Vereinbarung zur Gemeinsamen Verantwortung über die Datenverarbeitung („Joint Control“)

zwischen
Universitätsklinikum Jena (UKJ)
vertreten durch den Klinikumsvorstand
Kastanienstraße 1
07747 Jena
– nachfolgend „UKJ“ –
und
mHealth Pioneers GmbH
Körtestraße 10
10967 Berlin
– nachfolgend „mHP“ –

– nachfolgend jeweils ein „Verantwortlicher“ und beide zusammen „die Verantwortlichen“ –

Präambel

Das UKJ und die mHP beabsichtigen zur wissenschaftlichen Erforschung der gesundheitlichen Langzeitfolgen von COVID-19, die unter dem Sammelbegriff „Long/Post COVID“ zusammengefasst werden, zusammenzuarbeiten. Das Krankheitsbild von Long COVID ist bislang nur unzureichend erforscht. Es ist mittlerweile jedoch unstreitig, dass die Gewinnung von weiteren Erkenntnissen über die Krankheitsbilder und die Therapierbarkeit von Long COVID dringend notwendig sind, um erkrankten Menschen eine gute gesundheitliche Versorgung und Unterstützung bei der Genesung von COVID-19 zu sichern.

Das UKJ beteiligt sich an der Erforschung und Behandlung von Long COVID unter anderem mit einer speziellen Long-COVID-Ambulanz, die Ärzt:innen und Expert:innen verschiedener Fachrichtungen einbezieht. Ein Ziel der klinischen Forschung des UKJ ist die Entwicklung eines Online-Programms zur Unterstützung von Patienten bei der Erholung von COVID-19.

Die mHP betreibt die Pulsatio-App (https://pulsatio.app). Mit Hilfe der Pulsatio-App können Teilnehmer:innen Vitaldaten, die mit Wearables (z. B. Fitnessarmbänder) gemessen werden, freiwillig für wissenschaftliche Studien und Projekte laufend zur Verfügung stellen. Die Pulsatio-App verfügt über eine Funktion zur Durchführung von In-App-Befragungen im Rahmen von sogenannten Teilprojekten. Die Teilnahme an Teilprojekten ist für die Nutzer:innen im Rahmen des WATCH-Projektes obligat. Die durch die Pulsatio-App ermöglichte kontinuierliche Erhebung von relevanten Vitaldaten und vergleichsweise einfache Durchführung von Befragungen nahezu ohne Zeitverzögerung in der derzeitigen Größenordnung ist bislang einzigartig. Daher soll die Pulsatio-App zukünftig verstärkt für die Erforschung von konkreten Fragestellungen zu Long COVID eingesetzt werden. Zugleich erlaubt dies der mHP weitere allgemeine Erkenntnisse zur Untersuchung von potenziellen Anwendungsfällen und den spezifischen Anforderungen beim Validieren von Mustererkennung und Entwicklung digitaler Biomarker für Long COVID.

Vor diesem Hintergrund beabsichtigen die beiden Verantwortlichen bei der Erforschung von Long COVID zusammenzuarbeiten. Dabei sollen die bei den beiden Verantwortlichen

jeweils vorhandenen spezifischen Kenntnisse und Fähigkeiten den wissenschaftlichen Fortschritt fördern und sowohl dem UKJ als auch der mHP die Gewinnung von neuen Erkenntnissen für die Corona-Forschung und insoweit auch die Erforschung von Long COVID ermöglichen. Konkret beabsichtigen die Parteien daher die Verbindung einer in der Post-COVID-Ambulanz des UKJ durchgeführten Projekts Mobile **W**ohnortn**A**he Versorgung zur Steuerung der sektorübergreifenden **T**herapie bei Post-**C**OVID-19 in T**H**üringen (WATCH) mit einer speziellen in der Pulsatio-App durchgeführten Teilprojekts zur Erfassung von "Wearable und Befragungsdaten“. Die Projektteilnehmer sind also Personen, die sowohl am WATCH-Projekt des UKJ teilnehmen als auch als Nutzer der Pulsatio-App an der entsprechenden Teilprojekts teilnehmen.

Das UKJ und die mHP haben die Mittel und Zwecke der beabsichtigen Forschungskooperation gemeinsam festgelegt und verstehen sich als gemeinsam Verantwortliche für die gemeinsame Datenverarbeitung im Rahmen der Forschungskooperation im Sinne des Art. 4 Nr. 7 DSGVO. Mit dieser Vereinbarung wollen die Verantwortlichen daher auch die sich aus der gemeinsamen Verantwortlichkeit ergebende Pflicht zur transparenten Regelung der jeweiligen Rechte und Pflichten der einzelnen Verantwortlichen gemäß Art. 26 Abs. 1 DSGVO erfüllen.

§ 1 Gegenstand der gemeinsamen Datenverarbeitung, Zuständigkeiten

(1) Die Verantwortlichen sind nach Maßgabe dieser Vereinbarung für die Datenverarbeitung bei der Durchführung des in der **Anlage 3** beschriebenen WATCH-Projekt gemeinsam Verantwortliche für die in diesem Rahmen stattfindende Verarbeitung personenbezogener Daten. Zur weiteren Beschreibung der gemeinsamen Verarbeitungsvorgänge sind dieser Vereinbarung auch die aktuellen Datenschutzhinweise für Projektteilnehmerer in der **Anlage 4** beigefügt, die Beschreibung in der Anlage 3 ergänzt.

Die gemeinsamen Verarbeitungsvorgänge im Zuständigkeitsbereich des UKJ werden auch als „Wirkbereich A" und die Verarbeitungsvorgänge im Zuständigkeitsbereich der mHP auch als „Wirkbereich B“ bezeichnet.

(2) Die unter die gemeinsame Verantwortlichkeit fallenden Verarbeitungsvorgänge umfassen ausschließlich die von den Wirkbereichen A und B umfassten Verarbeitungsvorgänge. Für Verarbeitungsvorgänge, die außerhalb dieser Wirkbereiche liegen, besteht keine gemeinsame Verantwortlichkeit im Anwendungsbereich dieser Vereinbarung.

(3) Soweit nachträgliche Änderungen der in **Anlage 3** oder **Anlage 4** beschriebenen Verarbeitungsvorgänge, Zwecke, Wirkbereiche, Zuständigkeiten oder sonstigen Umstände erfolgen sollen, haben die Verantwortlichen die betreffende Anlage unverzüglich anzupassen und die geänderte Anlage als neue und die entsprechende alte Anlage ersetzende Anlage schriftlich zu dieser Vereinbarung zu nehmen.

(4) Zur leichteren Verständlichkeit werden die von der gemeinsamen Verarbeitung betroffenen Personen in dieser Vereinbarung als „Projektteilnehmer“ bezeichnet. Klarstellend wird festgehalten, dass der Begriff des Projektteilnehmer in Einzelfällen auch Personen bezeichnen kann, die nicht am Watch-Projekt teilnehmen.

§ 2 Anlaufstelle für die betroffenen Personen

(1) Als primäre gemeinsame Anlaufstelle für die Geltendmachung des Rechts auf Löschung aus Art. 17 DSGVO benennen die Verantwortlichen die in der Datenschutzerklärung (**Anlage 4**) benannten Ansprechpartner bei den jeweils zuständigen Verantwortlichen.

(2) Ungeachtet des Absatzes 1 können die Projektteilnehmer die ihnen gegebenenfalls zustehenden Betroffenenrechte in Bezug auf die gemeinsame Datenverarbeitung gegenüber jedem Verantwortlichen geltend machen.

§ 3 Laufzeit dieser Vereinbarung

Die Laufzeit dieser Vereinbarung entspricht der Dauer der gemeinsamen Datenverarbeitung.

§ 4 Art der Daten

Die Datenarten, die Gegenstand der gemeinsamen Datenverarbeitung sind, ergeben sich aus der Datenschutzerklärung (**Anlage 4)**. Den Verantwortlichen ist bekannt, dass die gemeinsame Datenverarbeitung auch die Verarbeitung von Patientendaten und Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DSGVO umfasst, so dass ein entsprechend hoher Schutzbedarf besteht.

§ 5 Kreis der Betroffenen

Der Kreis der von der gemeinsamen Datenverarbeitung betroffenen Personen umfasst Personen, die an der in der Post-COVID-Ambulanz des UKJ durchgeführten Watch-Projekt teilnehmen oder teilgenommen haben und während ihrer Teilnahme in der Pulsatio-App der mHP am zugehörigen Teilprojekt teilnehmen oder teilgenommen haben.

§ 6 Wahrung der Betroffenenrechte

(1) In Bezug auf die gemeinsame Datenverarbeitung stehen den Projektteilnehmern die Rechte aus den Art. 15 bis 20 DSGVO zu („Betroffenenrechte“), zudem können die Projektteilnehmer die von Ihnen gegenüber dem UKJ und der mHP jeweils erteilten Einwilligungen widerrufen (Art. 7 Abs. 3 S. 4 DSGVO). Klarstellend wird festgehalten, dass den Projektteilnehmern nach Auffassung beider Verantwortlichen kein Widerspruchsrecht gem. Art. 21 DSGVO zusteht, da kein gemeinsamer Verarbeitungsvorgang auf die Rechtsgrundlage des Art. 6 Abs. 1 Buchstaben e oder f DSGVO gestützt werden wird. Jeder Verantwortliche verpflichtet sich, den Auskunfts-, Berichtigungs- oder sonstigen Betroffenenanträgen, soweit eine Pflicht zur Gewährleistung des Betroffenenrechts besteht, nachzukommen.

(2) Die Beantwortung von Betroffennanträgen (z.B. Auskunftersuchen, Löschaufforderungen, Widerrufserklärungen) erfolgt grundsätzlich durch den Verantwortlichen, an den der Projektteilnehmer das betreffende Ersuchen adressiert hat.

(3) Wenn nichts anderes vereinbart ist, beantwortet der vom Projektteilnehmer adressierte Verantwortliche das Ersuchen gegenüber dem Projektteilnehmer unverzüglich, spätestens aber innerhalb eines Monats (Art. 12 Abs. 3 DSGVO). Falls die Beantwortung unter Berücksichtigung der Komplexität und der Anzahl von Betroffenenanträgen eine längere Zeit in Anspruch nimmt, informiert der adressierte Verantwortliche den Projektteilnehmerer und den anderen Verantwortlichen über diesen Umstand und beantwortet das Ersuchen binnen eines angemessenen Zeitrahmens, der dem Projektteilnehmer unverzüglich – d. h. vor der verzögerten eigentlichen Beantwortung des Betroffenenantrags – mitzuteilen ist.

(4) Erhält ein Verantwortlicher einen Betroffenenantrag direkt von einem Projektteilnehmer, so unterrichtet er den anderen Verantwortlichen unverzüglich schriftlich oder in Textform. Jeder Verantwortliche trifft geeignete Maßnahmen, um dem jeweils anderen Verantwortlichen alle Informationen für die Erfüllung der Betroffenenrechte zur Verfügung zu stellen, soweit die Informationen von dem anderen Verantwortlichen nicht selbst identifiziert oder abgerufen werden können.

(5) Sollen personenbezogene Daten gelöscht werden, informieren sich die Verantwortlichen zuvor gegenseitig. Der jeweils andere Verantwortliche kann der Löschung aus berechtigtem Grund widersprechen, etwa sofern ihn eine gesetzliche Aufbewahrungspflicht trifft.

(6) Für die Erfüllung von etwaigen Mitteilungspflichten gemäß Art. 19 DSGVO im Zusammenhang mit einem Betroffenentrag ist der Verantwortliche zuständig, der gemäß Abs. 4 für die Beantwortung des jeweiligen Betroffenenantrags zuständig ist.

§ 7 Informationspflichten gegenüber den Betroffenen

(1) Die Verantwortlichen erfüllen in ihren jeweiligen Wirkbereichen alle sich aus der DSGVO ergebenden Informationspflichten in Bezug auf die gesamte gemeinsame Datenverarbeitung gegenüber dem betroffenen Projektteilnehmer nach Maßgabe dieses § 7.

(2) Zur Erfüllung der Informationspflichten in Bezug auf die gemeinsame Datenverarbeitung haben sich die Verantwortlichen über einheitliche Datenschutzhinweise für die Projektteilnehmer verständigt, die in der **Anlage 4** beigefügt sind („einheitliche Datenschutzhinweise"). Die Verantwortlichen gehen davon aus, dass diese einheitlichen Datenschutzhinweise alle gemäß Art. 13, 14 und 26 Abs. 2 S. 2 DSGVO den Projektteilnehmer in Bezug auf die gemeinsame Datenverarbeitung eventuell mitzuteilenden Informationen umfassen. Die Verantwortlichen verpflichten sich, im Rahmen ihrer jeweiligen Informationspflichten die einheitlichen Datenschutzhinweise zu verwenden, soweit dies im Einzelfall möglich und sachgerecht ist.

