OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG

DeinHaus 4.0 Technik im Alltag - Technik zum Leben OBERPFALZ

TELEPRÄSENZROBOTER FÜR DIE PFLEGE UND UNTERSTÜTZUNG VON SCHLAGANFALLPATIENTINNEN UND -PATIENTEN (TEPUS) IM REGIERUNGSBEZIRK OBERPFALZ: DEINHAUS 4.0

Arbeitspapier 1.01: Datenschutzkonzept, Version 1.1

Autor*innen: Christof Popp, Prof. Dr. Georgios Raptis

Wissenschaftliche Projektleitung: Prof. Dr. Karsten Weber

Herausgeber: Ostbayerische Technische Hochschule (OTH) Regensburg

Dezember 2021

gefördert durch
Bayerisches Staatsministerium für Gesundheit und Pflege

INHALT

Das vorliegende Arbeitspapier wurde im Rahmen des Projekts „Telepräsenzroboter für die Pflege und Unterstützung von Schlaganfallpatientinnen und -patienten (TePUS) im Regierungsbezirk Oberpfalz: DeinHaus 4.0“ von Christof Popp und Prof. Dr. Georgios Raptis, eHealth Labor, OTH Regensburg erstellt.

Identifikation des Dokuments: Datenschutzkonzept, Version 1.1, eHealth Labor, OTH Regensburg
Referenz: [OTH-eH_Datenschutz_v1.1] Revisions-Datum.: 22.12.2021 18:15 Nr.:11

Das Projekt wird vom Bayerischen Staatsministerium für Gesundheit und Pflege (StMGP) im Rahmen der Projektreihe „DeinHaus 4.0“, mit der intelligente Assistenztechnik für Pflegebedürftige erforscht und für die Bürger*innen erlebbar gemacht werden sollen, gefördert. Der Projektzeitraum erstreckt sich von Oktober 2019 bis Juni 2023.

Das vorliegende Papier sowie nachfolgende Ausarbeitungen sind einzelne Arbeitsschritte im Projekt und Teil des Gesamtberichts. Die Bearbeitung der Projektteile erfolgt durch jeweils zuständige Projektmitarbeiter*innen und findet unter der Leitung von Prof. Dr. Karsten Weber an der OTH Regensburg statt.

1 Ziel und Zweck des Datenschutzkonzeptes

Im Rahmen des Forschungsprojektes „Telepräsenzroboter für die Pflege und Unterstützung von Schlaganfallpatientinnen und -patienten (TePUS)“ der Ostbayerischen Technische Hochschule Regensburg werden personenbezogene und sensible Daten erhoben, gespeichert und verarbeitet.

Das Projekt dient dazu den Einsatz von Telepräsenzrobotern zur Unterstützung der Pflege und der Genesung von Schlaganfallpatient*innen zu testen und zu erforschen. Die daraus gewonnenen Erkenntnisse sollen einer Verbesserung der Versorgung in den Bereichen Pflege, Physiotherapie und Logopädie, der Unterstützung von Schlaganfallpatient*innen und einer Entlastung der Therapeut*innen dienen.

Hierbei sollen die Fragen beantwortet werden, welche Robotertypen sich zum Einsatz eignen, welche Funktionen diese unterstützen sollten, wie die Nutzbarkeit von den Proband*innen wahrgenommen wird und welche Akzeptanz die eingesetzten Roboter mit den vorhandenen Leistungen erfahren werden. Im Rahmen des Projektes müssen zudem sowohl fachliche Grenzen des Einsatzes als auch infrastrukturelle Gegebenheiten bewertet und nachvollzogen werden. Diese sollen Aufschluss darüber geben, welchen Nutzen eine Verwendung dieser Telepräsenzroboter geben kann und welche Voraussetzungen für einen sinnvollen Einsatz erfüllt sein müssen (Weber et al, 2019).

Im Zuge dessen verfolgt das vorliegende Datenschutzkonzept das Ziel, eine Dokumentation über die geltenden datenschutzrechtlichen Aspekte, Grundprinzipien und den benötigten Datenschutzmechanismen, die zum Schutz der sensiblen und personenbezogenen Daten nötig sind, übersichtlich und transparent darzustellen. Hierbei wird beschrieben, wie der Datenschutz im Rahmen des Forschungsprojekts berücksichtigt und umgesetzt wird.

