.
d) Umsetzung der Vorgaben aus Art. 32 DSGVO (Sicherheit der Verarbeitung).
e) Meldung von Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber und Bereitstellung aller relevanten Informationen zur Erfüllung seiner Informationspflichten gegenüber Betroffenen (Art. 33, 34 DSGVO).
f) Unterstützung im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde (Art. 36 DSGVO).

17. Rechte und Pflichten des Auftragnehmers

17.1. Erfüllung aller gesetzlichen Pflichten gemäß Art. 28–33 DSGVO.
17.2. Wahrung der Vertraulichkeit nach Art. 28 Abs. 3 S. 2 lit. b), 29, 32 Abs. 4 DSGVO, Einsatz nur entsprechend verpflichteter und geschulter Mitarbeiter.
17.3. Verarbeitung personenbezogener Daten ausschließlich gemäß Weisungen des Auftraggebers, sofern keine gesetzliche Verpflichtung zur anderweitigen Verarbeitung besteht.
17.4. Umsetzung und Einhaltung aller erforderlichen technischen und organisatorischen Maßnahmen nach Art. 28 Abs. 3 S. 2 lit. c), 32 DSGVO (Einzelheiten siehe Anlage IV).
17.5. Zusammenarbeit mit der Aufsichtsbehörde auf Anfrage.
17.6. Regelmäßige Kontrolle interner Prozesse sowie technischer und organisatorischer Maßnahmen zur Sicherstellung der datenschutzkonformen Verarbeitung und des Schutzes der Betroffenenrechte.
17.7. Nachweis der getroffenen Maßnahmen gegenüber dem Auftraggeber gemäß Ziffer 16 dieses Vertrags und Erfüllung der Pflichten aus Ziffer 21.

18. Meldung von Verletzungen des Schutzes personenbezogener Daten

18.1. 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.

19. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

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

19.2. 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);

19.3. 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:

a) 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;

b) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

c) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls 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;

19.4. 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.

20. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

20.1. 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:

20.2. 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);

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

20.4. 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.

20.5. 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 Anlage IV 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.

21. Unterauftragsverhältnisse

Hinsichtlich der Beauftragung von Unterauftragnehmern vereinbaren die Parteien Folgendes:

☐ Der Auftragnehmer darf Unterauftragsverhältnisse hinsichtlich der vertragsgegenständlichen Verarbeitung personenbezogener Daten nur nach vorheriger schriftlicher Zustimmung des Auftraggebers begründen (gem. Art. 28 Abs. 2 S. 1 DSGVO).

☒ Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, Unterauftragnehmer einzusetzen. Der Auftragsverarbeiter informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (gem. Art. 28 Abs. 2 S. 2 DSGVO).

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

21.2. Der Auftragnehmer hat den Unterauftragnehmer schriftlich in gleichem Umfang zu verpflichten, wie er selbst aufgrund dieses Vertrags gegenüber dem Auftraggeber verpflichtet ist.

21.3. Kommt der Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Unterauftragnehmers gem. Art. 28 Abs. 4 DSGVO.

21.4. Der Auftragnehmer wird sich vor Beauftragung von der Einhaltung der beim Unterauftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugen.

21.5. Sofern eine Einbeziehung von Unterauftragnehmern in Drittländern erfolgen soll, stellt der Auftragnehmer sicher, dass beim jeweiligen Unterauftragnehmer ein angemessenes Datenschutzniveau im Sinne der Art. 44 ff. DSGVO gewährleistet ist. Der Unterauftragnehmer hat einen Vertreter in der EU zu bestellen.

21.6. Der Auftraggeber stimmt hiermit der Begründung der Unterauftragsverhältnisse gemäß Anlage III Unterauftragnehmer zu.

22. Kontrollrechte des Auftraggebers

22.1. Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann.

22.2. Der Auftragnehmer wird im Rahmen der Prüfung alle erforderlichen Informationen und Auskünfte erteilen, Unterlagen vorlegen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachweisen. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch:

22.3. Die Einhaltung genehmigter Verhaltensregeln, gem. Art. 40 DSGVO

a) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO

b) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)

c) eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz).

22.4 Der Auftraggeber darf nach rechtzeitiger Abstimmung, zu den üblichen Geschäftszeiten, die technischen und organisatorischen Maßnahmen des Auftragnehmers zur Einhaltung dieser Vereinbarung prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

22.5 Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

23. Löschung und Rückgabe von personenbezogenen Daten

23.1. 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.

23.2. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Die gesetzlichen Aufbewahrungspflichten bleiben unberührt.

24. Gesetzliche Haftung

24.1. Es gelten die gesetzlichen Haftungsregelungen gem. Art. 82 DSGVO. Etwaige Haftungsbegrenzungen zwischen den Parteien (z.B. aus dem Hauptvertrag) finden diesbezüglich keine Anwendung.

25. Schlussbestimmungen

25.1. Für diese Vereinbarung gilt deutsches Recht.

25.2. Sollte eine Vertragsbestimmung unwirksam sein oder werden, so berührt dies die Gültigkeit des übrigen Vertragsinhalts nicht. Die Vertragsparteien werden sich bemühen, in einem solchen Fall eine in ihrem wirtschaftlichen Ergebnis dem jetzigen Sinn entsprechende Lösung zu finden. Dies gilt auch, wenn bei Durchführung des Vertrags eine ergänzungsbedürftige Lücke offenbar wird.

25.3. Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform. Dies gilt auch für die Aufhebung des Schriftformerfordernisses.