(3) Das UKJ stellt den Projektteilnehmern die einheitlichen Datenschutzhinweise im Rahmen der allgemeinen Projektinformationen und jedenfalls vor der Einholung der Teilnahmeerklärung des Projektteilnehmerers in Papier- und/oder ausdruckbarer elektronischer Form (z. B. als PDF-Datei oder als Webseite) zur Verfügung.

(4) Die mHP stellt den Projektteilnehmern die einheitlichen Datenschutzhinweise im Rahmen der Beschreibung des Teilprojekts in der Pulsatio-App zur Verfügung, wie dies auch bei den bisher durchgeführten Projekten erfolgt. Zusätzlich werden die einheitlichen Datenschutzhinweise von der mHP auf der offiziellen Website der Pulsatio-App (https://pulsatio.app/) bereitgestellt.

(5) Jeder Verantwortliche darf neben den einheitlichen Datenschutzhinweisen zusätzliche Datenschutzinformationen zu gemeinsamen Verarbeitungsvorgängen bereitstellen, sofern dies aus Transparenzgründen zweckmäßig erscheint (bspw. in Form von FAQs). Derartige zusätzliche Datenschutzinformationen dürfen nicht im Widerspruch zu den einheitlichen Datenschutzhinweisen stehen. Die Verwendung von zusätzlichen Datenschutzinformationen ist nicht Gegenstand der gemeinsamen Datenverarbeitung. Verantwortlich ist daher ausschließlich der Verantwortliche, der die zusätzlichen Datenschutzinformationen verwendet.

§ 8 Melde- und Benachrichtigungspflichten, Datenschutz-Folgenabschätzung und vorherige Konsultation, Verarbeitung zu anderen Zwecken

(1) Im Falle einer tatsächlichen oder vermuteten Verletzung des Schutzes personenbezogener Daten („Datenschutzvorfall") wird der betroffene Verantwortliche den anderen Verantwortlichen unverzüglich in Textform über den Datenschutzvorfall in Kenntnis setzen. Die Benachrichtigung beschreibt präzise die Art der (vermuteten) Verletzung des Schutzes personenbezogener Daten, einschließlich ihrer voraussichtlichen Folgen.

(2) Im Falle eines Datenschutzvorfalls arbeiten die Verantwortlichen nach Treu und Glauben zusammen, um die Umsetzung ihrer datenschutzrechtlichen Verpflichtungen zu erreichen, und stellen sicher, dass die Meldung an die zuständige(n) Aufsichtsbehörde(n) oder die vom Datenschutzvorfall betroffenen Projektteilnehmern innerhalb von 72 Stunden nach Kenntnisnahme der Verletzung personenbezogener Daten erfolgt.

(3) Die Verantwortlichen führen gemeinsam eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO („DSFA") für die gemeinsame Datenverarbeitung durch.

(4) Jeder Verantwortliche stellt dem anderen Verantwortlichen für die Zwecke der gemeinsamen DSFA nach Abs. 3 und zur allgemeinen datenschutzrechtlichen Bewertung und ordnungsgemäßen Dokumentation der gemeinsamen Datenverarbeitung erforderlichen Informationen aus seinem Wirkbereich zur Verfügung und dokumentiert die Ergebnisse und festgestellten Folgen der gemeinsamen DSFA.

(5) Der Prüfgegenstand der gemeinsamen DSFA nach Abs. 3 umfasst keine Verarbeitungsvorgänge oder sonstigen Umstände, die außerhalb der Wirkbereiche A oder B

liegen. Soweit solche außerhalb der gemeinsamen Datenverarbeitung liegenden Umstände für die Bewertung der von der gemeinsamen Datenverarbeitung geschaffenen Datenschutzrisiken im Allgemeinen oder im Rahmen der gemeinsamen DSFA sachdienlich sind (im Sinne von Kontextinformationen, die einem nicht vorbefassten Leser das Verständnis des Verarbeitungszwecks oder das Nachvollziehen von DSFA-Ergebnissen erleichtern oder erst ermöglichen), umfasst die Pflicht zur Informationsbereitstellung nach Abs. 4 auch Informationen zu außerhalb der gemeinsamen Datenverarbeitung liegenden Umständen.

(6) Soweit für einen außerhalb der gemeinsamen Verantwortung liegenden Verarbeitungsvorgang bereits eine DSFA durchgeführt worden ist, auf deren Ergebnisse sich ein Verantwortlicher zur Erfüllung seiner Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO ganz oder teilweise beruft („vorbestehende DSFA“), umfasst die Pflicht dieses Verantwortlichen zur Informationsbereitstellung nach Abs. 4 auch die Zurverfügungstellung der relevanten wesentlichen Dokumentation der vorbestehenden DSFA für den anderen Verantwortlichen. Als wesentliche Dokumentation gelten die dem anderen Verantwortlichen nicht bereits vorliegenden Informationen, die ihm die Überprüfung und ggf. Verwertung der relevanten Ergebnisse der vorbestehenden DSFA im Rahmen der Dokumentation oder Bewertung der gemeinsamen Datenverarbeitung ermöglichen. Dies erfordert mindestens die Zurverfügungstellung des Prüfgegenstands der vorbestehenden DSFA sowie eine nachvollziehbare Risikoanalyse. Aus dieser Vereinbarung folgt keine vertragliche Pflicht eines Verantwortlichen, für außerhalb der gemeinsamen Verantwortung liegende Verarbeitungsvorgänge eine diesbezügliche DSFA durchzuführen.

(7) Die mHP stellt dem UKJ während der Dauer der gemeinsamen Verantwortlichkeit den jeweils aktuellen DSFA-Bericht bzw. die wesentliche Dokumentation der vorbestehenden DSFA für die Pulsatio-App in Textform unaufgefordert zur Verfügung, soweit diese für die sachgerechte Bewertung der mit der gemeinsamen Datenverarbeitung verbundenen Datenschutzrisiken notwendig sind. Mit der Zurverfügungstellung gilt die Pflicht der mHP zur Informationsbereitstellung nach Abs. 4 in Bezug auf die Datenverarbeitungsvorgänge im Rahmen der Pulsatio-App als erfüllt.

Die zum Zeitpunkt des Abschlusses dieser Vereinbarung aktuelle Version des DSFA-Berichts für die Pulsatio-App (Version 2.2 vom 20.06.2022) liegt dem UKJ vor.

(8) Plant ein Verantwortlicher nachträglich, d. h. nach Beendigung der gemeinsamen Datenverarbeitung, die im Rahmen der gemeinsamen Verantwortung erhobenen personenbezogenen Daten für einen anderen als den Projektteilnehmern im Rahmen der einheitlichen Datenschutzhinweise 4 mitgeteilten Zwecken zu verarbeiten, ist dies grundsätzlich gemäß den gesetzlichen Vorgaben für Zweckänderungen (insbesondere Art. 6 Abs. 4 DSGVO) zulässig. Klarstellend wird festgehalten, dass eine solche Verarbeitung zu anderen Zwecken durch einen Verantwortlichen ausschließlich in dessen eigener Verantwortlichkeit und somit außerhalb der gemeinsamen Datenverarbeitung erfolgen kann und grundsätzlich eine Information der betroffenen Projektteilnehmern über die weitere Verarbeitung gemäß Art. 13 bzw. 14 DSGVO erfordert. Während der Dauer der gemeinsamen Datenverarbeitung ist eine Zweckänderung nur bei einer entsprechenden Änderung dieser Vereinbarung nach Maßgabe des § 1 Abs. 3 zulässig.

§ 9 Beiderseitige, nicht aufteilbare Verpflichtungen aus der DSGVO

(1) Jeder Verantwortliche hat geeignete technische u. organisatorische Maßnahmen in seinem Wirkbereich zu ergreifen, welche ein dem Schutzbedarf der Daten angemessenes Schutzniveau in Bezug auf die gemeinsame Datenverarbeitung gewährleisten. Hiervon ist u.a. die Fähigkeit umfasst, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme auf Dauer sicherzustellen. Die Herstellung eines angemessenen Sicherheitsniveaus im eigenen Wirkbereich ist Aufgabe jedes einzelnen Verantwortlichen.

(2) Da die gemeinsame Datenverarbeitung in beiden Wirkbereichen jeweils besondere Datenkategorien nach Art. 9 Abs. 1 DSGVO umfasst (insbesondere Gesundheitsdaten bzw. Patientendaten), gehen die Verantwortlichen in Bezug auf sämtliche im Rahmen der gemeinsamen Datenverarbeitung verarbeiteten Daten von einem hohen Schutzbedarf aus und verpflichten sich in ihrem Wirkbereich jeweils mindestens zur Umsetzung von zur Gewährleistung des hohen Schutzbedarfs von Gesundheits- und Patientendaten entsprechenden Maßnahmen. Eine verbindliche, aber nicht abschließende Festlegung konkreter technisch-organisatorischer Maßnahmen erfolgt in den **Anlagen 1 (UKJ) und 2 (mHP)**.

(3) Die Wahrung des Datengeheimnisses ist durch die Verantwortlichen in ihrem jeweiligen Wirkbereichen sicherzustellen. Alle für die Verantwortlichen handelnden Personen, die auf personenbezogene Daten der Projektteilnehmern zugreifen können, müssen auf das Datengeheimnis und die Vertraulichkeit verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Zweckbindung belehrt werden.

(4) Jeder Verantwortliche hat ein eigenes Verzeichnis über die gemeinsamen Verarbeitungstätigkeiten zu führen.

(5) Im Übrigen ist jeder Verantwortliche im Hinblick auf die sich aus der gemeinsamen Datenverarbeitung ergebenden Verpflichtungen aus den Regelungen der DSGVO und anderer anwendbarer Vorschriften über den Datenschutz selbst verantwortlich.

§ 10 Unterauftragsverhältnisse

(1) Die Einschaltung von Unterauftragnehmern ist (beidseitig) grundsätzlich nur mit vorheriger gegenseitiger schriftlicher Zustimmung gestattet. Die Zustimmung darf von keinem Verantwortlichen unbillig verweigert werden. Sämtliche vertragliche Vereinbarungen mit dem/den Unterauftragnehmer/n sind so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen den Verantwortlichen entsprechen. Für die in der **Anlage 7** genannten Unterauftragnehmer gilt die Zustimmung des anderen Verantwortlichen nach Satz 1 als erteilt.

(2) Bei der Unterbeauftragung sind dem anderen Verantwortlichen Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung beim Unterauftragnehmer einzuräumen. Dies umfasst auch die Pflicht des Verantwortlichen, der sich zum Einsatz eines oder mehrerer Unterauftragnehmer entscheidet, auf schriftliche Anforderung des anderen Verantwortlichen im Rahmen dieser Vereinbarung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis zu geben.

§ 11 Haftung u. uneingeschränkte Verantwortlichkeit gegenüber Betroffenen

(1) Nach Art. 26 Abs. 3 und Art. 82 Abs. 4 DSGVO kann im Falle von Schadenersatzansprüchen eines Projektteilnehmers jeder der Verantwortlichen für den gesamten Schaden haften, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist. Hat nach den vorgenannten Vorschriften einer der Verantwortlichen einer betroffenen Person Schadensersatz für den erlittenen Schaden gezahlt, so ist dieser Verantwortliche gemäß Art. 82 Abs. 5 DSGVO berechtigt, von dem anderen Verantwortlichen den Teil des

Schadensersatzes zurückzufordern, der seinem jeweiligen Anteil an der Verantwortung für den Schaden entspricht.

(2) Ergänzend gelten die gesetzlichen Regelungen zur Gesamtschuld.

§ 12 Schlussbestimmungen

(1) Diese Vereinbarung besteht aus diesem Dokument und den darin in Bezug genommenen Anlagen.

(2) Bestandteile Änderungen und Ergänzungen dieser Vereinbarung – einschließlich etwaiger Zusicherungen durch einen Verantwortlichen – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Es gilt das Recht der Bundesrepublik Deutschland.

§ 13 Salvatorische Klausel

(1) Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam oder undurchführbar sein oder nach Vertragsschluss unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit dieser Vereinbarung im Übrigen unberührt.

(2) An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll diejenige wirksame und durchführbare Regelung treten, deren Wirkungen der (datenschutz-)rechtlichen Zielsetzung am nächsten kommen, welche die Verantwortlichen mit der unwirksamen bzw. undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich diese Vereinbarung als lückenhaft erweist.