Personenbezogene oder personenbeziehbare Gesundheitsdaten werden zum Zweck der Evaluation und Ableitung von Forschungsergebnissen von den zuständigen Mitarbeiter*innen der Teilprojekte, entsprechend ihres Aufgabenbereichs und ihrer Berechtigungen einmalig erhoben und ausgewertet. Hierbei werden Daten für die physiotherapeutische Betreuung, logopädische Betreuung, pflegewissenschaftliche Betreuung sowie technische Betreuung erhoben. Der Schutz dieser Daten wird als höchste Priorität unter Einhaltung der Vorgaben und Bestimmungen der Europäischen Datenschutzgrundverordnung (DSGVO) und - sofern anwendbar - des Bundesdatenschutzgesetzes (BDSG(neu)), des Bayerischen Datenschutzgesetzes (BayDSG) und der Schweigepflicht (§ 203 StGB) angesehen.

Die Prinzipien des Datenschutzes, die im Rahmen dieses Projektes berücksichtigt werden, sind unter anderen:

- Das Persönlichkeitsrecht des Einzelnen auf informationelle Selbstbestimmung und somit die Hoheit über seine erhobenen Daten
- Wahrung der Vertraulichkeit
- Sicherung der Integrität
- Gewährleistung der Verfügbarkeit
- Schaffung von Transparenz
- Zweckbindung, Datenminimierung und Wahrung der Betroffenenrechte

Damit diese Prinzipien gewährleistet werden können, müssen bestimmte Anforderungen an den Datenschutz eingehalten werden. Hierbei müssen die Aspekte der:

- Allgemeinen Datenverarbeitung
- Verarbeitung von besonderen Arten personenbezogener Daten
- Automatisierten Datenverarbeitung
- Verarbeitung im Auftrag
- Nutzung von Internetdiensten / Telekommunikationsdiensten

besonders beachtet, berücksichtigt und behandelt werden.

2 METHODIK

Für die Erstellung des vorlegenden Datenschutzkonzeptes wurde der „Leitfaden für die Erstellung von Datenschutzkonzepten im Gesundheitswesen“ (Deutsche Gesellschaft für Medizinische Informatik et al., 2016) als Vorlage verwendet. Der Leitfaden berücksichtigt zwar u.a. das Standard-Datenschutzmodell (SDM), jedoch wurde er vor der Geltung der DSGVO und des Standard-Datenschutzmodells erstellt. Aus diesem Grund wurde der Leitfaden punktuell modifiziert, um das SDM und die DSGVO besser abzubilden. Insbesondere wurden aus dem Leitfaden, wie empfohlen, die für das vorlegende Konzept anwendbaren Begriffsdefinitionen und die Gliederung übernommen. Bei Begriffen, die jedoch explizit in der DSGVO definiert werden, wurde die Definition aus der DSGVO übernommen.

Zudem wurde das Standard-Datenschutzmodell Version 2.0b als Referenz und zusätzlicher Leitfaden verwendet. Dieses wurde in der vorliegenden Version am 17.04.2020 von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder beschlossen. Es dient als Werkzeug zur Auswahl und Bewertung technischer und organisatorischer Maßnahmen um eine DSGVO-konforme Verarbeitung von personenbezogenen Daten zu ermöglichen und als Methodologie, um eine Schwellwertanalyse durchzuführen (AK Technik der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, 2020).

Es ist schwierig, ein Datenschutzkonzept für eine Art der Datenverarbeitung ohne feste Bezugspunkte im Sinne von Best Practices zu modellieren. Im Projekt werden Gesundheitsdaten von einer geringen Anzahl (max. 100) Patient*innen durch eine überschaubare Anzahl Mitarbeiter*innen erhoben und verarbeitet. Eine Arztpraxis ist zu dieser Konstellation vergleichbar, wenngleich die Datenverarbeitung dort risikoreicher ist: Es werden Gesundheitsdaten von i.d.R. 10mal mehr Patient*innen verarbeitet inzwischen auch über telemedizinische Methoden (Videosprechstunde). Die Erhebung ist nicht einmalig für ein umschriebenes Projekt, sondern regelhaft auf Dauer. Die Daten werden nicht pseudonymisiert. Sie werden regelmäßig an externe Institutionen (andere Ärzt*innen, KV zur Abrechnung und Qualitätsmanagement usw.) weitergeleitet. Wenn also die Anforderungen an Datenschutz und Informationssicherheit, welche von den Arztpraxen erfüllt werden müssen, auch im Projekt erfüllt werden, dürften die Datenschutzrisiken ausreichend adressiert werden, insbesondere weil die Datenverarbeitung in den Arztpraxen weitaus mehr Risiken als im vorliegenden Projekt ausweist.