25.4. Anlagen zu diesem Vertrag sind:

Anlage I:	Art der Daten und Kategorien betroffener Personen
Anlage II:	Liste der Parteien
Anlage III:	Unterauftragnehmer
Anlage IV:	Technische und organisatorische Maßnahmen des Auftragnehmers

26. Verstöße gegen die Klauseln und Beendigung des Vertrags

26.1. 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.

26.2. Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

26.3. 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;

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

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

26.6. 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 Punkt 10.2. verstoßen.

26.7. 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.

Anlage I: Art der Daten und Kategorien betroffener Personen

Art der Daten

Folgende Datenarten sind Gegenstand dieses Auftrags (*bitte Zutreffendes ankreuzen*):

☒ Personenstammdaten (z. B. Name, Adresse)

☐ Kommunikationsdaten (z. B. Telefon, E-Mail)

☐ Alter

☒ Besondere Kategorien pb. Daten nach Art. 9 Abs. 1 DSGVO (z.B. Gesundheitsdaten)

☐ Bewerberdaten

☐ Vertrags-/Mitarbeiterstammdaten (z.B. Personal- und Identifikationsnummer)

☐ Lohn- und Gehaltsdaten

☐ Steuer-/Buchhaltungsdaten

☐ Arbeitszeitdaten

☐ Mitarbeiterbewertungen

☐ Mitarbeiterqualifikation und -Eigenschaften

☐ Telekommunikationsabrechnungsdaten

☐ Telekommunikationsverbindungsdaten

☒ Planungs- und Steuerungsdaten

☐ Vertragsabrechnungs- und Zahlungsdaten

☐ Kundenhistorie

☐ Kundenverhaltensdaten

☐ Nutzerkennungen

☒ Passwörter

☒ Zugangsdaten

☐ Bankverbindungsdaten

☐ Kreditkartendaten

☐ Audiodaten

☐ Bilddaten

☐ Videodaten

☐ Auskunftsangaben (Auskunfteien; öffentliche Verzeichnisse etc.)

☒ Sonstige, und zwar Maschinendaten, Therapiedaten

Kategorien betroffener Personen

Folgende Kreise von Betroffenen sind Gegenstand des Auftrags:

☒ Beschäftigte

☐ Auszubildende und Praktikanten

☐ Bewerber

☐ ehemalige Arbeitnehmer

☐ freie Mitarbeiter

☐ Gesellschafter

☐ Angehörige von Beschäftigten

☐ Kunden

☐ Interessenten

☐ Lieferanten und Dienstleister

☐ Mieter

☐ Geschäftspartner

☐ Berater

☐ Besucher

☐ Pressevertreter

☐ Abonnenten

☐ Handelsvertreter

☐ Ansprechpartner

☒ Sonstige, und zwar Patienten

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.

Anlage II: Liste der Parteien

Verantwortliche(r):

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

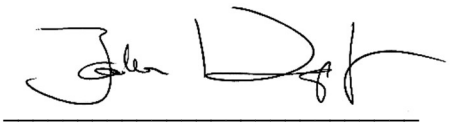
Auftragsverarbeiter: [*Name und Kontaktdaten des/der Auftragsverarbeiter/s und gegebenenfalls des Datenschutzbeauftragten des Auftragsverarbeiters*]

Name: medica Medizintechnik GmbH

Anschrift: Blumenweg 8 88454 Hochdorf

Name, Funktion und Kontaktdaten der Kontaktperson:

Dr. Jonathan Kopf
CEO



Dr, Jonathan Kopf, CEO

Anlage III: Unterauftragnehmer

Der Auftraggeber stimmt der Beauftragung folgender Unterauftragnehmer durch den Auftragnehmer zu:

Unternehmens-bezeichnung / Firma des Unterauftrag-nehmers	Postadresse	Sonstige Kontaktdaten (E-Mail, Telefon)	Ansprech-partner	Gegenstand des Unterauftrags
Dividat AG	Neuhofstrasse 3, CH 8834 Schindellegi	info@dividat.ch +41 44 586 88 34	Joris van het Reve	Bereitstellung von Softwareanwendungen (SaaS) im Bereich der Pflege und Gesundheits-förderung
Unternehmensbezeichnung / Firma des Unterauftragnehmers	Post-adresse	Sonstige Kontaktdaten	Ansprech-partner	Gegenstand des Unterauftrags
Unternehmensbezeichnung / Firma des Unterauftragnehmers	Post-adresse	Sonstige Kontaktdaten	Ansprech-partner	Gegenstand des Unterauftrags
Unternehmensbezeichnung / Firma des Unterauftragnehmers	Post-adresse	Sonstige Kontaktdaten	Ansprech-partner	Gegenstand des Unterauftrags

Anlage IV: Technische und organisatorische Maßnahmen des Auftragnehmers

medica Medizintechnik GmbH
Blumenweg 8
88454 Hochdorf

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

Stand: Dezember 2023
Autor: Wählen Sie ein Element aus.

Beschreibung

Technische und organisatorische Maßnahmen i. S. d. Art. 32 Abs. 1 DSGVO

Formblatt | Stand: 19.12.2023 | Klassifikation: **vertraulich** | Verantw.: DSB | Version 2.1

Inhaltsverzeichnis

THERA-Trainer by medica Medizintechnik GmbH
Blumenweg 8 | 88454 Hochdorf
Tel +49 7355-93 14-0 | info@thera-trainer.com | www.thera-trainer.com

Beschreibung

Technische und organisatorische Maßnahmen i. S. d. Art. 32 Abs. 1 DSGVO

Formblatt | Stand: 19.12.2023 | Klassifikation: **vertraulich** | Verantw.: DSB | Version 2.1

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 sind die Anforderungen an 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 Art. 28 Abs. 3 lit. c) DSGVO nachzukommen.