Für die mHP:

_____ _____

Ort, Datum Stempel/ Unterschrift

Für das UKJ:

_____ _____

Ort, Datum Stempel/ Unterschrift

_____ _____

Ort, Datum Stempel/ Unterschrift

Anlage 1 Technisch-organisatorische Maßnahmen des UKJ gemäß Art. 32 DSGVO

Anlage 1 entspricht Anhang 5 zum Datenschutzkonzept (Anlage 9 zum Vertrag nach § 140a SGB V über eine WohnortnAhe Versorgung zur Steuerung der sektorenübergreifenden Therapie bei Post-COVID-19 in THüringen (WATCH) vom 01.11.2023)

Technisch-organisatorische Maßnahmen des UKJ gemäß Art. 32 DSGVO

a) Technisch-organisatorische Maßnahmen des UKJ

Das UKJ betreibt ein Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001:2013 und ist mit dem Geltungsbereich "Bereitstellung von IT-Verfahren, zur Betreibung von kaufmännischen und klinischen Prozessen, die zur Sicherstellung der medizinischen Dienstleistung beitragen." zertifiziert.

Für alle Datenverarbeitungsprozesse, die auf zentralen IT-Systemen des UKJ durchgeführt werden, gelten die allgemeinen technischen und organisatorischen Maßnahmen aus dem Annex A der ISO/IEC 27001. Diese sind nachfolgend dargestellt:

Tabelle 1: Allgemeine technische und organisatorische Maßnahmen des UKJ

Technisch Organisatorischen Maßnahmen des UKJ

			betrifft Schutzziel				
gem. Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO	**Maßnahmen im UKJ**	**Art**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Transparenz**	**Nachweis / Verknüpfung zur ISO27001**
Pseudonymisierung und Verschlüsselung personenbezogener Daten	Einsatz von VPN-Technologie für die sichere Datenübertragung mit externen Partnern oder Einrichtungen	technisch	x		x		A.13.1
	Bereitstellung externer Web-Dienste über verschlüsselte Kanäle (https, sftp etc.)/Sicherung von Anwendungsdiensten in öffentlichen Netzwerken	technisch	x	x	x		A.14.1.2

		Richtlinie zur Kryptographie/ Kryptographische Maßnahmen	organisatorisch / technisch	x				A.10.1
		Anweisung der Mitarbeiter auf Verschlüsselung externer Datenträger/Notebooks bei Verarbeitung/Transport personenbezogener Daten	organisatorisch	x		x		IT-Nutzerordnung A.6.2.1
		Anforderungen zur Pseudonymisierung	organisatorisch / technisch	x				*s. Tabelle 2*
die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen	Zutritts-kontrolle (Räume)	Sicherheitszonenkonzept für Räumlichkeiten, in denen sensible Informationen verarbeitet werden	organisatorisch			x	x	A.11.1
		zutrittsgesicherter Bereich (Schließung Toska/Schlüssel)	organisatorisch / technisch			x		A.11.1
		Zutrittsrechte werden regelmäßig überprüft und sofern erforderlich, wieder entzogen	organisatorisch				x	A.11.1
		Regelung für Arbeiten in Sicherheitsbereichen	organisatorisch	x		x		A.11.1
		Anforderungen zur Platzierung und Schutz von Geräten und Betriebsmitteln	organisatorisch / technisch	x		x		A.11.2
	Zugangs-kontrolle	Zentrale Zugangssteuerung	organisatorisch / technisch	x	x	x		A.9.1
		Verwendung sicherer Passwörter	organisatorisch / technisch	x				IT-Nutzerordnung
		Zugangssicherung zu Netzwerken und Netzwerkdiensten	organisatorisch / technisch	x	x	x		A.9.1
		Zentrale Benutzerzugangsverwaltung/ Benutzerverantwortlichkeiten	organisatorisch / technisch	x	x	x		A.9.2/ A.9.3
		Zentrale Netzwerksteuerungsmaßnahmen	organisatorisch / technisch	x	x	x		A.13.1

		Verwaltung privilegierter Zugangsrechte	organisatorisch	x	x			A.13.1
		Authentifizierungsschutz bei externen Netzwerkzugriffen	technisch	x	x			A.13.1
		Sensibilisierungs- und Schulungsmaßnahmen für Mitarbeiter	organisatorisch				x	A.7.2
		Anweisung der Mitarbeiter keine personenbezogenen Daten lokal zu speichern	organisatorisch	x				IT-Nutzerordnung
	Trennungs-kontrolle	Trennung von Produktiv- und Testumgebungen	organisatorisch / technisch	x		x		A.12.1
		physische und logische Netzwerktrennung durch Router- und Firewallsysteme	organisatorisch / technisch	x		x		A.13.1
		Steuerung über Berechtigungskonzept	organisatorisch / technisch	x			x	A.9.1
		Einschränkungen von Softwareinstallationen	organisatorisch / technisch	x	x	x		A.12.6.2/ IT-Nutzerordnung
	Verfügbarkeits-kontrolle	Brand- und Einbruchmeldeanlagen	technisch			x		A.11.1
		Feuerlöschanlagen	technisch			x		A.11.1
		redundante Stromversorgung bei zentralen Komponenten (USV)	technisch			x		A.17.2
		Kapazitätssteuerung (Systemmonitoring)	organisatorisch / technisch			x		A.12.1
		Changemanagement	organisatorisch			x		A.12.1
		Maßnahmen gegen Schadsoftware	technisch		x	x		A.12.2
		Zentrale Steuerung von Software im Betrieb (Softwaremanagement)	organisatorisch / technisch		x	x		A.12.5
		Handhabung technischer Schwachstellen	organisatorisch / technisch	x		x		A.12.6

	Weitergabekontrolle	Datenschutzbelehrungen bei Umgang mit personenbezogenen Daten (Verschlüsselungsmethoden für externe Weitergabe)	organisatorisch	x				A.7.2
		Regelungen zur Informationsübertragung	organisatorisch /technisch	x	x			A.13.2
		Einsatz von VPN-Technologie für die sichere Datenübertragung mit externen Partnern oder Einrichtungen (inkl. Zwei-Faktorauthentifizierung)	organisatorisch / technisch	x		x		A.13.1
	Eingabe-kontrolle	Ereignisprotokollierung (Administrator-/Bedienerprotokolle)	technisch	x	x		x	A.12.4
		Zugriffsprotokollierung bei hochsensiblen Datenzugriffen	technisch	x	x		x	A.12.4
		Klare Zuständigkeit für Löschung	organisatorisch	x			x	*s. Tabelle 2*
die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen		Aufrechterhalten der Informationssicherheit durch Business-Continuity-Management (IT-Notfallmanagement)	organisatorisch / technisch			x		A.17
		Zentrales IT-Servicemanagement (Incidentmanagement)	organisatorisch / technisch			x		A.16.1
		Maßnahmen zur Handhabung Informations-/IT-Sicherheitsvorfällen	organisatorisch / technisch	x	x	x		A.16.1
		Zentrale Datensicherung (Backupkonzept) - Aufbewahrung in unterschiedlichen Brandabschnitten	organisatorisch / technisch			x		A.12.3
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der		regelmäßige interne und externe Audits bzgl. Zertifizierung der ISO9001 und ISO27001 (inkl. Datenschutz/Compliance)	organisatorisch	x	x	x	x	Normkapitel 9 (ISO/IEC 27001)

Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung	stichprobenartige Kontrollen auf Datenschutz durch DSB/ISB in den Einrichtungen	organisatorisch	x	x	x	x	A.12.7

Anlage 2: Technisch-organisatorische Maßnahmen der mHP gemäß Art. 32 DSGVO

Technisch-organisatorische Maßnahmen zur Datensicherheit (Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste) der mHP (Applikation der Pulsatio-App)

Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren – *z.B.: Zutrittskontrollsystem, Ausweisleser, Magnetkarte, Chipkarte, Schlüssel, Schlüsselvergabe, Werkschutz, Pförtner, Überwachungseinrichtung, Alarmanlage, Türsicherung*

Unbefugten Personen ist der Zugriff auf Datenverarbeitungssysteme aus Büros und Rechenzentren des Unternehmens durch folgende Maßnahmen erschwert:
<u>Rechenzentrum:</u>

- Zutrittsvereinzelung
- Anmeldung notwendig
- Personalausweis und persönliche PIN notwendig
- Dauerhafte Begleitung durch Rechenzentrumsmitarbeiter
- Racks werden pro Kunde vergeben, sind verschlossen und können nur durch autorisierte Personen geöffnet werden

<u>Büroumgebung:</u>
Der Sitz der mHP befindet sich in einem Bürogebäude in Berlin Kreuzberg. Die Eingänge zum Büro sind mit je zwei Türen geschützt. Ein automatisches Alarmsystem überwacht Türen und Bewegungen. Weitere Maßnahmen:

- Eingangstüren sind grundsätzlich verschlossen.
- Fenster sind zu schließen sobald sich kein Mitarbeiter im Raum befindet.
- Sobald der Arbeitsplatz verlassen wird, ist der Bildschirm zu sperren, so dass nur mit erneuter Eingabe des individuellen Passworts Zugriff auf die IT-Infrastruktur erlangt werden kann.

Bei Besuch externer Parteien ist der jeweils Termin-Verantwortliche dafür verantwortlich, dass der Besuch innerhalb der Büroräume stets begleitet wird.

Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können – *z.B.: Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren (Beispiele: Kennwortverfahren, Automatische Sperrung, Einrichtung eines Benutzerstammsatzes pro User, Verschlüsselung von Datenträgern)*

Die mHP nutzt die folgenden Maßnahmen, um zu verhindern, dass nicht autorisierte Personen die Datenverarbeitungsanlagen für die Verarbeitung oder Nutzung personenbezogener Daten verwenden:
Die mHP stellt für Mitarbeiter, falls erforderlich, über einen eigenen Mitarbeiterzugang Zugang zu den Systemen/Services von der mHP her. Die Zugangsrechte beschränken sich dabei auf die Verantwortlichkeiten des jeweiligen

Mitarbeiters bzw. Teams. Bei Ausscheiden eines Mitarbeiters wird der entsprechende Account sofort deaktiviert.
Den Zugang zu den eigenen Systemen regelt die mHP über Passwortverfahren (Webauthentication sowie individuell) sowie den Einsatz eines VPNs.
Administratorzugang zu zugrundeliegenden Servern ist nur per SSH möglich.
Außerdem hat die mHP eine Vorschrift zur Erstellung von Passwörtern erlassen. So wird eine hohe Sicherheit auch bei Systemen gewährt, die einen passwortbasierten Zugang bieten. Die Passwörter müssen die folgenden Eigenschaften erfüllen:

- Mindestens 8 Stellen
- Mischung aus Groß- und Kleinbuchstaben sowie Zahlen
- Passwörter dürfen nicht notiert werden
- Passwörter werden nicht an Dritte weitergegeben
- Sollte der Verdacht oder die Möglichkeit bestehen, dass Dritte Kenntnis von Passwörtern erlangt haben, sind diese unverzüglich zu ändern

Das Kommunikationsnetz des Unternehmens wird mit Sicherheitsmaßnahmen nach aktuellem Stand abgesichert. Dazu gehören:

- Verbindungen vom internen Netz zum externen Netz sind durch Firewall-Systeme (z. B. Router, Gateways etc.) geschützt.
- Verbindung nach außen sind nur nach Bedarf ausgehend aufzubauen – nach innen gerichtete Verbindungsaufbauten sind nicht zulässig.
- Deaktivierung aller Funktionalitäten (Dienste, Ports etc.) der Firewall-Komponenten, die nicht für die Internet-Kommunikation benötigt werden.

Für die Kommunikation mit internen Diensten (bspw. Wissensdatenbank, Ticket-Management-System etc.) müssen externe Geräte über ein VPN mit individuellem Zugang mit unserem Netz verbunden sein.