In diesem Sinne wurden für die Erstellung des vorliegenden Datenschutzkonzeptes zusätzlich berücksichtigt:

- die DSGVO-Anforderungen des Bayerischen Landesamtes für Datenschutzaufsicht an Arztpraxen, als Institutionen, welche vergleichbare Datenverarbeitungen vornehmen,
- die Technische Anlage aus den Hinweisen und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung von 2018,

- die Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist („Muss-Liste“) der Datenschutzkonferenz,
- das Kurzpapier Nr. 5, Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO der Datenschutzkonferenz.

Das vorliegende Datenschutzkonzept ist generisch aufgebaut. D.h. es werden Datenschutz-Aspekte in Bezug zu einem generischen Prozess der Datenverarbeitung im Projekt beschrieben. Zum gegenwärtigen Zeitpunkt sind jedoch nicht alle konkreten Datenverarbeitungen im Projekt bekannt. Neue Verfahren werden im Laufe des Projektes etabliert. Diese müssen zu den Grundsätzen dieses Datenschutzkonzeptes konform sein. Für jede einzelne Datenverarbeitung müssen dann im Sinne eines modularen Ansatzes entsprechende Festlegungen, Erklärungen, Einwilligungen usw. aufgenommen werden. Ein Verzeichnis der Verarbeitungstätigkeiten wird erstellt und laufend aktualisiert, wenn technische Aspekte im Projekt feststehen, welche konkrete Datenverarbeitungen umsetzen.

Ebenfalls werden im Laufe des Projektes externe Software, Apps, Hosting-Anbieter usw. eingesetzt. Die Datenschutzerklärungen, Verträge usw. dieser externen Instanzen und Datenverarbeitungen werden in einer Liste im Anhang dieses Dokuments referenziert. Ein Einsatz wird nur dann erfolgen, wenn die Zusicherungen aus den Datenschutzerklärungen bzw. Verträgen, den Festlegungen in diesem Datenschutzkonzept erfüllen.

3 Definitionen und Begrifflichkeiten

Die folgenden Definitionen und Begrifflichkeiten werden aus dem Leitfaden (Deutsche Gesellschaft für Medizinische Informatik et al., 2016), dem SDM (AK Technik der Konferenz der Unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, 2020) und die DSGVO entnommen. Bei anderen Quellen (z.B. DIN- oder ISO-Normen), werden diese angegeben.

Anonymisieren

Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

Auftragsverarbeitung

Die Datenverarbeitung von personenbezogenen Daten durch einen Auftragnehmer, der dies im Auftrag und nach ausdrücklicher Weisung des Projektes durchführt.

Ausdrückliche Zustimmung

Genehmigung, die aus freien Stücken und unmittelbar gegeben und entweder mündlich oder schriftlich zum Ausdruck gebracht werden. (DIN ISO IEC 27000)

Authentizität

Eigenschaft einer Einheit, das zu sein, was sie zu sein vorgibt. (Quelle: DIN ISO IEC 27000)

Automatisierte Datenverarbeitung

Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen.

Autorisierung

Erteilung von Privilegien, einschließlich des Privilegs für den Zugriff auf Daten und Funktionen. (DIN EN ISO 22600-1)

Betroffener

Ein Betroffener ist eine bestimmte oder bestimmbare natürliche Person.

Datenbeauftragter

Person, die die Verwendungszwecke der Daten und die Art und Weise, in der personenbezogene Daten bearbeitet werden oder bearbeitet werden sollen, festlegt. (DIN EN 15713)

Datenbearbeiter

Person, (anderer als die Mitarbeiter des Datenbeauftragten) die die Daten im Auftrag des Datenbeauftragten bearbeiten. (DIN EN 15713)

Datenintegrität

Eigenschaft, dass Daten nicht auf unautorisierte Art geändert oder zerstört worden sind. (DIN EN ISO 27799)

Datenlöschung

Arbeitsgang, der zur dauerhaften, unwiderruflichen Entfernung der Informationen über die betreffende Person oder den Gegenstand aus dem betreffenden Speicher oder Speichermedium führt. (DIN CEN ISO/TS 14265)

Datennutzung

Handhabung von oder Umgang mit Informationen für einen spezifischen Zweck. (DIN CEN ISO/TS 14265)