THERA-Trainer by medica Medizintechnik GmbH
Blumenweg 8 | 88454 Hochdorf
Tel +49 7355-93 14-0 | info@thera-trainer.com | www.thera-trainer.com

2 Organisatorisches

Das Unternehmen 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 etwaiger Unterbeauftragten fallen oder aus Gründen der Aufrechterhaltung der Sicherheit nicht detailliert veröffentlich werden.

3 Datenschutz-Management

Maßnahmen, die gewährleisten, dass personenbezogene Daten und Personen, die mit diesen arbeiten, organisatorisch auf den Umgang hingewiesen bzw. verpflichtet wurden.

Folgende Maßnahmen wurden im Unternehmen getroffen:

- Die Rollen DSKO, (e)DSB im Bereich Datenschutz sind benannt und über den Umfang ihrer jeweiligen Aufgaben informiert.
- Die Fachkunde des (e)DSBs wird sichergestellt.
- Es existiert ein on-boarding Prozess für neue Beschäftigte in dem Datenschutzthemen berücksichtigt werden und die Vergabe der Rechte durch die IT-Abteilung geregelt ist.
- Alle Beschäftigten haben eine Verpflichtung zur Einhaltung der Vertraulichkeit unterschrieben
- Alle neuen Beschäftigten erhalten bei der Verpflichtung zur Vertraulichkeit Informationen zum Datenschutz. Des Weiteren sind die Beschäftigten auf das Datengeheimnis verpflichtet worden.
- Die Beschäftigten werden regelmäßig durch Datenschutzschulungen/Awarenessmaßnahmen auf datenschutzgerechtes Verhalten geschult.
- Es existiert ein off-boarding Prozess zum Umgang mit ausscheidenden Beschäftigten und dem Entzug der erteilten Rechte/Betriebsmittel.

4 Schutzmaßnahmen

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

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

4.1.1 Zutrittskontrolle

Die Zutrittskontrolle umfasst Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (bspw. automatisches Zutrittskontrollsystem, manuelles Schließsystem, Videoüberwachung, Wachpersonal etc.).

TT-Cloud spezifische Maßnahmen durch Microsoft Azure:

THERA-Trainer by medica Medizintechnik GmbH
Blumenweg 8 | 88454 Hochdorf
Tel +49 7355-93 14-0 | info@thera-trainer.com | www.thera-trainer.com

Beschreibung

Technische und organisatorische Maßnahmen i. S. d. Art. 32 Abs. 1 DSGVO

- Physische Sicherheitsmaßnahmen in Microsoft Azure-Rechenzentren, einschließlich:
- Strenge Zutrittskontrollen mit biometrischer Identifikation und mehrstufiger Authentifizierung
- 24/7-Überwachung durch Sicherheitspersonal
- Videoüberwachung und Alarmmanagement
- Redundante Stromversorgung, Klimatisierung und Brandschutzsysteme
- Zertifizierungen gemäß ISO 27001, SOC 2

Maßnahmen durch unser Unternehmen:

- Auswahl von Azure-Regionen innerhalb der EU zur Einhaltung der DSGVO
- Nutzung von Azure Security Center zur Überwachung sicherheitsrelevanter Ereignisse
- Begrenzung administrativer Zugriffe auf Azure-Administratorkonten (Zero-Trust-Prinzip)
- Logging aller Zugriffsvorgänge auf die Cloud-Ressource
- Regelmäßige Überprüfung von Microsofts Sicherheitsberichten und Zertifizierungen

medica IT/Entwicklungs- spezifische Maßnahmen

- Bebauungsart:
  - Es ist ein freistehender Gebäudekomplex, das Grundstück offen zugänglich.
  - Es ist ein Grundstück mit Werksgelände, das Grundstück ist offen zugänglich.
  - Es handelt sich um eine geschlossene Bebauung.
  - Es existiert ein Gebäudesicherungskonzept.
  - Die Zufahrt zum Firmengelände ist frei zugänglich.
  - Es existiert eine Besucherverwaltung und alle Besucher des Unternehmens müssen sich am zentralen Empfang anmelden und dürfen die nicht-öffentlichen Bereiche nur in Begleitung betreten. Zusätzlich findet eine Erfassung der Besucher im Besucherbuch statt.
- Das Unternehmen setzt ein automatisches Zugangskontrollsystem ein, die berechtigten Personen verwenden zur Verifizierung Chipkarten / Token.
- Im Unternehmen werden teilweise / ausschließlich Sicherheitsschlösser eingesetzt.
- Das Unternehmen hat ein manuelles Schließsystem.
- Es existiert eine dokumentierte Schlüsselvergabe für die Schlüssel / Token / Chipkarten.
- Das Unternehmen setzt ein Schließsystem mit Codesperre ein.
- Das Unternehmen hat eine Personenkontrolle, welche alle Besucher kontrolliert.
- Zur Überwachung des Firmengeländes und des -gebäudes werden Lichtschranken / Bewegungsmelder eingesetzt, die mit der Firmensicherheitszentrale verbunden sind und diese alarmieren.
- Die Verwaltung und Wartung der maschinellen Zutrittskontrollsysteme ist geregelt und dokumentiert.
- In den Zutrittskontrollanlagen werden personenbezogene Daten gespeichert, sodass nachvollziehbar ist, wer wann einen bestimmten räumlichen Bereich betreten und ggf. auch wieder verlassen hat (eventuell inkl. Auswertung bei Sicherheitsverletzungen).
- Es sind Sicherheitszonen unterschiedlicher Klassifizierung und Sensibilität vorhanden.
- Der Gebäudekomplex ist außerhalb der Geschäftszeiten geschlossen und kann nur von berechtigten Personen manuell geöffnet werden.
- Die Büroräume des Unternehmens sind separat gesichert über ein elektronisches Sicherheitsschloss /
- Entsprechende Regelungen für den Zutritt von externen Personen (Wartungsdienst; Reinigungsdienst; Besucher) sind implementiert. Externe Personen, die Zutritt zum Rechenzentrum benötigen, halten sich ausschließlich in Beisein der IT-Administration im Rechenzentrum auf.
- Serverraum:

THERA-Trainer by medica Medizintechnik GmbH
Blumenweg 8 | 88454 Hochdorf
Tel +49 7355-93 14-0 | info@thera-trainer.com | www.thera-trainer.com

- Die Unternehmensserver werden in einem abgeschlossenen und zutrittsgesicherten Raum betrieben; zu diesem Serverraum haben nur befugte Personen Zutritt.
- Es sind Maßnahmen zur Raumüberwachung des Serverraums/Rechenzentrums getroffen (Bewegungsmelder) worden.

4.1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (bspw. Maßnahmen zur Authentifikation, VPN-Verbindungen)

TT- Cloud spezifische Maßnahmen:

- Identitäts- und Zugriffsmanagement (IAM)
  - Nutzung von Microsoft Entra ID (ehemals Azure AD) zur zentralen Verwaltung von Benutzerrechten
  - Rollenbasierte Zugriffskontrolle (RBAC) zur Vergabe minimaler Rechte (Least Privilege-Prinzip)
  - Regelmäßige Überprüfung und Anpassung der Berechtigungen
- Authentifizierungssicherheit
  - Multi-Faktor-Authentifizierung (MFA) für alle administrativen und sensiblen Zugriffe
- Absicherung der Anmeldeverfahren
  - Single Sign-On (SSO) für eine sichere und zentrale Authentifizierung
  - Nutzung von Azure Password Protection zur Erzwingung sicherer Passwörter und Verhinderung schwacher Passwörter
  - Protokollierung von Anmeldeversuchen über Microsoft Defender for Cloud
- Netzwerkbasierte Zugangskontrollen
  - Beschränkung des Zugriffs auf kritische Dienste durch Azure Virtual Network (VNet) und Network Security Groups (NSG)

medica IT spezifische Maßnahmen:

- Der Zugang zu den EDV-Systemen ist nur mit individuellen Benutzernamen und Kennwörtern möglich.
- Der Zugang zu den EDV-Systemen ist nur den Beschäftigten des Unternehmens möglich, welche hierfür die Zugangsberechtigung erhalten haben.
- Es ist mit der Geschäftsführung ein Vergabeprozess für die Zugangsrechte definiert und die Freigabe erfolgt nach diesem definierten Prozess.
- Es erfolgt eine Protokollierung der Benutzeranmeldungen und des jeweiligen Zeitpunktes der Anmeldung.
- Es gibt für alle Informationssysteme und Dienste eine formale Benutzer-Registrierung und Deregistrierung zur Vergabe und Rücknahme von Zugangsberechtigungen.
- Es ist sichergestellt, dass nur berechtigte Personen logischen Zugang zu den Netzwerkkomponenten haben.
- Es existieren ausreichende Maßnahmen zur Identifikation und Authentisierung von externem Wartungspersonal (z. B. sicherer Passwortschutz, eigener Benutzeraccount).
- Es werden Initialpasswörter verwendet und eine Änderung wird systemseitig bei der ersten Anmeldung erzwungen. Zusätzlich werden die Beschäftigten regelmäßig aufgefordert ihr Passwort zu ändern. Die fehlerhaften Passworteingaben werden protokolliert.
- Erfolgt ein (Fern-) Wartungsvorgang wird dieser überwacht und protokolliert. Der Anwender hat jederzeit die Möglichkeit die Verbindung zu beenden.

THERA-Trainer by medica Medizintechnik GmbH
Blumenweg 8 | 88454 Hochdorf
Tel +49 7355-93 14-0 | info@thera-trainer.com | www.thera-trainer.com

- Der Zugriff auf das Unternehmensnetzwerk von außerhalb erfolgt über verschlüsselte Verbindungen (bspw. VPN) und einer separaten Authentisierung.
- Zur Authentisierung kommen biometrischen Verfahren zum Einsatz.
- Im Unternehmen erfolgt die Zuordnung von Benutzerprofilen zu den jeweiligen IT-Systemen.
- Im Unternehmen werden auf allen IT-Systemen Anti-Viren-Lösungen eingesetzt.
- Das Unternehmen schaltet überflüssige Dienste ab.
- Das Unternehmen schützt die IT-Infrastruktur durch Software- und Hardware-Firewalls.
- Die Authentifikation erfolgt mit Benutzername / Passwort.
- Es findet eine Reduktion zugriffberechtigter Personen auf ein Minimum statt.
- Es existiert eine funktionelle Beschränkung der Nutzung von Clientsystemen und Bildschirmarbeitsplätzen (restriktive Rechtevergabe).
- Die IT-Abteilung setzt ein Netzwerkmonitoring mit Alarmierung ein.
- Es wird ein separates Gäste-WLAN eingesetzt, so dass ein Zugang über dieses zum Firmennetzwerk nicht möglich ist.