Zugriffskontrolle
Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können – *z.B.: Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren](Beispiele: differenzierte Berechtigungen wie Profile, Rollen etc. Auswertungen, Kenntnisnahme, Veränderung, Löschung)*

Die mHP implementiert die folgenden Maßnahmen, um sicherzustellen, dass diejenigen, die autorisiert sind ein Datenverarbeitungssystem zu verwenden, nur auf Daten in Übereinstimmung mit ihrer Zugriffsberechtigung zugreifen können, und dass personenbezogene Daten während der Verarbeitung und Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:
<u>Workstations:</u>
Jeder Zugriff auf das unternehmensinterne Netzwerk bzw. Unternehmensgeräte und Rechner ist ausschließlich durch einen individuellen Zugang mit entsprechendem Passwort möglich.
Passwortrichtlinien: siehe Zugangskontrolle
Festplatten sind verschlüsselt (bspw. VeraCrypt), um nur autorisierten Personen Zugriff zu gewähren und auch bei physischem Verlust Datensicherheit zu gewährleisten.
<u>Verwaltungsplattform:</u>

Kundendaten können im System prinzipiell nur über zwei Wege eingesehen werden:

1. Backoffice (Zugriff auf Daten mehrerer Nutzer, abhängig von den individuellen Account-Zugriffsrechten)
- Zugriff auf Daten erfolgt über mehrstufiges Authentifizierungssystem
    - Zugriff auf Anmeldeoberfläche des Systems nur über VPN/IP-restriction & Web-Auth.
    - Zugriff auf Backend-Daten nur nach erfolgreicher Anmeldung am System durch individuellen Login.
    - Pro individuellem Login sind genau zugeschnittene Zugriffsrechte auf Kundendaten im Backend definiert.
    - Nutzerrechte werden über Nutzergruppenrechte zugewiesen und verwaltet – von Nutzergruppen abweichende Rechte werden vermieden.
    - Alle Nutzer und Nutzergruppen mit Zugang zu beiden Systemebenen werden in einer strukturierten Liste aufgeführt, Zugänge werden bei bspw. Ausscheiden aus dem Unternehmen unverzüglich deaktiviert.
    - Aktionen innerhalb des Backoffice werden nutzerbezogen gespeichert und erlauben eine Nachverfolgung-
- Die strikte Trennung der im Auftrag durch den Auftraggeber verarbeiteten Daten von den anderen durch die mHP verarbeiteten Daten wird über eine logische Mandantentrennung innerhalb des Systems sichergestellt.
- Mitarbeiter von Kunden der mHP erhalten im Zuge dieser Mandantentrennung jeweils ausschließlich Zugriff auf die Daten ihrer Nutzer (d.h. derjenigen Nutzer, deren Daten auf Grundlage des Leistungsvertrags des jeweiligen Kunden mit der mHP entstanden sind).
- Jede fehlerhafte Passworteingabe wird aufgezeichnet.

2. Datenbank (speichert alle Informationen)
- Zugriff auf die Datenbank ist nur durch die Persistenzplattform bzw. über den Server möglich:
    - Zugriff nur über VPN/IP-restriction
    - Zugriff erfordert individuelles Login
    - Zugriff wird nur begrenztem Personenkreis (Administratoren bzw. verantwortliche Entwickler) gewährt
- Physischer Zugriff auf die Datenbank ist durch Haftungs- und Datenschutzkonzept des Housingdienstleisters begrenzt:
    - Firmensitz und Rechenzentrum des Housingdienstleister liegen in Deutschland und unterliegen damit den deutschen Datenschutzbestimmungen.
    - Rechenzentrumsmitarbeiter sind auf Datenschutz verpflichtet.
- Persönliche Informationen (Name, Vorname, Adresse) werden als Hashes (salted MD5 bzw. SHA3) in einer separaten Tabelle gespeichert.

Zugriff auf sensible Daten
- Sensible Daten dürfen nicht außerhalb der Verwaltungsplattform (bspw. lokale Workstation etc.) gespeichert werden.
- Gesundheitsdaten dürfen nur pseudonymisiert lokal gespeichert werden.

- Zugriff auf pseudonymisierte Daten ist nur einem beschränkten und genau definierten Personenkreis gewährt.

Weitergabekontrolle
Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern 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 - *z.B.: Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren, elektronische Signatur*

Das Ziel der Weitergabekontrolle ist es sicherzustellen, dass personenbezogene Daten bei der elektronischen Übertragung, dem Transport oder während der Aufzeichnung auf Datenspeichergeräten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Außerdem soll sichergestellt werden, dass es möglich ist zu ermitteln und zu prüfen, an welche Stellen personenbezogene Daten gesandt werden. Die mHP regelt die Übermittlung personenbezogener Daten in Bezug auf die elektronische Übertragung, Datentransport, Transfer-Checks usw. mit folgenden Maßnahmen:
Überschneidung mit Zugriffskontrolle, siehe oben.
Vertragliche Datenschutzverpflichtungen:
- Die mHP verpflichtet alle Parteien, mit denen eine Zusammenarbeit besteht und die ggf. Zugriff auf Daten bekommen könnten, auf das Datengeheimnis und die Einhaltung der unternehmenseigenen Datenschutz-Richtlinie.
- Umfang und Art des Datenzugriffs wird darüber hinaus vertraglich festgelegt.
- Mitarbeiter müssen eine Datenschutzbelehrung absolvieren und am ersten Arbeitstag eine DS-Verpflichtung unterschreiben

Eingabekontrolle
Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind - *z.B.: Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung gewährleisten, etwa durch Protokollierungs- und Protokollauswertungssysteme*

Die mHP gewährleistet durch folgende Maßnahmen, was die genauen Umstände der Dateneingabe sind, und kann diese anschließend überprüfen und feststellen:
Durch die Einhaltung der oben aufgeführten Regeln zu Zutrittskontrolle, Zugangskontrolle und Zugriffskontrolle wurde die Grundlage für die Eingabekontrolle der Systeme geschaffen, die personenbezogenen Daten verarbeiten.
Die Änderung von Daten wird in der Verwaltungsoberfläche protokolliert. Diese Änderungen werden dauerhaft aufbewahrt.
Den Nutzern werden Rollen zugewiesen (Administrator, Partner-Administrator, Partner-Mitarbeiter), denen entsprechende Rechte zugewiesen sind. Partner mit Account dürfen jeweils nur Daten aus Ihrem Nutzerfeld einsehen. Nur Partner-Administratoren dürfen neue Mitarbeiter anlegen.
Jede Anmeldung in der Verwaltungsoberfläche wird durch den Server protokolliert.

Zugriffs-Backups (bspw. Wiederherstellungs-CDs) werden, in jedem Fall getrennt von den betreffenden Geräten, gesichert aufbewahrt.

Auftragskontrolle
Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können - *z.B.: konkrete Arbeitsanweisungen, die eine einheitliche Umsetzung der Weisungen sicherstellen (z.B. vorgegebener Interviewleitfaden, festgelegte Arbeitsanweisungen zu Art und Weise der Datenerhebung, Ort der Datenspeicherung usw.). Im Falle der Genehmigung einer Unterbeauftragung: Abgrenzung der Kompetenz zwischen Auftragsverarbeiter und Subunternehmer (Beispiel: eindeutige Vertragsgestaltung, Kriterien zur Auswahl des Subunternehmers, Kontrolle der Vertragsausführung).*

Wenn Daten im Auftrag gemäß Art. 28 DSGVO verarbeitet werden, muss sichergestellt werden, dass die Datenverarbeitung durch die Maßnahmen an Ort und Stelle (technische und organisatorische), die die Verantwortlichkeiten definieren, in Einklang mit den Anweisungen von Auftraggeber und Auftragnehmer durchgeführt wird. Mitarbeiter der mHP werden bei Arbeitsantritt und danach wiederkehrend über die Datenschutzverpflichtungen informiert und schriftlich auf die Einhaltung datenschutzrechtlicher und IT-sicherheitsbezogener Vorgaben verpflichtet. Soweit Subunternehmen für die Verarbeitung personenbezogener Daten im Auftrag eingesetzt werden sollen, werden diese auf die Einhaltung technisch-organisatorischer Maßnahmen verpflichtet, die mindestens denen dem Auftraggeber zugesicherten Umfang entsprechen.

Verfügbarkeitskontrolle
Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind - *z.B.: Maßnahmen zur Datensicherung (z.B.: Backup-Verfahren, Spiegeln von Festplatten, redundante Rechenzentren, unterbrechungsfreie Stromversorgung, Firewall, Notfallkonzept)*

Die mHP stützt sich auf die folgenden Maßnahmen, um Daten vor Verlust und Zerstörung zu schützen: Die Daten der Kunden müssen bestmöglich gesichert sein - zum einen, um Missbrauch vorzubeugen und zum anderen, um die aus einem Missbrauch resultierenden, geschäftsschädigenden Konsequenzen zu verhindern. Bei Auswahl und Entwicklung der Systemplattform achtet die mHP auf eine weitreichende Abdeckung der OWASP Sicherheitskriterien und gängiger Sicherheitslücken. Im Auftrag unserer Kunden können ebenfalls Security-Audits von spezialisierten Firmen durchgeführt werden, bei dem systematisch Schwachstellen des Systems (Plattform, Drittsoftware, Hardwarekonfiguration etc.) untersucht und protokolliert werden. Unter anderem sichert das Unternehmen System und Daten auf technischer Ebene mit folgenden Maßnahmen.
<u>Rechenzentrum:</u>
Die im Verwaltungssystem gespeicherten Daten werden mindestens täglich automatisiert gesichert. Das Rechenzentrum verfügt über Redundanzen aller kritischer Systeme (Firewall, Switch, Strom, Klima, Internetanbindung, Backup-System, Festplatten, Cores etc.).
<u>Weiterentwicklung:</u>
Für die Weiterentwicklung von Verwaltungsplattform und Algorithmen kann die Verwendung der im System vorhandenen Daten notwendig sein. Diese Daten sind

grundsätzlich nur in der geschützten Umgebung der Verwaltungsplattform verfügbar. Für Entwicklungszwecke können Abzüge der Produktivdatenbank erstellt werden, in denen Daten ausschließlich pseudonymisiert vorliegen.
Workstations:
Alle Rechner müssen mit aktueller Antiviren-Software ausgestattet sein, die in regelmäßigen Abständen (<1Monat) eine volle Prüfung des Systems durchführt.
Alle Rechner müssen eine aktuelle und aktive Firewall-Software einsetzen.
Unternehmensgeräte:
Beruflich zu verwendende Geräte werden ausschließlich durch das Unternehmen beschafft, eingerichtet und bereit gestellt. Eine private Mitnutzung von Unternehmensgeräten ist nicht zulässig.
Verwendung von mobilen Datenträgern:
Datenträger sind vor Benutzung von autorisierter Stelle (Administration) auf Unbedenklichkeit zu prüfen (bspw. Virenprüfung).
Benutzung von Workstations:
Das Öffnen von Links/Anhängen in Mails von unbekannten Absendern ist nicht gestattet. Der Eingang entsprechender Mails muss im Unternehmen veröffentlicht werden.
Das Öffnen von ausführbaren Dateien die von Dritten verschickt wurden ist nicht gestattet.
Beispielhafte Auflistung von Datenpannen und dafür vorgesehenen Maßnahmen:

- Bei Verlust von Geräten (Diebstahl, liegenlassen)
    - Sind für alle darauf eingerichteten Accounts die Passwörter zu ändern
    - Sind eventuell ausgegebene Zertifikate für darauf eingerichtete Accounts zu sperren
- Bei Verlust von Daten
    - Identifikation der verlorenen Daten (betroffene Accounts, Zeitraum, Daten)
    - Proaktive Information unserer Kunden

Identifikation der Ursache, ggf. vollständiges Abschalten des Zugriffs auf historische Daten unserer Nutzer

Maßnahmen zur Sicherstellung der Zweckbindung
Trennungskontrolle
Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können - *z.B.: Rechte- und Rollenkonzept, Mandantenfähigkeit, kundenbasierte Speichersysteme, Funktionstrennung zwischen Produktion / Test*

Das Ziel der Trennungskontrolle ist sicherzustellen, dass für verschiedene Zwecke gesammelte Daten getrennt verarbeitet werden können. Datenhaltung und Datenzugang erfolgt im Rahmen der Auftragsdatenverarbeitung grundsätzlich mandantenbezogen. Mitarbeiter des Auftraggebers haben im Rahmen Ihres individuellen Logins auf Basis eines Rechte- und Rollenkonzepts jederzeit ausschließlich Zugriff auf die Ihrem Mandanten zugeordneten Nutzerdaten.

Die Weiterentwicklung der Software findet auf Test-System statt, die von den Produktiv-Systemen getrennt sind. Das heißt, für Entwicklungszwecke werden Abzüge der Produktivdatenbank erstellt, in denen ausschließlich pseudonymisierte Daten vorliegen.

Maßnahmen zur Transparenz, Richtigkeit der Datenverarbeitung
Wahrung der Betroffenenrechte
Es ist zu gewährleisten, dass Anfragen zu Betroffenenrechten fristgemäß und umfassend beantwortet und die entsprechenden Maßnahmen beim Auftragsverarbeiter umgesetzt werden können - *z.B.: internes Konzept zum Umgang mit Datenpannen inkl. Maßnahmen zur Vermeidung von Nachteilen für betroffene Personen; Arbeitsanweisung, wie, an wen und und in welcher Frist Anfragen von betroffenen Personen zu ihren Daten weiterzuleiten sind; Konzept zu datenschutzgerechtem Löschen*

Die mHP informiert das UKJ unverzüglich bei vermuteten oder festgestellten Datenpannen. Bei Anfragen Betroffener zur Auskunft oder Löschung der Daten ist - bei vorliegendem Nutzertoken zur Authentifizierung - eine umgehende Bearbeitung und Beantwortung über die Backoffice-Managementoberfläche möglich. Anfragen zur Datenlöschung können sowohl fernmündlich als auch per Schnittstelle übermittelt werden, entsprechende Aufträge werden bestätigt und Nutzerdaten automatisch vollständig durch das System gelöscht. Ein spezielles Teilprogramm übernimmt die vollständige Löschung der Daten des entsprechenden Nutzertokens. Die Löschung wird auch im Rahmen der automatischen Backups sichergestellt, bei der auf dem Server gespeicherte Daten täglich auf einem separaten Bandspeicher gesichert werden. Um Ausfallsicherheit sicher zu stellen werden dabei rolllend abwechselnd zwei Bänder beschrieben. Backups werden nach maximal dreißig Tage neu überschrieben (spätester Zeitpunkt der vollständig Datenlöschung).