Datenschutz

Festgelegte technische und soziale Vorgehensweise für die Verhandlung, Verwaltung und Sicherstellung von Geheimhaltung, Vertraulichkeit und Sicherheit von Informationen (DIN CEN ISO/TS 14265)

Datenverarbeiter

Jegliche Personen (andere als die Mitarbeiter des Datenbeauftragten), die die Daten im Auftrag des Datenbeauftragen bearbeiten. (DIN EN 15713)

Datenverarbeitung

Jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung

oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung (Art. 4 Abs. 2 DSGVO)

Dritter

Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten. (Art. 4 Abs. 10 DSGVO)

Einwilligung

Der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. (Art. 4 Abs. 11 DSGVO)

Entpersonalisierung

Allgemeine Bezeichnung für jeden Prozess, bei dem der Bezug eines identifizierenden Datensatzes auf die betreffende Person aufgehoben wird. (DIN CEN ISO/TS 14265)

Personenbezogene Daten

Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind (Art. 4 Abs. 1 DSGVO)

Persönliche Gesundheitsinformationen

Informationen über eine identifizierbare Person, die sich auf den körperlichen oder geistigen Gesundheitszustand der betreffenden Person oder auf die Erbringung von Gesundheitsdienstleistungen für die betreffende Person beziehen.
(Quelle: DIN CEN ISO/TS 14441)

Projektteilnehmer

Ein Projektteilnehmer ist eine bestimmte oder bestimmbare natürliche Person, die dafür ausgewählt wurde und eingewilligt hat, sich an dem Projekt zu beteiligen.

Pseudonymisieren

Die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und

organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden (Quelle: Art. 4 Abs. 5 DSGVO)

Transparenz

Personenbezogene Daten müssen auf eine für die betroffene Person nachvollziehbare Weise verarbeitet werden. (Art. 5 Abs. 1a DSGVO)

Verarbeitung

Erfassung, Aufzeichnung, Aufbewahrung, Änderung, Abruf, Löschung oder Offenlegung von Daten
(Quelle: DIN CEN ISO/TS 14265)

Verfügbarkeit

Eigenschaft, auf Anforderung einer autorisierten Entität zugänglich und nutzbar zu sein
(Quelle: DIN EN ISO 22600-1)

Vertraulichkeit

Eigenschaft, die dazu führt, dass die betreffende(n) Information(en) keinen Personen, Entitäten oder Prozessen, die nicht über die entsprechende Autorisation verfügen, verfügbar gemacht oder diesen gegenüber offengelegt wird (Quelle: DIN EN ISO 22600-1)

Weisung

Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch einen Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

Datenschutzrechtliche Rahmenbedingungen

Für die Erhebung, Speicherung und Verarbeitung von Daten innerhalb des Projekts gelten die Regelungen der Datenschutzgrundverordnung.

4 Fachliche und organisatorische Hintergründe

Bei diesem Projekt handelt es sich um ein durch das Bayerische Staatsministerium für Gesundheit und Pflege gefördertes und durch ein Projektteam der Ostbayerischen Technischen Hochschule (OTH) Regensburg durchgeführtes Forschungsprojekt.

Das Projekt beschäftigt sich damit, die Möglichkeiten zur Unterstützung von Personen, die an den Folgen eines Schlaganfalls leiden, zu untersuchen. Die damit verbundene Datenerhebung und Datenverarbeitung dient dazu, Erkenntnisse über die Möglichkeiten und Voraussetzungen zur Verbesserung der Versorgung der Schlaganfallpatient*innen durch den Einsatz von unterschiedlichen Telepräsenzrobotern zu liefern.

Hierbei sollen die Fragen, welche Robotertypen sich zum Einsatz eignen, welche Funktionen diese besitzen sollten, wie die Nutzbarkeit von den Probanden wahrgenommen wird und welche Akzeptanz die eingesetzten Roboter mit den vorhandenen Leistungen erfahren, beantwortet werden. Im Rahmen des Projektes müssen zudem sowohl fachliche Grenzen des Einsatzes als auch infrastrukturelle Gegebenheiten bewertet und nachvollzogen werden. Diese sollen Aufschluss darüber geben, welchen Nutzen eine Verwendung von Telepräsenzroboter stiften kann und welche Voraussetzungen für einen sinnvollen Einsatz erfüllt sein müssen (Weber et al, 2019).