4.1.3 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 (bspw. automatische Prüfung der Zugriffsberechtigung mittels Passwort, differenzierte Zugriffsberechtigungen auf Anwendungsprogramme).

TT-Cloud spezifische Maßnahmen:

Berechtigungskonzept & Rollenverwaltung

- Implementierung eines rollenbasierten Zugriffskonzepts (RBAC)
- Minimalprinzip („Least Privilege") und Need-to-Know-Prinzip:
  - Nur erforderliche Berechtigungen für Mitarbeiter und Dienstleister
  - Regelmäßige Überprüfung und Anpassung der Rollen
- Automatische Deaktivierung von inaktiven Benutzerkonten

Datensicherheit & Zugriffsbeschränkung

- Verschlüsselung von Daten bei Speicherung und Übertragung mit Azure Storage Encryption (AES-256) und TLS 1.2/1.3
- Zugriff auf medizinische Patientendaten erfolgt nur durch berechtigte Benutzergruppen

Protokollierung & Monitoring

- Logging und Überwachung aller Zugriffe über Microsoft Defender for Cloud
- Nutzung von Azure Monitor und Log Analytics zur Erkennung von Anomalien und unerlaubten Zugriffen

Sitzungsmanagement & Zugriffsbeschränkung

- Automatische Sitzungstimeouts für ungenutzte Sitzungen

medica IT/Entwicklungs- spezifische Maßnahmen:

- Es existiert ein Rollen- und Berechtigungskonzept; die Berechtigungsprüfungen erfolgen auf Basis dieses Konzeptes.

THERA-Trainer by medica Medizintechnik GmbH
Blumenweg 8 | 88454 Hochdorf
Tel +49 7355-93 14-0 | info@thera-trainer.com | www.thera-trainer.com

- Es existiert eine im Berechtigungskonzept umgesetzte Trennung von Abrechnungs- und Kundenstammdaten.
- Die Berechtigungsvergabe basiert auf dem «need-to-know-Prinzip»
- Es existiert eine Anweisung an die Benutzer, wie mit den DV-Systemen bei Verlassen des Arbeitsplatzes (Sperren) umzugehen ist.
- Personenbezogene Daten können nur im Rahmen des Berechtigungskonzepts gelesen, kopiert, verändert oder entfernt werden.
- Eine Verwendung fortlaufend aktualisierter Virenschutzsoftware ist technisch durch die IT-Abteilung sichergestellt.
- Eingehender E-Mail-Verkehr wird durch ein zentrales Virenschutz- und Spamfiltersystem auf Viren und Spam überprüft.
- Es existiert eine Passwortrichtlinie, welche die aktuellen Empfehlungen des BSI berücksichtigt. Die Mindestkriterien sind systemseitig festgelegt.
- Es ist ein softwareseitiger Ausschluss (Berechtigungskonzept) etabliert.
- Die Zugriffsmöglichkeiten der Benutzer sind auf den benötigten Umfang eingeschränkt.
- Es sind restriktive Zugriffsberechtigung/projektbezogene Zugänge etabliert.
- Es existiert ein abgestimmtes Berechtigungsvergabeverfahren.
- Die IT-Abteilung hat IT-Sicherheitsrichtlinien/Policies erstellt und die Beschäftigten darauf geschult.
- Es erfolgt eine Verschlüsselung der Daten auf Dateiebene/Verzeichnisebene.
- Es existiert eine Anweisung an die Mitarbeiter, wie mit nicht mehr benötigten Datenträgern (Festplatten, USB-Sticks, Papierform) umzugehen ist.
- Es existiert eine Anweisung über die Entsorgung von Geräten inkl. Speichermedien.

4.1.4 Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (bspw. Trennung Test- und Produktivumgebung, Trennung Managementnetz von Produktionsnetz, logische Trennung etc.).

Cloud spezifische Maßnahmen:

Technische Maßnahmen zur Datentrennung

- Mandantenfähige Architektur in Microsoft Azure:
  - Nutzung separater Azure Subscriptions und Resource Groups zur Trennung von Entwicklungs-, Test- und Produktivumgebungen
- Datenbank- und Speichertyp-Trennung:
  - Trennung sensibler Patientendaten von allgemeinen System- oder Log-Daten
  - Nutzung von separaten Datenbanken und Zugriffsbeschränkungen für Patientendaten
- Zugriffssteuerung auf Applikationsebene:
  - Implementierung von rollenbasierten Zugriffsbeschränkungen (RBAC) zur Trennung von Benutzergruppen (z. B. Administratoren, Therapeuten, technische Mitarbeiter)

medica IT/Entwicklungs- spezifische Maßnahmen:

- Das Unternehmen setzt ein Test- und Freigabeverfahren für Softwareprodukte ein.
- Im Unternehmen erfolgt die Trennung der Produktiv- von der Test- und Entwicklungsumgebung.
- Das Managementnetz ist vom Produktionsnetz getrennt.
- Es erfolgt eine logische Trennung der Systemlandschaft gemäß dem Rollen- und Berechtigungskonzept.
- Im Unternehmen werden die Testdaten von Produktivdaten getrennt.
- Die Entwicklungs- und Produktionsprogramme sind voneinander getrennt.