Datenvalidierung
Es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf den Zweck ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden - *z.B.: internes Konzept zur Datenvalidierung, z.B. 4-Augen-Prinzip, Stichprobenkontrolle, Verfahrensanweisung zum Umgang mit Weisungen zur Korrektur von Daten*
Der Umfang der zu verarbeitenden Daten ist durch die vereinbarte Leistungsbeschreibung eingegrenzt. Die Daten werden unverändert von dem Fitness-Tracker-Anbieter übernommen. Die mHP setzt Weisungen durch den Auftraggeber zur Korrektur von Daten unverzüglich um.

Evaluierung
Es ist ein Verfahren zu etablieren, dass eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der zum Einsatz kommenden technischen und organisatorischen Maßnahmen durch die Vertragsparteien ermöglicht - *z.B. Verfahrensanweisung; Zuweisung von Zuständigkeiten für die Evaluierung, Dokumentation der Evaluierung, bestehendes Informationssicherheitsmanagementsystems (ISMS) und /oder Datenschutzmanagementsystem (DSMS)*

Die mHP prüft automatisch und manuell die Verfügbarkeit und Sicherheit des Systems sowie das Schutzniveau der eingeführten technisch-organisatorischen Maßnahmen. Anlassbezogene Prüfungen ergehen bspw. bei Fehlermeldungen der automatischen Monitoringtools zur Verfügbarkeit von Zugriffspunkten (API, Verknüpfungswebsite) oder zur Auswertung der System-Protokolle oder System-Last, bei Benachrichtigungen durch das automatische Zutrittsmonitoring im Büro

bzw. nach Rückmeldung durch Mitarbeiter, bspw. zu veröffentlichten IT-Sicherheitslücken. Regelmäßige Prüfungen erfolgen zur organisatorischen Umsetzung im Rahmen der Datenschutzbelehrungen bzw. im Rahmen interner IT-Reviews.

Anlage 3: Projektbeschreibung

WATCH ist ein Versorgungsprojekt, das von der Post-COVID-Ambulanz am UKJ und der mHP gemeinsam durchgeführt wird. Das Projekt setzt sich im Wesentlichen aus zwei Bestandteilen zusammen:

- Klinische UKJ-Komponente
- Teilprojekt in Pulsatio-App

Im Rahmen des Projekts werden Aspekte untersucht zu Zusammenhängen zwischen
(1) Auf Befragung basierten Items zu physischen (z.B. Symptome, Belastungsintoleranz, Fatigue, Lebensqualität), kognitiven (z.B. Einschränkung von Konzentration und Aufmerksamkeit) und psychischen (z.B. Krisenmanagement) Items
(2) Aktivität (z.B. gegangenen Schritten),
(3) Vitaldaten (z.B. Herzschlägen in Ruhe am Tag und in der Nacht, Schlafdauer),
(4) Daten, die in der Post-Covid Ambulanz des UKJ erhoben werden (z.B. Veränderungen der Symptombelastung).

Zu diesem Zweck sollen mit Hilfe von Messdaten von Fitnessarmbändern/ Smartwatches (sogenannten „Wearables“) über die Pulsatio-App Daten erhoben werden. Diese Daten aus der Pulsatio-App werden mit den durch die Post-Covid-Ambulanz des UKJ erhobenen Daten zum psychischen Wohlbefinden unter Verwendung eines Pseudonyms verknüpft und wissenschaftlich ausgewertet. Die Projektpartner unterstützen sich bei der Wahl geeigneter Analyseverfahren, der Datenaufarbeitung, und Interpretation.

Das Projekt WATCH dient folgenden Forschungszwecken:

- Es sollen Erkenntnisse darüber gewonnen werden, ob mit Hilfe von Wearables erhobene Aktivitäts- und Vitaldaten (z.B. Schlafdauer oder Anzahl der Schritte) identifiziert werden können.
- Es sollen Zusammenhänge zwischen Wearable basierten Daten und Befragungsdaten im Kontext langfristiger Folgen nach einer Covid19-Erkrankung eruiert werden für physische, kognitive und psychische Items.
- Es sollen Erkenntnisse darüber gewonnen werden, ob mit Hilfe von Wearables und Apps die Behandlung von Long-COVID-Patient:innen im Rahmen von digitalen Interventionen unterstützt und in die Regelversorgung überführt werden kann.
- Es sollen Erkenntnisse über Symptome, Verbreitung und Auswirkungen von Long-COVID in der Bevölkerung gewonnen werden.
- Es sollen allgemeine Erkenntnisse über geeignete Anwendungsfälle und spezifische Anforderungen an neuartige App-/Wearable-basierte epidemiologische Surveillance-Instrumente gewonnen werden.

Zukünftiger Nutzen:

- Bessere Versorgung von Long-COVID-Betroffenen
- Long-COVID-betroffene können schneller auf geeignete Unterstützungsangebote hingewiesen werden.

Zuständigkeiten des UKJ: Wirkbereich A
Das UKJ erstellt den zur Projektdurchführung notwendigen Ethikantrag und reicht diesen zur Begutachtung bei der zuständigen Ethikkommission ein. Das UKJ stellt der mHP die zur Zusammenführung der vom UKJ erhobenen Daten mit den aus dem Projekt erhobenen Daten zur Verfügung. Dazu zählen neben Pseudonym, Alter, Geschlecht, auch die Werte auf den in der Eingangsbefragung erhobenen Basisdaten. Zu keinem Zeitpunkt stellt das UKJ die persönlich indentifizierenden Daten wie Name, Adresse, Telefonummer, Email-Adresse der mHP zur Verfügung. Das UKJ wertet die zusammengeführten Daten im Rahmen der von den Projektteilnehmerern erteilten Einwilligungen aus. Das UKJ ist für die persönliche Betreuung der Projektteilnehmerer zuständig.

Die Einwilligung zur Teilnahme (Teilnahmeerklärung) wird vom UKJ im Rahmen des Einschlusses nach Aufklärung erhoben. Das UKJ holt auch die datenschutzrechtliche Einwilligung für die Verarbeitung im Wirkbereich A ein.

Zudem informiert das UKJ die Projektteilnehmerer schriftlich mittels der von der mHP bereitzustellenden Datenschutzinformationen und Einwilligungsformulare über die allgemeine Datenverarbeitung durch die App sowie die spezifische Datenverarbeitung für die Zwecke der des Teilprojekts und holt im Anschluss für die mHP die Einwilligung der Projektteilnehmerer für die Datenverarbeitung durch die App für die Zwecke des Projekts schriftlich ein.

Zuständigkeiten der mHP: Wirkbereich B
Im Rahmen des Projektes stellt die mHP für WATCH innerhalb der Pulsatio-App Daten zur Verfügung und erhebt mit Hilfe dieser App sensorbasiert Aktivitäts-, Schlaf- und Vitaldaten. Die mHP ist für die technische Umsetzung und Gestaltung der Pulsagio-App zuständig. Die mHP stellt dem UKJ die im Rahmen des Projekts erhobenen Sensordaten sowie den dazugehörigen Pseudonymen, der eine Zusammenführung mit den in der Post-Covid-Ambulanz des UKJ erhobenen Daten ermöglicht, zur Verfügung. Die mHP wertet die zusammengeführten Daten im Rahmen der von den Projektteilnehmerern erteilten Einwilligungen aus.

Die Einwilligung für die App-Nutzung im Rahmen des Projekts holt die mHP über die App ein. Zudem stellt die mHP dem UKJ die den Projektteilnehmerern bereitzustellenden Datenschutzhinweise und Einwilligungsformulare für die die allgemeine Datenverarbeitung durch die App sowie die spezifische Datenverarbeitung für die Zwecke des WATCH-Projekts zur Verfügung.

Zuständigkeiten des UKJ und der mHP: Wirkbereiche A und B
Das UKJ und die mHP führen die für zur Beantwortung der jeweiligen Forschungsfragen relevanten Analysen und Auswertungen im Rahmen der gemeinsamen Datenverarbeitung eigenständig oder gemeinsam durch. Soweit die

Analyse und Auswertung gemeinsam durchgeführt wird, liegt die betreffende Datenverarbeitung in den Wirkbereichen beider Parteien.

Anlage 4: Datenschutzerklärung für Projektteilnehmer mit Prozesshinweisen

Diese Datenschutzerklärung gilt ergänzend zu den Datenschutzhinweisen der mHP für die Pulsatio-App und den Datenschutzhinweisen des UKJ für die in der Post-COVID-Ambulanz in Jena durchgeführte Projekt WATCH

Datenschutzhinweise zu WATCH: Mobile WohnortnAhe Versorgung zur Steuerung der sekTorübergreifenden Langzeittherapie bei Post-COVID-19 in THüringen (WATCH)

WATCH ist ein optionales Versorgungsprojekt für Patienten der post-COVID-Ambulanz des Universitätsklinikum Jena (nachfolgend UKJ genannt). Das Projekt wird vom UKJ und der Gesundheitsdatenplattform Thryve durchgeführt (Verantwortlich für die Ausgestaltung der Pulsatio-App).

WATCH hat als übergeordnetes Ziel, die Versorgung behandlungsbedürftiger Post-COVID-Patient*innen unter Berücksichtigung der Kosteneffektivität, über eine mobile Post-COVID-Ambulanz und eine multimodale Symptom-übergreifende telemedizinische Versorgungslösung („BRAIN, BODY, SOUL“) zu verbessern. Zentrale Elemente sind die interdisziplinäre Diagnostik in einer mobilen Post-COVID-Ambulanz (PoCO-Bus) sowie eine multimodale („holistische“) Intervention basierend auf telemedizinischen Modulen.

Teil der Evaluation der telemedizinischen Versorgungslösung ist Analyse von (1) psychologischen Variablen (z.B. Körperliche und mentale Gesundheit, Belastungsintoleranz (2) Aktivität (z.B. Anzahl der zurückgelegten Schritte pro Tag, Metabolisches Äquivalent (MET min), Schlafdauer), (3) Vitaldaten (z.B. Puls in Ruhe am Tag und in der Nacht). Zu diesem Zweck soll mit Hilfe Ihres Smartphones und Ihres Fitnessarmbandes oder Ihrer Smartwatch (sogenannten "wearables“) Daten erhoben werden. Diese Daten werden mit den Daten des UKJ verknüpft und wissenschaftlich analysiert.

WATCH verfolgt zwei Hauptziele:

Ziel A: Mit Hilfe von mit Fitnessarmbändern und Smartwatches sollen Aktivitäts- und Vitaldaten (z.B. Anzahl der zurückgelegten Schritte pro Tag, Metabolisches Äquivalent (MET min), Schlafdauer) im Zusammenhang mit Fragebogendaten (z.B. körperliches und mentales Wohlbefinden) analysiert werden.
Zukünftiger Nutzen: Mittels wearables können kontinuierlich und schnell Veränderungen in körperlichen Faktoren mit kognitiven und psychischen Komponenten in Zusammenhang analysiert werden. Dies ermöglicht es digitale

Gesundheitsanwendungen hinsichtlich der Prävention und Therapie von Langzeitfolgen nach einer SARS-CoV-2 Infektion besser zu verstehen und ggf. zu steuern.

Ziel B: Insofern Personen an einem Betreuungsangebot an der PostCovid-Ambulanz teilnehmen, kann durch die Verknüpfung der Wearable- und UKJ-Daten die Wirksamkeit der telemedizinischen Intervention überprüft und verbessert werden.
Zukünftiger Nutzen: Telemedizinische Versorgungs- und Untersuchungsangebote können besser auf individuelle Bedürfnisse zugeschnitten werden und als Basis für die Einführung dieser Angebote in die Regelversorgung dienen.

Die folgende Datenschutzerklärung und die sich anschließende Einwilligung zur Teilnahme beziehen sich ausschließlich auf WATCH.