Damit diese Anforderungen und Fragen hinreichend beantwortet werden können, ist der Aufbau einer eigenen, sicheren technischen Infrastruktur notwendig. Hierfür wird den Teilnehmern ein Netzwerk, welches über eine Mobilfunkverbindung (LTE) kommuniziert, zur Verfügung gestellt. Die Kommunikation der Roboter nach Außen erfolgt mittels eines speziell dafür aufgespannten und abgesicherten Virtuellen Privaten Netzwerks (VPN).

Neben dem Regensburg Center of Health Sciences and Technology (RCHST) fungieren folgende Institutionen als Kooperationspartner (auf Grundlage von LOIs, in alphabetischer Reihenfolge):

- Asklepios Klinik Schaufling: Bereitstellung von Daten, Hilfe bei der Findung von Patientinnen und Patienten.
- Barmherzige Brüder Krankenhaus Regensburg: Unterstützung und Beratung bei der Entwicklung von Lehr- und Informationsmaterialien, Unterstützung bei Netzwerkaktivitäten, Unterstützung bei der Rekrutierung von Patientinnen und Patienten.
- Bayerische TeleMedAllianz: Unterstützung und Beratung bei der Entwicklung von Lehr- und Informationsmaterialien.
- Betriebskrankenkasse BMW (BKK BMW): Gemeinsame Informationsveranstaltungen, Austausch von Wissen bzgl. gesundheitsökonomischer Aspekte des Projekts.
- BioPark Regensburg: Unterstützung bei Netzwerkaktivitäten.
- Caritas Krankenhaus St. Josef: Unterstützung und Beratung bei der Entwicklung von Lehr- und Informationsmaterialien.
- Caritasverband der Diözese Regensburg e.V.: Allgemeine organisatorische Hilfe, Unterstützung bei Netzwerkaktivitäten, Unterstützung und Beratung bei der Entwicklung von Lehr- und Informationsmaterialien.
- Der Landrat des Landkreises Neustadt an der Waldnaab, Herr Andreas Meier: Allgemeine organisatorische Hilfe, Unterstützung bei Netzwerkaktivitäten, Unterstützung und Beratung bei der Entwicklung von Lehr- und Informationsmaterialien.
- Deutscher Bundesverband für Logopädie e.V. (dbl): Unterstützung und Beratung bei der Entwicklung von Lehr- und Informationsmaterialien, Unterstützung bei Netzwerkaktivitäten.
- Die Oberbürgermeisterin der Stadt Regensburg, Frau Gertrud Maltz-Schwarzfischer: Allgemeine organisatorische Hilfe, Unterstützung bei Netzwerkaktivitäten, Unterstützung und Beratung bei der Entwicklung von Lehr- und Informationsmaterialien, Unterstützung bei der Rekrutierung von Proband*innen.
- Die Landrätin des Kreises Regensburg, Frau Tanja Schweiger: Allgemeine organisatorische Hilfe, Unterstützung bei Netzwerkaktivitäten, Unterstützung und Beratung bei der Entwicklung von Lehr- und Informationsmaterialien.

- Universitätsklinikum Regensburg, Klinik und Poliklinik für Hals-Nasen-Ohren-Heilkunde sowie Phoniatrie und Pädaudiologie: Wissenschaftliche Begleitung insbesondere bei Fragen der Logopädie.

Diese Liste kann während des Projektverlaufes erweitert werden, da neue Kooperationspartner für das Projekt hinzukommen können.

5 Beschreibung und Zielsetzung des Vorhabens

5.1 Ziele

Die allgemeine Beschreibung und Zielsetzung des Projektes wird in Kap. 4 und insbesondere im Projektantrag (Weber et al., 2019) erläutert. Anbei eine repräsentative Auswahl von relevanten Punkten:

Die Studie dient der Untersuchung des Nutzens, der Akzeptanz sowie möglicher Anwendungsrisiken eines Einsatzes von verschiedenartigen Telepräsenzrobotern bei Schlaganfallpatient*innen. Die aus diesen Untersuchungen gewonnenen Ergebnisse sollen bestehende Forschungslücken schließen. Dies geschieht durch die Bereitstellung eines Telepräsenzroboters und eines dazu ausgerichteten für die Patient*innen erarbeiteten Pflege- und Therapieangebots. Die Telepräsenzroboter werden auf Praxistauglichkeit geprüft und auf Basis der vorhandenen Fähigkeiten und Anforderungen der Geräte, Therapeut*innen und Patient*innen ein Unterstützungsangebot entwickelt. Die Unterstützung und die Akzeptanz der eingesetzten Roboter werden in mehreren Teilschritten evaluiert.