THERA-Trainer by medica Medizintechnik GmbH
Blumenweg 8 | 88454 Hochdorf
Tel +49 7355-93 14-0 | info@thera-trainer.com | www.thera-trainer.com

- Es existiert ein Änderungsmanagement mit differenziertem Freigabeverfahren.
- Es ist ein softwareseitiger Ausschluss (Mandantentrennung) etabliert.
- Es werden Maßnahmen zur Anonymisierung / Pseudonymisierung eingesetzt.

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

4.2.1 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 (bspw. Vernichtung, Löschung und Verschlüsselung von Datenträgern, VPN-Verschlüsselung, Hardwareverschlüsselung).

Cloud spezifische Maßnahmen

Technische Maßnahmen zur Absicherung der Datenübertragung

- Ende-zu-Ende-Verschlüsselung aller Datenübertragungen:
  - TLS 1.2/1.3 für alle Netzwerkverbindungen
  - Azure Storage Encryption für gespeicherte Daten
- Sichere API- und Systemkommunikation:
  - REST API mit JWT Authentifizierungstoken

Organisatorische Maßnahmen zur Kontrolle der Datenweitergabe

- Strikte Zugriffskontrollen für Datenexporte:
  - Nur berechtigte Benutzer dürfen Daten exportieren oder weitergeben
  - Genehmigungsverfahren für externe Datenweitergaben
  - Protokollierung und Nachverfolgung aller Datenweitergaben
- Vertragsmanagement und AVV mit externen Empfängern:
  - Abschluss von Datenschutzvereinbarungen (AVV) mit allen externen Dienstleistern
  - Regelmäßige Datenschutzprüfungen bei externen Empfängern

medica IT/Entwicklungs- spezifische Maßnahmen:

- Bei der Weitergabe von Daten werden nur freigegebene Verschlüsselungslösungen / Nutzung von VPN-Tunneln bei Übertragungen eingesetzt.
- Es existiert ein unternehmensweit gültiges Klassifizierungskonzept von Daten bzgl. der Vertraulichkeitsstufe.
- Der Zugriff auf die Daten und Dateien über das Web erfolgt über eine SSL-verschlüsselte Verbindung.
- Regelung des Systemkommunikationsverkehrs (zentrale Firewall, exklusive WAN-Verbindungen (Wide Area Network) mit Zugriffkontrollen), Protokollierung (Userauthentifizierung, Zeitpunkt).
- Der Aufbau der Transportverbindung findet nur zwischen definierten und durch Zertifikate gesicherten Systemen statt.
- Die Beschäftigten können nur über VPN-Zugänge von ihren mobilen Arbeitsplätzen/ Heimarbeitsplätzen auf das Unternehmensnetzwerk zugreifen.
- Die Beschäftigten können Dienste nur nutzen, die von der IT freigegebenen wurden.
- Es findet eine kontrollierte Vernichtung von Datenträgern und Papierdokumenten nach DIN 66399 statt.

THERA-Trainer by medica Medizintechnik GmbH
Blumenweg 8 | 88454 Hochdorf
Tel +49 7355-93 14-0 | info@thera-trainer.com | www.thera-trainer.com

4.2.2 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 (bspw. Benutzerprofile, Protokollierung eingegebener Daten (Verarbeitungsprotokoll), gescheiterte Anmeldeversuche, administrative Tätigkeiten über ein Ticketsystem).

TT-cloud spezifische Maßnahmen

- Benutzeridentifikation & Authentifizierung:
  - Individuelle Benutzerkonten für alle Eingaben (keine anonymen oder gemeinsamen Konten)
- Feldbasierte Validierung & Prüfmechanismen:
  - Eingaben durch Pflichtfelder, Plausibilitätsprüfungen und Wertebereiche absichern
  - Automatische Warnmeldungen bei fehlerhaften Eingaben
  - Spring JPA Repositories und JDBC mit ausschließlich named oder indexed/positional Parameters. *(Die Parameter werden nicht direkt in den SQL-String eingebaut, sondern sicher als Variablen verarbeitet, wodurch SQL-Injections ausgeschlossen sind.)*

Organisatorische Maßnahmen zur Eingabekontrolle

- Klare Rollenverteilung und Berechtigungskonzepte für Datenänderungen
- Schulung der Mitarbeiter zu sicheren und korrekten Dateneingaben
- Regelmäßige Datenschutz- und Sicherheitsüberprüfungen der Eingabeverfahren

medica IT/Entwicklungs- spezifische Maßnahmen:

- Im Unternehmen werden systemseitige Plausibilitätskontrollen umgesetzt.
- Es ist ein Rollen- und Berechtigungskonzept vorhanden.
- Alle Beschäftigten haben auf deren Berechtigungsumfang angepasste Benutzerprofile.
- Im Unternehmen erfolgt eine Protokollierung der eingegebenen Daten (Verarbeitungsprotokoll).
- Für (Fern-) Wartungstätigkeiten findet eine Zugriffsprotokollierung statt.
- In den EDV-Systemen sind Benutzeridentifikationen etabliert.
- Es findet eine Firewall-Protokollierung (TCP/IP) statt.
- Die Systeme sind so konfiguriert, dass eine Protokollierung der gescheiteten Anmeldeversuche stattfindet.
- Im Active Directory ist die Protokollierung der Benutzer aktiviert.

THERA-Trainer by medica Medizintechnik GmbH
Blumenweg 8 | 88454 Hochdorf
Tel +49 7355-93 14-0 | info@thera-trainer.com | www.thera-trainer.com

4.3 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 (bspw. USV und Notstromaggregat, Alarmanlage, redundante Datenspeicherung (RAID-Festplattensysteme), Firewalls, Virenschutzprogramme, mehrfache inkrementelle Datenbank- und Systembackups, Datensicherungskonzepte).