1) Verantwortlichkeit nach Art. 26 Datenschutzgrundverordnung (DSGVO)

Das UKJ und das die mHP arbeiten im Rahmen der des Projekts WATCH eng zusammen. Dies betrifft auch die Verarbeitung Ihrer Daten. Das UKJ und die mHP haben die Zwecke und Mittel der Verarbeitung personenbezogener Daten in den einzelnen Prozessen gemeinsam festgelegt und sind innerhalb der nachfolgend beschriebenen Prozesse daher gemeinsam für den Schutz Ihrer personenbezogenen Daten verantwortlich (Art. 26 DSGVO).

2) Prozesse, für die eine gemeinsame Verantwortlichkeit besteht

Die Erhebung der Wearable Daten findet über die Pulsatio-App der mHP statt. Die mHP ist vollständig für die technische Gestaltung und Umsetzung der App, sowie der damit verknüpften Gesundheitsplattform zuständig. Die Datenhaltung der Wearable-Daten erfolgt auf sicheren Servern der mHealth Pioniers GmbH.

Die gemeinsame Verantwortlichkeit besteht im Rahmen der von Ihnen erteilten Einwilligungen für folgende Prozesse:

- Verwaltung der Basisdaten der Projektteilnehmerer am UKJ inkl. Onboarding von Projektteilnehmerern
- Erhebung von Befragungsdaten im Rahmen des WATCH-Projekts innerhalb der Pulsatio-App
- Erhebung von Befragungsdaten im Rahmen des WATCH-Projekts in der PostCOVID-Ambulanz des UKJ in Jena
- Übermittlung der Befragungsdaten zwischen mHP und UKJ
- Übermittlung von Vitaldaten durch die mHP an das UKJ
- Speicherung und Zusammenführung der verschiedenen Befragungs- und Vitaldaten unter Verwendung eines Pseudonyms
- Auswertung der zusammengeführten Datensätze zu den mitgeteilten Forschungszwecken

Die Datenhaltung der Wearable-Daten erfolgt auf sicheren Servern der mHP. Der Einschluss in das Projekt sowie die Erhebung persönlich identifizierender Informationen wie Name und Kontaktdaten erfolgt über das UKJ (post-COVID-Zentrum).

Vereinbarung zwischen dem UKJ und der mHP
Im Rahmen ihrer gemeinsamen datenschutzrechtlichen Verantwortlichkeit haben das UKJ und die mHP vereinbart, wer von ihnen welche Pflichten nach der DS-GVO erfüllt. Dies betrifft insbesondere die Wahrnehmung der Rechte der betroffenen Personen und die Erfüllung der Informationspflichten gemäß den Artikeln 13 und 14 DSGVO. Diese Vereinbarung ist notwendig, da im Rahmen des Projektes personenbezogene Daten in unterschiedlichen Prozessabschnitten und Systemen verarbeitet werden, die entweder vom UKJ oder von der mHP betrieben werden.

Auswirkung für Betroffene: Auch wenn eine gemeinsame Verantwortlichkeit besteht, erfüllen das UKJ und mHP die datenschutzrechtlichen Pflichten entsprechend ihrer jeweiligen Zuständigkeiten für die einzelnen Prozessabschnitte wie folgt: Im Rahmen der gemeinsamen Verantwortlichkeit ist

- das UKJ für die Verarbeitung der personenbezogenen Daten der Post-Covid-Ambulanz zuständig und
- Thryve für die Verarbeitung personenbezogener Daten im Abschnitt sensorbasierte Datenerhebung und Datenspeicherung auf der Thryve Plattform zuständig.

Das UKJ und Thryve stellen Ihnen für die jeweiligen Bereiche die gemäß Art. 13 und 14 DSGVO erforderlichen Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache unentgeltlich zur Verfügung und informieren sich unverzüglich gegenseitig über von Betroffenen geltend gemachte Rechtspositionen. Sie stellen einander sämtliche für die Beantwortung von Auskunftsersuchen notwendigen Informationen zur Verfügung. Datenschutzrechte können sowohl bei dem UKJ als auch bei Thryve geltend gemacht werden. Wenden Sie sich bitte bei Fragen zu Prozessabschnitt 1) an das UKJ und bei Fragen zu Prozessabschnitt 2) an die mHealthPioniers GmbH.

3) Einwilligungen zur Datenverarbeitung

Ihre Teilnahme an WATCH ist freiwillig. Ihre Einwilligung liefert die rechtliche Grundlage, Ihre personenbezogenen Daten zu dem oben genannten Zwecken zu verarbeiten.

Ihre ausdrücklichen Einwilligungen, die Sie gegenüber dem UKJ und in der Pulsatio-App gegenüber der mHP erteilen, bilden die rechtliche Grundlage für die Verarbeitung Ihrer personenbezogenen Daten zu den oben genannten Zwecken. Ihre Projektteilnahme und somit auch die Erteilung der von uns erbetenen Einwilligungen für WATCH sind selbstverständlich freiwillig und jederzeit widerrufbar.

4) Widerruf Ihrer Einwilligungen / Beendigung Ihrer Teilnahme

Ihre Einwilligungen können jederzeit ohne Angabe von Gründen widerrufen werden. Durch einen Widerruf wird die Rechtmäßigkeit der aufgrund der betreffenden Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt.

Die Einwilligung zur Teilnahme kann jederzeit ohne Angabe von Gründen widerrufen werden. Um die Teilnahme zu widerrufen können sie den Schieberegler, mit dem Sie zur Teilnahme an der WATCH zugestimmt haben, nach links schieben. Sollten Sie die App deinstalliert haben, können Sie die Teilnahme an dem Projekt per Mail (postcovidzentrum@med.uni-jena.de) widerrufen. Der Widerruf hat zur Folge, dass innerhalb einer Frist von 28 Tagen alle auf der Thryve Plattform und mit dem Pseudonym verknüpfte Daten automatisch und unwiderruflich gelöscht werden. Welche Daten des UKJ gelöscht werden hängt davon ab, ob sie an Betreuungsangeboten der Post-Covid-Ambulanz teilnehmen oder nicht. Bitte teilen sie bei einer Löschanfrage mit, welche Daten sie löschen möchten. Technisch ist es möglich, sich nach einem erfolgten Widerruf für die Teilnahme an dem Projekt wieder einzuschreiben (d.h., den Slider erneut nach rechts schieben). Der Zuvor erteilte Widerruf bleibt dadurch unberührt und wird ausgeführt. Weitere Hinweise zum Widerruf von Einwilligungen in Bezug auf die Verarbeitung durch die App finden Sie in der Datenschutzerklärung der mHP für die Pulsatio-App sowie in der FAQ unter https://pulsatio.app/.

5) Datenerhebung

Die Datenerhebung des UKJ und Thryve Plattform finden unabhÃ¤unabhängig voneinander statt. Die Daten werden erst nachträglich zur wissenschaftlichen Auswertung zusammengeführt.

Datenerhebung auf der Thryve Plattform:
Die Projekt-App ermöglicht es End-Nutzern nach zuvor erteilter Einwilligung, Daten Ihres Fitnessarmbands auf Basis eines automatisch erzeugten Pseudonyms (z.B.: IgQ3D24PnSzEHpvv) zur Verfügung zu stellen. Der Umfang der notwendigen Autorisierungen für bspw. Aktivitäts- und Vitaldaten, ist abhängig von den Wearable-Anbietern. Die Datenerhebung auf der Thryve Plattform findet pseudonymisiert statt. Das bedeutet, dass Ihnen als Person eine zufällige Folge aus Buchstaben und Zahlen zugeordnet und zusammen mit Ihren Daten gespeichert wird (Beispiel-Pseudonym: aEzX6s7essasss1345bsoe). Das Pseudonym wird bei der Installation der App automatisch generiert. Dazu erhalten Sie einen QR-Code zum ersten Termin in der mobilen post-COVID-Ambulanz. Nutzen Sie das Login in die Pulsatio-App in dem Sie auf das Feld QR-Code scannen drücken. Sie werden damit automatisch angemeldet und das Pseudonym wird Ihnen zugewiesen. Das Pseudonym ist u.a. dazu notwendig, um die Wearable-Daten mit den Daten aus der post-Covid-Ambulanz zu verknüpfen. Es werden Daten über die Pulsatio-App erhoben und auf der Thryve-Plattform gespeichert. Nach Ihrer Freigabe in der Pulsatio-App durch die Verbindung zu Ihrem Fitnessarmband/Smartwatch werden die für die Durchführung des Projekts notwendigen Daten vom Server des Wearable-Herstellers an Thryve übermittelt. Neben manuell getätigten Eingaben in der Pulsatio-App, werden folgende Wearable-Daten erfasst:

- Aktivitätsdaten: z.B. Informationen zurückgelegte Schritte pro Tag, Schlaf- und Ruhephasen, metablisches Äquivalent (MET min))
- Vitaldaten: (z.B. Puls am Tag und in der Nacht, maximale Herzfrequenz am Tag)
- Schlafdaten: (z.B. Schlafdauer, Einschlafzeitpunkt, Aufwachzeitpunkt)

Weitere Informationen zur Verarbeitung Ihrer personenbezogenen Daten durch die App erfahren Sie in der Datenschutzerklärung der mHP für die Pulsatio-App.

Die Pulsatio-App erhebt solange Daten, bis Sie die Verknüpfung mit der App löschen. Dies geschieht z.B. dadurch, dass Sie Ihr Konto löschen. Außerdem können Sie jederzeit die Freigabe der Daten in der Pulsatio-App zurücknehmen. Zum Zurücknehmen der Freigabe der Daten folgen Sie bitten diesen Schritten:

1 Öffnen Sie die Pulsatio-App
2 Öffnen Sie das Menü in der Pulsatio-App (oben links)
3 Wählen Sie den Messzeitpunkt und Datenquellen aus
4 Trennen Sie die Verbindung bei den entsprechenden Quellen
Wurde die Verknüpfung mit den Datenquellen getrennt, werden keine Daten mehr an die Thryve-Plattform übermittelt. Bitte beachten Sie, eine Deinstallation der App ist nicht ausreichend, um die Datenübertragung zu trennen. Wenn Sie die App bereits deinstalliert haben, trennen Sie die Verbindung bitte im Account Ihres Wearable-Herstellers.

Datenerhebung im UKJ:
Durch die Nutzung der Betreuungsangebote der Post-Covid-Ambulanz werden folgenden Daten in der mobilen post-COVID-Ambulanz erfasst:

- Umfassende interdisziplinäre Diagnostik („one-stop-shopping-Konzept“) zur Erfassung der Post-COVID-Beschwerden: COVID-Anamnese, ggf. Vervollständigung der Fragebögen (siehe nächster Punkt), ein Tablet-basierter Konzentrations-, Aufmerksamkeits- und Gedächtnistest (Oxford Cognitive Screen plus, (OCS-plus)), ein einminütiger Sit-to-Stand-Test sowie eine Handkraftdynamometrie zur Erfassung der körperlichen Leistungsfähigkeit sowie eine Lungentonometrie zur Charakterisierung von Störungen der Atemmechanik

- Befragungsdaten in Form von Fragebögen zu:
  Körperliche Gesundheit, Mentale Gesundheit, Screening Depression, Aktuelle Bewältigungsanstrengungen zur Krankheitsverarbeitung (emotional, kognitiv), Status und Schweregrad psychischer Störungen, Körperliche und mentale Fatigue, Tägliche kognitive Probleme, Schlafqualität, Immunologische Erholung/Beanspruchung, Belastungsintoleranz, Aktuelle und zukünftige subjektive Arbeitsfähigkeit, Interview: Nutzungsverhalten, Adhärenz, Akzeptanz; Blutentnahme

6) Datenspeicherung

Die Daten werden auf einem sicheren Server in Deutschland gespeichert, welche den geltenden Sicherheitsstandards entsprechen. Abbildung 1 kennzeichnet den Datenfluss inklusive Datenerhebung und Datenaustausch.

7) Datenaustausch zwischen dem UKJ und der mHP

Zur Beantwortung der wissenschaftlichen Fragestellungen ist es notwendig, Daten aus dem UKJ und aus der Pulsatio-App zu verknüpfen. Zur Verknüpfung findet ein nicht-automatisierter Austausch pseudonymisierter Daten zwischen dem UKJ und der mHP statt. Dem jeweils anderen Partner

werden nur die Daten zur Verfügung gestellt, die zur Beantwortung der wissenschaftlichen Fragestellung notwendig sind.

Die mHP stellt dem UKJ folgende Daten zu Verfügung:
1) das Pseudonym, Aktivitäts-, Schlaf- und Vitaldaten die für die Dauer der Nutzung der Pulsatio-App erhoben werden.
2) Ausgefüllte Fragebögen in der Pulsatio-App, die Teil von WATCH sind und je nach Messzeitpunkt per Papier oder/und Pulsation App erhoben werden können.
Die Daten von Teilnehmern an der WATCH werden nach vollständigem Abschluss der

Das UKJ stellt der mHP folgende Daten zur Verfügung:
(1) das Pseudonym

(2) Eingaben aus der Eingangsbefragung und Folgeerhebungen (siehe Punkt 6 Datenerhebung UKJ).