Der Einsatz der Maßnahmen wird so gestaltet, dass bereits bestehende Behandlungen nicht beeinträchtigt werden. Es ist nicht Ziel, etablierte Pflege- und Therapiemaßnahmen durch die Telepräsenzroboter zu ersetzen, sondern sie durch Technik zu unterstützen.

Für die Studie wurden folgende Forschungsfragen formuliert (vgl. Weber et al. 2019; Haug et. al. 2020, Ettl et al. 2020):

- Wie hoch sind Akzeptanz und Nutzungsbereitschaft technischer Assistenzsysteme (Telepräsenzroboter) bei Schlaganfallpatient*innen, bei ihren Angehörigen sowie bei Stakeholdern im beruflich-gesundheitlichen Umfeld der Zielgruppe?
- Welche Faktoren beeinflussen Akzeptanz und Nutzungsbereitschaft technischer Assistenzsysteme (Telepräsenzroboter) bei Schlaganfallpatient*innen, bei ihren Angehörigen sowie bei Stakeholdern im beruflich-gesundheitlichen Umfeld der Zielgruppe?
- Welche Auswirkungen zeigt der Einsatz der technischen Assistenzsysteme (Telepräsenzroboter) bei den anwendenden Personen im ethischen, rechtlichen, sozialen und gesundheitsökonomischen Kontext?
- Welche Unterschiede ergeben sich bei unterschiedlichen Telepräsenzrobotern (Gerätevergleich), insbesondere in Bezug auf die Einstellung zur Nutzung?
- Welcher Mehrwert, welche Risiken und welche besondere Anforderungen (technisch, organisatorisch und kompetenzorientiert) sind mit einem Einsatz der Assistenzsysteme verbunden?

    (1) Welche Auswirkungen zeigen sich in Bezug auf Kommunikation, soziale Teilhabe, Sicherheit im Alltag und Mobilität bei den Patient*innen?

(2) Welche ethischen Leitlinien ergeben sich aus und für den Einsatz von technischen Assistenzsystemen?

(3) Welche datenschutzrechtlichen Fragen müssen durch den Einsatz von technischen Assistenzsystemen beantwortet und geklärt sein?

(4) Wie lässt sich die Technologie in die Arbeitsprozesse der beteiligten Stakeholder einbetten?

- Welche ökonomischen Potenziale sind mit einem Einsatz verbunden?
- Evaluierung der Machbarkeit und ggf. auch der Wirksamkeit der eingesetzten technischen Assistenzsysteme im pflegerischen und therapeutischen Kontext
- Inwieweit sind technische und organisatorische Nutzungskompetenzen sowie die Nutzungsbereitschaft bei Schlaganfallpatient*innen und Angehörigen gegeben?
- Inwieweit wirken sich regelmäßige Telenursingangebote in Form von Beratung und Begleitung auf die Anwendung der Telepräsenzangebote aus?
- Inwieweit können durch den Einsatz der Apps kognitive Fähigkeiten (v.a. Aufmerksamkeit, Gedächtnis) und Kommunikationshäufigkeit erhöht, Vereinsamung vorgebeugt und krankheitsspezifisches Wissen erworben werden?
- Inwieweit lässt sich ein Zusammenhang zwischen Telenursingangeboten in Form von Beratung und Begleitung sowie der Nutzung von Apps und der selbst eingeschätzten Lebensqualität der Schlaganfallpatient*innen und deren Angehörigen nachweisen?
- Wie erleben Schlaganfallpatient*innen und Angehörige den Einsatz von Telepräsenzrobotern in ihrem Alltag?
- Wie beeinflusst die Anwendung von Telepräsenzrobotik die Stimmung, die soziale Teilhabe und das Sicherheitsempfinden von Schlaganfallpatient*innen und Angehörigen?
- Welchen Einfluss hat der Einsatz von Telepräsenzrobotern auf körperliche und kognitive Fähigkeiten sowie kommunikative Aktivität bei Schlaganfallpatient*innen und Angehörigen unter krankheitsspezifischen, umwelt- und personenbezogenen Einflussfaktoren?
- Gibt es Risiken die durch die Nutzung von Telepräsenzrobotern und Telenursingangeboten im häuslichen Setting von Schlaganfallpatient*innen auftreten können?
- Welchen Informations- und Beratungsbedarf haben die standardmäßigen und intensiv begleiteten Schlaganfallpatient*innen und Angehörigen bei den Videosprechstunden?
- Sind teletherapeutische Angebote aus dem Bereich Logopädie und Physiotherapie im Einzel- und Gruppensetting für Menschen nach Schlaganfall über Telepräsenzroboter in der häuslichen Umgebung umsetzbar?
- Ist eine integrierte physio- und sprachtherapeutische Gruppenintervention machbar?
- Profitieren die Proband*innen von den Interventionen im Hinblick auf Funktion, Aktivitäten, Teilhabe und Lebensqualität?
    a. Gibt es einen erhöhten Gebrauch des betroffenen Armes im Alltag?