TT-cloud spezifische Maßnahmen:

Technische Maßnahmen zur Sicherstellung der Verfügbarkeit
Hochverfügbarkeit & Redundanz

- Nutzung von Azure Availability Zones & Region Replication, um den Betrieb auch bei Störungen sicherzustellen

Backup & Disaster Recovery

- Automatisierte, verschlüsselte Backups mit Azure Backup & Site Recovery
  - Tägliche Backups mit definierten Aufbewahrungsrichtlinien
  - Speicherung in Azure Blob Storage-Lösungen
- Disaster-Recovery-Strategien:
  - Regelmäßige Tests von Notfallplänen (Disaster-Recovery-Tests)
  - Einrichtung eines Business Continuity Plans (BCP) zur schnellen Wiederherstellung nach Ausfällen
  - Notfallhandbuch für Systemwiederherstellung

DDoS- und Angriffsschutz

- DDoS Protection Standard zur Abwehr von Überlastungsangriffen
- Firewall & Web Application Firewall (WAF) zur Sicherstellung der Verfügbarkeit von Cloud-Diensten

Organisatorische Maßnahmen zur Sicherstellung der Verfügbarkeit

- Definierte Notfallprozesse und Eskalationsstufen bei Systemausfällen
- Regelmäßige Schulungen für Administratoren und IT-Personal zur Notfallwiederherstellung
- Regelmäßige Überprüfung der Systemlast und Kapazitätsplanung

medica IT/Entwicklungs- spezifische Maßnahmen:

- Die personenbezogenen Daten sind ständig verfügbar und durch regelmäßige Datensicherungen gegen zufällige Zerstörung oder Verlust geschützt.
- Es ist ein Datensicherungskonzept mit regelmäßigen Backups aufgebaut. Die Backups werden in getrennten Bereichen sowie in verschlüsselter Form aufbewahrt.
- Es ist ein Backup-/Recoverykonzept ausgearbeitet und etabliert.
- Es ist ein Notfallhandbuch implementiert und wird regelmäßig aktualisiert.
- Die Serverräume/Rechenzentren sind über ein getrenntes Zutrittskontrollsystem besonders geschützt.
- Das Unternehmen verwendet Brandschutzvorrichtungen im Gebäude zur Sicherung der EDV-Systeme.
- Die Serverräume / Rechenzentren verfügen über redundante Stromzuführungen, sowohl georedundant als auch doppelte Netzteile.
- Die Serverräume / Rechenzentren haben eigene Überwachungssteme, welche direkt in der IT-Abteilung auflaufen.
- Es kommen unterbrechungsfreie Stromversorgung inkl. Überspannungsschutz und Notstromaggregat zum Einsatz.
- Im Serverraum / Rechenzentrum ist eine geeignete Löschanlage (Gaslöschanlage) vorhanden. Zusätzlich gibt es eine Feuer-/Rauchmeldeanlage.
- Das Gebäude und der Serverraum / Rechenzentrum verfügen über Blitzschutzeinrichtungen.

THERA-Trainer by medica Medizintechnik GmbH
Blumenweg 8 | 88454 Hochdorf
Tel +49 7355-93 14-0 | info@thera-trainer.com | www.thera-trainer.com

- Im Serverraum / Rechenzentrum kommt eine Klimaanlage zum Einsatz. Die Klimatechnik ist beim Unternehmen dokumentiert.
- Die Netzwerkkomponenten zum Zweck der Risiko-/Ausfallminimierung ist auf mehrere geschützten Bereiche verteilt.
- Es ist ein Überspannungsschutz integriert.
- Die eingesetzte Alarmanlage hat eine direkte Weiterleitung an die Leitstelle, den Werksschutz, die Feuerwehr, den Wachdienst etc.
- Im Serverraum / Rechenzentrum werden keine brennbaren Materialien/Gegenstände gelagert.
- Die Serverräume/das Rechenzentrum sind so konzipiert und geplant, dass keine wasserführenden Leitungen vorhanden sind.
- Die Serversysteme setzen RAID-Festplattensystemen ein, um eine Ausfallsicherheit zu gewährleisten.

4.3.1 Rasche Wiederherstellbarkeit

Anforderung: Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können. (Art. 32 Abs. 1 Hs. 2 lit. c) DSGVO)

TT-cloud spezifische Maßnahmen:

Backup- und Wiederherstellungsstrategie

- Automatisierte Datensicherung mit Azure Backup & Site Recovery
  - Tägliche automatisierte Backups mit Versionierung
  - Verschlüsselte Backups mit AES-256 und Schlüsselverwaltung via Azure Key Vault
- Wiederherstellung innerhalb definierter RTO- und RPO-Zeiten
  - Recovery Time Objective (RTO): Maximale Wiederherstellungszeit von 24h
  - Recovery Point Objective (RPO): Maximaler Datenverlust von 24h

Disaster Recovery & Notfallmanagement

- Azure Site Recovery für automatisierte Failover-Szenarien
  - Notfall-Wiederherstellungspläne für kritische Systeme
  - Failover in eine alternative Region bei kritischen Störungen
- Regelmäßige Tests der Wiederherstellung
  - Simulierte Disaster-Recovery-Tests mindestens einmal pro Jahr
  - Dokumentation und Optimierung der Wiederherstellungsprozesse
- Echtzeit-Monitoring mit Azure Monitor
  - Automatische Erkennung von Systemausfällen und Bedrohungen
  - Benachrichtigung von Administratoren & Eskalationsprozesse

Organisatorische Maßnahmen zur schnellen Wiederherstellung

- Notfallplan & Eskalationsrichtlinien für IT-Ausfälle
  - Definierte Verantwortlichkeiten & Kontaktketten im Notfall
  - Schulung von Mitarbeitern im Umgang mit Systemausfällen
  - Regelmäßige Audits & Reviews der Wiederherstellungsprozesse

medica IT/Entwicklungs- spezifische Maßnahmen:

- Es ist ein Backup vorhanden
- Es ist ein Backup-/Recoverykonzept ausgearbeitet und etabliert.