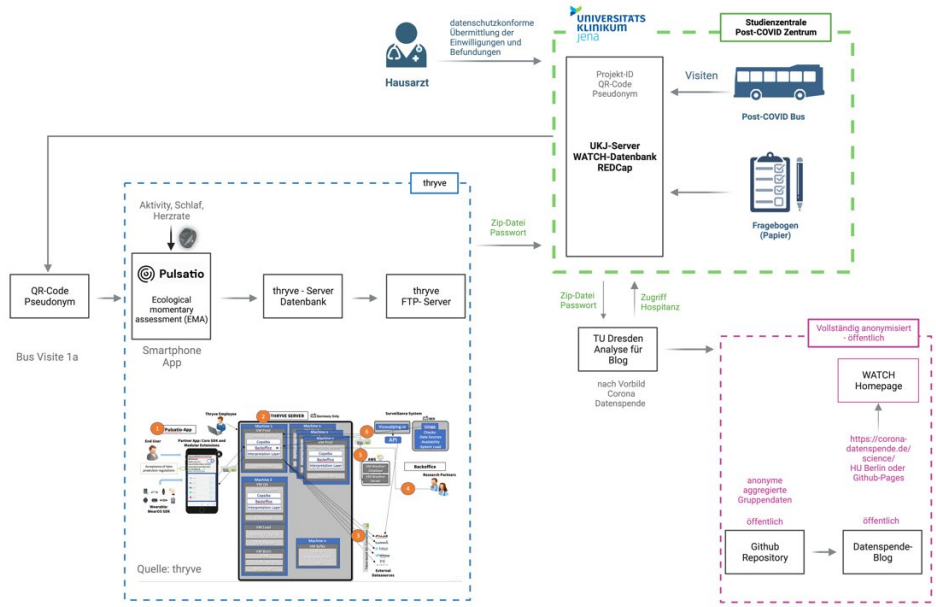

Abb. 1: Datenfluss nach Bus-Visite V1a differenziert nach Pulsatio-App (Firma mHealth Pioneers GmbH), UKJ und Konsortialpartner, Corona-Datenspende-Blog sowie Projekthomepage.

8) Betroffenenrechte gemäß Datenschutzgrundverordnung (DSGVO):

Solange die Daten Ihrer Person zugeordnet werden können haben Sie das Recht

1. Auskunft zu verlangen zu Kategorien der verarbeiteten Daten, Verarbeitungszwecken, etwaigen Empfängern der Daten, der geplanten Speicherdauer (Art. 15 DSGVO);

2. die Berichtigung bzw. Ergänzung unrichtiger bzw. unvollständiger Daten zu verlangen (Art. 16 DSGVO);

3. eine erteilte Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen (Art. 7 Abs. 3 DSGVO);

4. einer Datenverarbeitung, die aufgrund eines berechtigten Interesses erfolgen soll, aus Gründen zu widersprechen, die sich aus Ihrer besonderen Situation ergeben (Art 21 Abs. 1 DSGVO);

5. in bestimmten Fällen im Rahmen des Art. 17 DSGVO die Löschung von Daten zu verlangen - insbesondere soweit die Daten für den vorgesehenen Zweck nicht mehr erforderlich sind bzw. unrechtmäßig verarbeitet werden, oder Sie Ihre Einwilligung gemäß oben (c) widerrufen oder einen Widerspruch gemäß oben (d) erklärt haben;

6. unter bestimmten Voraussetzungen die Einschränkung von Daten zu verlangen, soweit eine Löschung nicht möglich bzw. die Löschpflicht streitig ist (Art. 18 DSGVO);

7. auf Daten-Übertragbarkeit, d.h., Sie können Ihre Daten, die Sie uns bereitgestellt haben, in einem gängigen maschinenlesbaren Format wie z.B. CSV erhalten und ggf. an andere übermitteln (Art. 20 DSGVO).

9) Löschung

Bei der Löschung wird zwischen gespeicherten Daten auf der (1) Pulsatio-Plattform und (2) auf denen des UKJ unterschieden. Bei der Löschung von (1) und (2) handelt es sich um voneinander unabhängige Prozesse. Die Trennung ist notwendig, um bei einer eventuellen Teilnahme an Betreuungsangeboten der PostCovid-Ambulanz des UKJ sicherzustellen, dass die Löschung der Wearable-Daten nicht automatisch zur Löschung der für die Teilnahme der Betreuung notwendigen Daten führt. Bitte teilen Sie uns bei einer Löschanfrage mit, welche Daten Sie löschen möchten. Aufgrund von technischen Gegebenheiten kann die vollständige Löschung bis zu 30 Tage in Anspruch nehmen.

Löschung der Daten auf der Pulsatio-Plattform

Es stehen unterschiedliche Möglichkeiten zur Verfügung, die Daten auf der Pulsatio-Plattform zu löschen. ***Möglichkeit 1 – die App ist installiert:*** Um Ihre Daten auf der Pulsatio-Plattform zu löschen, folgen Sie bitte folgenden Schritten.

a. Öffnen Sie die Pulsatio-App

b. Öffnen Sie das Menü in der App (oben links)

c. Wählen Sie den Menüpunkt „Nutzer löschen“ aus

d. Bestätigen Sie die Löschung

Möglichkeit 2 – die App ist deinstalliert: Schreiben Sie eine E-Mail an *Watch-Koordinator(in) am UKJ watchkoordination@med.uni-jena.de* (Betreff: „Datenlöschung Pulsatio-App“ - Nachrichteninhalt: ihr Pseudonym). Bitte beachten Sie, dass nur die Wearable-Daten gelöscht werden.

Löschung der Daten am UKJ

Wenn Sie NUR die Daten am UKJ löschen wollen, schreiben Sie eine E-Mail an *Watch-Koordinator(in) am UKJ: watchkoordination@med.uni-jena.de* (Betreff: „Datenlöschung Projektteilnahme- Nachrichteninhalt: ihr Pseudonym).

Löschung der am UKJ und der in der Pulsatio-Plattform gespeicherten Daten

Für den Fall, dass Sie alle Daten löschen lassen möchten, schreiben Sie eine Nachricht an *Projektleiter des UKJ* (Betreff: „Datenlöschung Projektteilnahme und Pulsatio-App - Nachrichteninhalt: ihr Pseudonym).

Sonstige Hinweise

Veröffentlichung der Ergebnisse (z.B. in wissenschaftlichen Zeitschriften)

Ergebnisse des Projekts werden in anonymisierter Form (d.h. in einer Form, die keine Rückschlüsse auf Sie als einzelne Person zulassen) in wissenschaftlichen Fachzeitschriften, auf Kongressen und im Internet präsentiert und veröffentlicht. Anonymisierte Datensätze und daraus hervorgegangene Ergebnisse und Veröffentlichungen können rückwirkend nicht mehr gelöscht werden, werden aber in zukünftigen Analysen nicht mehr berücksichtigt und gelöscht.

Möglicher Nutzen für die Teilnehmenden bzw. die Allgemeinheit

- Der mögliche Nutzen für die Teilnehmenden bzw. die Allgemenheit lässt sich über die beiden zentralen Ziele des UKJ und der mHP abbilden:
- **Ziel UKJ:** Es wird überprüft, ob mit Hilfe von Fitnessarmbändern und Smartwatches erhobenen Aktivitäts- und Vitaldaten (z.B. Schlafdauer oder Anzahl der Schritte) erkannt werden kann, ob und wie schwer eine Person durch langfristige Folgen einer Covid19-Erkrankung in ihrer physischen, psychischen und sozialen Lebensqualität beeinträchtigt ist. Zukünftiger Nutzen: Belastete Personen können schneller auf geeignete Unterstützungsangebote hingewiesen werden.
- **Ziel mHP:** Untersucht werden Informationen zu Covid-19 bezogenen Langfristfolgen mit dem Ziel der Validierung von Mustererkennung und Entwicklung digitaler Biomarker für Long COVID.

Kontaktdaten der Datenschutzbeauftragten

UKJ:
Heike Tödter
Beauftragte für Datenschutz
Zentrum für Gesundheits-und Sicherheitsmanagement,
Beauftragte für Datenschutz
datenschutzbeauftragter@med.uni-jena.de
Telefon: +49 3641 9-325624
Fax: +49 3641 9-399925

mHP

Hannes Schenk
Datenschutzbeauftragter von der mHP
mHealth Pioneers GmbH
Körtestraße 10
10967 Berlin

privacy@thryve.de

Kontaktdaten der zuständigen Datenschutz-Aufsichtsbehörden

Zuständig für die mHP ist der
Berliner Beauftragte für Datenschutz und Informationsfreiheit
Alt-Moabit 59-61
10555 Berlin
mailbox@datenschutz-berlin.de

Zuständig für die UKJ ist der
Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI)
Häßlerstraße 8
99096 Erfurt

Anlage 5 – Einwilligungserklärung für die Pulsatio-APP

Datenschutzhinweise und Einwilligungserklärung zur Teilnahme an Pulsatio

Um an der Pulsatio-App teilnehmen zu können, müssen Sie der nachfolgend beschriebenen Verwendung Ihrer Gesundheitsdaten durch die mHealth Pioneers GmbH zustimmen. Das Gesamtsystem der Pulsatio-App umfasst die Pulsatio-App („App“) sowie den Pulsatio-Server („Server2).

1. Verantwortung für Datenverarbeitung

Für die Verarbeitung Ihrer Daten ist die mHealth Pioneers GmbH, Körtestr. 10, 10967 Berlin, verantwortlich. Datenschutzbeauftragter ist Hannes Schenk, datenschutz@thryve.de

2. Zweck der Pulsatio-App

Die Pulsatio-App ermöglicht Forschenden, Gesundheitsdaten aus Sensoren, wie z.B. Fitnessarmbändern und über Fragebögen berichteten Gesundheitsangaben zu kombinieren, um daraus neue Erkenntnisse abzuleiten.

3. Art der für den Zweck verarbeiteten Daten

Welche Daten zu welchem Zweck und auf welcher Grundlage benötigt und verarbeitet werden, richtet sich maßgeblich nach den von Ihnen genutzten Projekten bzw. dem Umfang der erteilten Einwilligungen. Übergeordneter Zweck der Datenverarbeitung ist stets das Aufdecken neuer wissenschaftlicher Zusammenhänge in Verbindung mit Gesundheitssensorik. Pulsatio ist weder eine medizinische Beratung noch eine individuelle Diagnostik.

3.1. Gesundheitsdaten und weitere besondere Datenkategorien

In Pulsatio werden regelmäßig Gesundheitsdaten im Sinne von Art. 9 Abs. 1 DSGVO verarbeitet. Gesundheitsdaten sind alle Daten, die Informationen zum Gesundheitszustand einer Person enthalten. Dazu gehören nicht nur Angaben zu früheren und aktuellen Krankheiten, sondern auch zu Krankheitsrisiken einer Person.

Darüber hinaus können in seltenen Einzelfällen weitere besondere Kategorien von personenbezogenen Daten, etwa biometrische Daten verarbeitet werden, die möglicherweise in den Datensätzen von verbundenen Datenquellen enthalten sind. Da es sich bei den verarbeiteten Fitness-Tracker-Daten jedenfalls potenziell um Gesundheitsdaten handelt, behandelt die mHealth Pioneers GmbH vorsorglich alle Datenspenden als Gesundheitsdaten. Rechtsgrundlage für diese Verarbeitung Ihrer Gesundheitsdaten und ggf. weiterer Datenkategorien im Sinne von Art. 9 Abs. 1 DSGVO ist jeweils Ihre ausdrückliche Einwilligung (Art. 6 Abs. 1 lit. a und Art. 9 Abs. 2 lit. a DSGVO), die Sie beim Einrichten der App und/oder bei der Anmeldung für ein Projekt erteilt haben.

3.2. Pseudonym, PIN

Sobald Sie in die Teilnahme an Pulsatio eingewilligt haben, erzeugt die App ein Pseudonym. Das Pseudonym wird mit Ihren gespendeten Daten verbunden. Wenn Sie Ihre Datenschutzrechte ausüben, benötigen Sie zudem die PIN, die zusammen mit Ihrem Pseudonym generiert wird. So soll verhindern werden, dass einer unbefugten Person, die Ihr Pseudonym kennt, Ihre zu Ihrem Pseudonym gespeicherten Gesundheitsdaten übermittelt, verändert oder gelöscht werden. Rechtsgrundlage dieser Verarbeitung Ihrer Daten ist Ihre ausdrückliche Einwilligung (Art. 6 Abs. 1 lit. a und Art. 9 Abs. 2 lit. a DSGVO), die Sie bei der Einrichtung der App erteilt haben.