   b. Haben die Interventionen einen Einfluss auf die Kommunikationsfähigkeit?

- Wie erleben die Proband*innen die Interventionen im Telepräsenzsetting und die Eigenübungen?
   a. Welche Bestandteile der Interventionen empfinden die Proband*innen als nützlich?
   b. Wie ist das Erleben der selbständigen Übungsdurchführung?
   c. Wie wird die VR-Brille in Bezug auf Motivation und Freude am Üben erlebt?
- Welche Unterschiede ergeben sich hinsichtlich Umsetzbarkeit, Wirkung und subjektivem Erleben in Abhängigkeit vom genutzten Robotersystem?
- Lassen sich Prädiktoren für den Nutzen der Interventionen identifizieren?

Mit dem vom Gesundheitsministerium bewilligten, Forschungsprojekt sind die folgenden Ziele verbunden:

- Lebensqualität der pflegebedürftigen Personen aufgrund eines Schlaganfalls verbessern
- Qualität und Quantität der Pflegeleistungen selbst verbessern
- Arbeitsbedingungen professioneller Pflegekräfte ebenso wie informell Pflegender verbessern
- Akzeptanz von Pflegetechnik mit besonderer Berücksichtigung von Telepräsenzrobotern bei allen Stakeholdern verbessern
- Kosten-Nutzen-Relation von Technik mit besonderer Berücksichtigung von Telepräsenzrobotern in der Pflege- und Gesundheitsversorgung verbessern

(Weber et al., 2019).

Damit diese Fragen beantwortet werden können, ist im Laufe des Projekts die Auswertung von erhobenen Daten notwendig. Hierbei werden:

- Nutzungsdaten
- Technische Daten zum Betrieb
- Gesundheitsdaten
- Daten aus Interviews
- Daten aus Fragebögen
- Daten aus therapeutischen Assessments
- Administrative personenbezogene Daten
- soziodemografische Daten

von den Mitarbeiter*innen des Projektes erhoben und verarbeitet.

5.2 Zweckbestimmung, Anonymisierung oder Pseudonymisierung

Im Projekt werden sowohl technische Daten als auch Gesundheitsdaten erhoben und verarbeitet. Diese dienen folgenden Zwecken:

- geeignete Teilnehmer für das Projekt zu rekrutieren
- die im Kap. 5.1 festgelegten Ziele zu erreichen.

Für die Veröffentlichung von Forschungsergebnissen werden die aggregierten und statistisch verarbeiteten Daten **anonymisiert**.

Für die Verarbeitung der Daten im Projekt zum Zwecke der Analyse und Statistik ist es notwendig, Verläufe zu erkennen und eine Zuordnung von Robotern und

Patient*innen herzustellen. Eine Anonymisierung kann deshalb hier nicht vorgenommen werden. Die Daten werden **pseudonymisiert**. Die Zuordnung der Pseudonyme wird separat von den Daten und zugangsbeschränkt (z.B. Papierliste in abgeschlossenen Schrank oder passwortgeschützter Rechner oder verschlüsselte Datei) aufbewahrt; Zugang wird nur autorisierten Personen im 4-Augen-Prinzip gewährt.

Für die Rekrutierung der Patient*innen, für die Lieferung der Roboter (inkl. Lieferscheine, Leihscheine, Reisekostenabrechnungen usw.) und technische Unterstützung vor Ort sowie für die unmittelbare Erhebung der Daten im Rahmen einer Therapiesitzung oder pflegerischen Maßnahmen ist die **Identität der Personen** sowie weitere personenbezogene Daten (z.B. Adresse, Telefonnummer, IP-Adresse, SIM-Karten-Nr.) notwendig. Diese Daten werden nur für die vorgesehenen Zwecke verarbeitet, für welche die Identitäts- bzw. identifizierenden Angaben auch erforderlich sind. Sie können dann zwar auch weiter im Projekt verarbeitet werden (z.B. Analyse der Befunde), jedoch erst nach entsprechender Pseudonymisierung oder Anonymisierung.