THERA-Trainer by medica Medizintechnik GmbH
Blumenweg 8 | 88454 Hochdorf
Tel +49 7355-93 14-0 | info@thera-trainer.com | www.thera-trainer.com

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

4.4.1 Datenschutz-Management

Das Unternehmen medica Medizintechnik GmbH betreibt ein Datenschutzmanagement-System (DSMS) nach den Vorgaben des Art. 5 Abs. 2 DSGVO. Es orientiert sich an dem PDCA-Zyklus und unterliegt damit einer dauerhaften Wirksamkeitsüberwachung.

4.4.2 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 von Vorfällen ist durch entsprechende Vertretungsregelungen sichergestellt.

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

Grundsätzlich werden nur Daten erhoben und verarbeitet, die für die Geschäftstätigkeiten zweckmäßig und erforderlich sind. Verfahren der automatisierten Datenerfassung- und -verarbeitung sind so gestaltet, dass nur die erforderlichen Daten erhoben werden können.

4.4.4 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (bspw. Verpflichtung auf die Vertraulichkeit bzw. Datengeheimnis, insbesondere der IT-Administratoren, Vertrag zur Auftragsverarbeitung nach Vorgabe des Art. 28 DSGVO, Sperrung der Zugriffe nach außen bspw. bei Fernwartung durch Externe, Vergabe restriktiver Zugriffsberechtigungen, Einbindung des Datenschutzbeauftragten/Informationssicherheitsbeauftragten etc.).

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.
- Auf die betreffenden technischen Umgebungen werden nur restriktive Zugriffsberechtigungen vergeben. Bei externem Zugriff auf das System wird der Zugang nach Beendigung der Zusammenarbeit deaktiviert oder gesperrt.
- Für die Übermittlung von personenbezogenen Daten an externe Dienstleister steht eine Vertragsvorlage zur Auftragsdatenverarbeitung zur Verfügung, die entsprechende Regelungen zur Kontrolle enthält.

THERA-Trainer by medica Medizintechnik GmbH
Blumenweg 8 | 88454 Hochdorf
Tel +49 7355-93 14-0 | info@thera-trainer.com | www.thera-trainer.com

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

4.5.1 Pseudonymisierung

Sofern eine direkte Personenbeziehbarkeit nicht erforderlich ist, wird von der Pseudonymisierung Gebrauch gemacht, wenn dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht (Datensparsamkeit).

Zudem werden Maßnahmen zu Privacy by design und Privacy by default, inkl. entsprechenden Schulungsmaßnahmen im Produktbereich, nach den Grundsätzen der Datenvermeidung und Datensparsamkeit umgesetzt.

4.5.2 Verschlüsselung auf Dateiebene:

(Bspw. Verschlüsselung von vertraulichen Dokumenten, verschlüsselte Übertragungswege via VPN, Aufbau Transportverbindung nur zwischen definierten und durch Zertifikate gesicherten Systemen, Datenübertragung von der Website erfolgt über eine SSL-Verschlüsselung).

- Es werden Verschlüsselungstechnologien nach dem aktuellen Stand der Technik eingesetzt. Das bedeutet, es kommen TLS(SSL)-Verschlüsselungen, Hash-Verschlüsselungen etc. zum Einsatz.

4.5.3 Verschlüsselung auf Hardwareebene:

(Bspw. Verschlüsselung von Festplatten in Notebooks, passwortgeschützte Hardware etc.).

Es werden Verschlüsselungstechnologien für die Hardwareebene nach dem aktuellen Stand der Technik eingesetzt (z.B. Bitlocker)

THERA-Trainer by medica Medizintechnik GmbH
Blumenweg 8 | 88454 Hochdorf
Tel +49 7355-93 14-0 | info@thera-trainer.com | www.thera-trainer.com

5 Kooperation

Zur Einhaltung der datenschutzrechtlichen Vorgaben nach der DSGVO, arbeitet das Unternehmen medica Medizintechnik GmbH mit der DDSK GmbH zusammen. Neben der Erstellung von Richtlinien und Handlungshilfen berät die DDSK GmbH das Unternehmen 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.

DDSK GmbH

Stefan Fischerkeller

Dr. Klein-Straße 29, 88069 Tettnang

Tel. 07542 / 949 21 00

E-Mail: datenschutz@thera-trainer.com

Web: www.ddsk.de

DDSK
DEUTSCHE
DATENSCHUTZKANZLEI

Maximilian Musch

Magister Artium, geprüfter fachkundiger Datenschutzbeauftragter (udis)

Deutsche Datenschutzkanzlei – Maximilian Musch

Richard-Wagner-Straße 2, 88094 Oberteuringen

Tel.: 07542 / 949 21 02

E-Mail: musch@ddsk.de

Web: www.ddsk.de