3.3. Daten aus verbundenen Datenquellen

Wenn Sie eine Datenquelle verbinden und diese zur Datenweitergabe an Pulsatio autorisieren, werden Ihre Fitness-Tracker-Daten an den Server übermittelt und unter Ihrem Pseudonym gespeichert. Das Autorisierungsverfahren wird von den jeweiligen Anbietern der Datenquellen festgelegt (in der Regel müssen Sie sich bei der jeweiligen Datenquelle über eine Website oder App des Anbieters einloggen und dort eine Freigabe für Pulsatio erteilen).

Wenn Sie die App mit einer anderen Datenquelle als Apple Health oder Samsung Health verbinden, stellt der Server der jeweiligen Datenquelle einen Token für den Server aus, der dort an Ihrem Pseudonym gespeichert wird. Mit diesem Token ruft der Server die von Ihnen freigegebenen Daten vom Server der Datenquelle. Dies funktioniert ohne Beteiligung der App, also auch dann, wenn Ihr Smartphone nicht mit dem Internet verbunden ist oder Sie die App löschen. Bei den Datenquellen Apple Health und Samsung Health werden die Daten lokal übergeben, d. h. die Health-Apps von Apple bzw. Samsung geben die freigegebenen Daten auf Ihrem Gerät über eine spezielle Schnittstelle an die App weiter.

Die von den externen Datenquellen bereitgestellten Fitness-Tracker-Daten enthalten Vitaldaten und teilweise auch sog. Profildaten: Vitaldaten sind Informationen zu Ihren körperlichen Aktivitäten und Vitalfunktionen, etwa die Anzahl Ihrer täglichen Schritte, Informationen zu Ihren sportlichen Betätigungen (Art der Aktivität wie beispielsweise Laufen oder Fahrradfahren, Zeitpunkt und Dauer), Ihrem Schlafverhalten (Schlafzeiten und Schlafphasen) und zu Ruhezeiten. Daneben umfassen Vitaldaten auch Messdaten zu Ihren Vitalfunktionen wie beispielsweise Puls, Herzratenvariabilität, Stress, Temperatur und Blutdruck. Profildaten sind Daten wie Ihre E-Mail-Adresse, Ihr Name, Ihr Geburtsdatum, Ihre Adresse, Ihr Geschlecht, Ihr Benutzername und sonstige Nutzer- oder Geräte-Kennungen, über die Sie direkt oder indirekt identifiziert werden könnten. a) Die Datensätze der Datenquellen Apple Health, Samsung Health, Garmin, Fitbit, Oura, Polar und Withings enthalten keine Profildaten. b) Die Datensätze der Datenquelle Google Fit enthalten Profildaten (Profilbild, falls im Google-Konto hinterlegt, sowie die Google-ID) übermittelt. Diese Daten werden für die Pulsatio nicht benötigt und daher noch während des Empfangsvorgangs gelöscht. c) Wenn die App mit Polar verbunden wird, ist der Abruf von Profildaten (Name, Vorname, Geburtsdatum, Größe, Gewicht, Geschlecht) möglich. Bei Verbindung mit der Datenquelle Samsung Health erlaubt deren Anbieter den Abruf der Geräte-IDs des

mobilen Endgeräts und ggf. eines registrierten Fitness-Trackers. Von diesen Abrufmöglichkeiten macht Pulsatio keinen Gebrauch. Rechtsgrundlage dieser Verarbeitung Ihrer personenbezogenen Daten ist Ihre ausdrückliche Einwilligung (Art. 6 Abs. 1 lit. a und Art. 9 Abs. 2 lit. a DSGVO), die Sie beim Einrichten der App erteilt haben. Den Wortlaut dieser Einwilligung finden Sie am Ende dieser Datenschutzhinweise.

3.4. Befragungen in Projekten

Die Projektteilnahme erfolgt durch die Beantwortung von Fragebögen, die in der App angezeigt und per Push-Benachrichtigung angekündigt werden. Mögliche Themen sind beispielsweise bestimmte Aspekte der Herzgesundheit oder der mentalen Gesundheit. Wenn Sie an einem Projekt teilnehmen, werden die Befragungsdaten im Rahmen Ihrer Einwilligung mit den bisherigen und zukünftigen Fitness-Tracker-Daten und ggf. Befragungsdaten aus anderen Projekten verknüpft, um mögliche Zusammenhänge zwischen den Befragungsergebnissen und den Vital- und Aktivitätsdaten zu erkennen. Wenn Sie allgemein in die Teilnahme an Projekten einwilligen, wird dies auf dem Server unter Ihrem Pseudonym gespeichert, so dass Sie per Push-Benachrichtigung auf neue Fragebögen zu den von Ihnen aktivierten Projekten hinweisen kann. Sie können nur an Befragungen teilnehmen, wenn Sie der App die Anzeige von Push-Mitteilungen erlauben. Die App nutzt die Push-Dienste der jeweiligen Betriebssystemhersteller: Firebase Cloud Messaging von Google (Android) und Apple Push Notifications (iOS). Dabei generieren Google und Apple jeweils eine verschlüsselte Registration-ID. Ein Rückschluss auf den einzelnen Nutzer ist für die mHealth Pioneers GmbH nicht möglich. Rechtsgrundlage dieser Verarbeitung Ihrer Befragungsdaten und Ihrer Registration-ID für den Versand von Push-Mitteilungen ist Ihre ausdrückliche Einwilligung für die betreffenden Projekte (Art. 6 Abs. 1 lit. a und Art. 9 Abs. 2 lit. a DSGVO).

3.5. Zugriffsdaten

Bei jedem Zugriff der App auf den Server müssen Daten über diesen Vorgang vorübergehend in einer Protokolldatei verarbeitet werden. Im Einzelnen werden über jeden Zugriff folgende Daten verarbeitet: IP-Adresse, Datum und Uhrzeit des Zugriffs (Zeitstempel), Anfragedetails und Zieladresse (Protokollversion, HTTP-Methode, Referer, UserAgent-String), Name der abgerufenen Datei und übertragene Datenmenge, Meldung, ob der Abruf erfolgreich war (HTTP Status Code). Diese Daten werden für sieben Tage in Form von Protokolldateien vorgehalten und anschließend durch Kürzung der IP-Adresse anonymisiert. Dies dient der Sicherstellung des Betriebs und dem Schutz und der Aufklärung vor Angriffen.

4. Trennen von verbundenen Datenquellen

Um die Datenquellen Apple Health und Samsung Health zu trennen, genügt es, wenn Sie die App löschen. Zudem können Sie in der jeweiligen Health-App (z. B. Apple Health) die Freigabe Ihrer Daten für die App zurücknehmen. Um die Verbindung zu anderen Datenquellen zu trennen, reicht eine einfache Löschung der App nicht aus, da dadurch die Server-zu-Server-Verbindung nicht getrennt wird. Die Verbindung zu der Datenquelle wird erst getrennt, wenn das zu Ihrem Pseudonym gespeicherte Token auf dem Server abläuft oder gelöscht wird. Sie können jederzeit die Verbindung

Ihrer Datenquellen im Menüpunkt „Datenquellen“ trennen. Wurde die Verbindung mit der Datenquelle getrennt, wird das entsprechende Token auf dem Server gelöscht.

5. Beendigung der Teilnahme

Wenn Sie nicht mehr an Pulsatio teilnehmen wollen, können Sie über den Button „Nutzer löschen“ im Menü in der App sowohl Ihr Konto als auch alle damit verbundenen und gespeicherten Informationen, sowohl in der App als auch auf dem Server löschen. Daten, die zu diesem Zeitpunkt bereits in Auswertungen eingeflossen sind und veröffentlicht wurden, können aus diesen nicht mehr rückwirkend entfernt werden, da sie ausschließlich in anonymisierter Form in die Auswertungen eingegangen sind. Die vollständige Löschung der Daten kann bis zu 30 Tage in Anspruch nehmen.

6. Löschung der Daten

Ihre personenbezogenen Zugriffsdaten in den Protokolldateien werden grundsätzlich nach sieben Tagen anonymisiert.

7. Weitergabe der Daten

Personenbezogene Daten werden von uns streng vertraulich behandelt und nicht an Dritte weitergegeben. Es werden keinerlei Daten an Analysedienste wie Google Analytics oder soziale Plattformen wie Facebook übermittelt. Mit der separaten Einwilligung in Projekte erhalten nur die für die wissenschaftliche Auswertung zuständigen Projektpartner Zugriff auf die personenbezogenen Daten.

8. Datensicherheit

Die mHealth Pioneers GmbH beschränkt den Zugriff auf die übermittelten Daten auf diejenigen Mitarbeiter, die den Zugriff für die Dienstleistungserbringung benötigen. Diese sind vertraglich und/oder von Gesetzes wegen auf die Einhaltung der gesetzlichen Datenschutzbestimmungen verpflichtet.
Um Ihre Daten zu schützen, wurden umfangreiche technische und organisatorische Maßnahmen umgesetzt (z.B. Firewalls, Verschlüsselungs- und Authentifizierungstechniken, Verfahrensanweisungen). Bitte behandeln Sie Ihr Pseudonym und Ihre PIN sorgfältig und halten Sie es vor dem Zugriff durch Dritte geschützt. Bei Verlust haben Sie keine Möglichkeit mehr, die Löschung, Auskunft oder Bearbeitung Ihrer Daten zu verlangen.

9. Datenschutzrechte

Sie haben folgende Datenschutzrechte nach Art. 15-20 und 77 Abs. 1 DSGVO:

1. Das Recht, Auskunft zu verlangen, welche Daten über Sie gespeichert wurden, und diese bei Unrichtigkeit berichtigen bzw. vervollständigen zu lassen.

2. Das Recht, die Sie betreffenden personenbezogenen Daten löschen oder für die Verarbeitung beschränken zu lassen.

3. Das Recht, die von Ihnen bereitgestellten Daten in einem strukturierten, gängigen maschinenlesbaren Format zu erhalten.

4. Das Recht, eine Einwilligung jederzeit ohne Angabe von Gründen mit Wirkung für die Zukunft zu widerrufen und die Benutzung der App zu beenden, ohne dass dadurch nachteilige Folgen für Sie entstehen.
5. Die Einwilligungen bezüglich der einzelnen Projekte können Sie jederzeit widerrufen, indem Sie den Schalter zum jeweiligen Projekt deaktivieren.

6. Wenn Sie Ihre Datenschutzrechte ausüben, benötigen Sie zudem die PIN, die zusammen mit Ihrem Pseudonym generiert wird. Bitte halten Sie Ihr Pseudonym und Ihre PIN daher vor dem Zugriff durch Dritte geschützt.

7. Das Recht, sich beim Datenschutzbeauftragten des Verantwortlichen (siehe Ziffer 1) oder bei einer Datenschutzbehörde zu beschweren.

Einwilligungserklärung

Ich möchte an Pulsatio teilnehmen.

1. Ich bin einverstanden, dass die mHealth Pioneers GmbH meine Daten für die oben genannten wissenschaftlichen Zwecke auf dem Server in pseudonymisierter Form speichert und zusammen mit den Daten von anderen Teilnehmern auswertet.

2. Ich bin einverstanden, dass die Ergebnisse in anonymer Form, die keinen Rückschluss auf meine Person zulässt, veröffentlicht und dauerhaft in einer wissenschaftlichen Datenbank gespeichert werden.

3. Diese Einwilligung kann ich jederzeit widerrufen. Nachteile entstehen mir dadurch nicht. Die bis zu meinem Widerruf durchgeführten Verarbeitungen bleiben davon jedoch unberührt.

Anlage 6 – Informationstext vor Widerruf

Wir bedauern, dass Sie Ihre Einwilligung zur Teilnahme an dem Projekt widerrufen möchten!
Durch Ihren Widerruf werden Ihre Daten innerhalb der nächsten 28 Tage unwiderruflich gelöscht.
Ich möchte nur die Datenübertragung beenden, nicht aber die Teilnahme an dem Projekt.
Wenn Sie nur die Datenübertragung unterbrechen wollen, nicht aber die Teilnahme an dem Projekt widerrufen möchten, trennen Sie die Verbindung zwischen Ihrem Wearable und der Pulsatio-App. In diesem Fall werden nur die bis zum Zeitpunkt der Trennung gesammelten Daten in WATCH wissenschaftlich ausgewertet.
Sind Sie sich sicher, dass die Ihre Einwilligung zur Teilnahme an WATCH widerrufen möchten?
[Checkbox] Ja → Weiter