5.3 Zu verarbeitende Daten

Sowohl gesundheitsbezogene Daten als auch nicht gesundheitsbezogene, personenbeziehbare Daten werden zum Erreichen von Forschungsergebnissen und zur Beantwortung der für das Projekt relevanten Fragen und Ziele erhoben und ausgewertet. Daraus ergibt sich ein sehr hoher Schutzbedarf der erhobenen Daten.

Für die gesundheitswissenschaftlichen Aspekte des Projekts ist es notwendig, gesundheitsbezogene Daten zu erheben und auszuwerten. Mit Hilfe dieser kann festgestellt werden, ob eine Person sich eignet, an der Studie teilzunehmen und welche Auswirkung der Einsatz der unterschiedlichen Geräte auf die Betroffenen hat. Dafür sind die folgenden Anforderungen bzw. Datenarten derzeit bekannt:

- Kontaktdaten
- Gesicherte medizinische Diagnose Schlaganfall mit Rückkehr nach Hause
- Einwilligungsfähigkeit
- Kognitive Beeinträchtigung
- Kommunikative Beeinträchtigungen (Sprache und Sprechen)
- Sensomotorische Beeinträchtigung
- Einschränkung der sozialen Teilhabe
- Alltagsfähigkeit
- Psychische Gesundheit
- Schwere der Erkrankung
- Sprachkenntnisse (deutsche Sprache)
- Lebensqualität
- Allgemeine Technikkompetenz und Technikakzeptanz
- Akzeptanz und Nutzung von Telepräsenzrobotern, Zahlungsbereitschaft
- Einstellungen und Verhalten in den Dimensionen soziale Teilhabe, Kommunikation, Partizipation, Mobilität, Sicherheit, Datenschutz und Datensicherheit
- Soziodemographische Variablen (Alter, Geschlecht, Bildungsabschluss, verfügbares Einkommen, Haushaltsgröße, Haushaltszusammensetzung, Wohnform und Wohnortgröße)
  (Haug et al. 2020)

Weiterhin werden folgende Daten aus technischer Sicht benötigt:

- Netzanbindung

- Name, Adresse, Telefonnummer, E-Mail-Adresse und ggf. weitere technische Nutzernamen und Identifikatoren (z.B. SIM-Nr. oder Username bei einem externen Dienst) für die Lieferung der Roboter und die technische Unterstützung (z.B. Fehlerbehebung)
- Technische Protokolle (Logs), IP-Adressen, technische Nutzungsdaten für die Fehlerbehebung

Im Rahmen der therapeutischen Interventionen und Maßnahmen werden entsprechende Daten aus der Patient*innen-Therapeutin-Beziehung zur Dokumentation der Behandlung erhoben und gespeichert. Diese werden auch im Projekt ausgewertet, jedoch erst nach Pseudonymisierung durch die Therapeut*innen selbst oder – falls ein/e Therapeut*in nicht Mitarbeiter*innen des Projektes sein sollte und die Pseudonymisierung selbst nicht vornehmen kann – unmittelbar nach Empfang der Daten durch ein/e Projektmitarbeiter*in.

Daten – auch personenbeziehbare Gesundheitsdaten – für die wissenschaftliche Analyse und Evaluation zwecks Beantwortung der Forschungsfragen, jeweils pseudonymisiert (falls Wiedererkennung zur Nachverfolgung / Therapieverlauf notwendig) oder anonymisiert. Z.B.

- Ausgefüllte Fragebögen oder aufgenommene Interviews
- Inhalte aus der Patientenakte
- Effekte von Therapiemaßnahmen inkl. Bild-, Video- oder Audio-Aufnahmen
- Effekte des Einsatzes der Telepräsenzroboter
- Nutzungsdaten der eingesetzten Apps und der technischen Infrastruktur

Weiterhin werden aus allen o.g. Datenklassen statistisch analysierte und aggregierte Daten verarbeitet und veröffentlicht (z.B. in wissenschaftlichen Publikationen), jedoch ohne Personenbezug, d.h. anonymisiert.

5.4 Rechtsgrundlage der Datenverarbeitung

Nach Art. 9 Absatz 2 Punkt a) der Datenschutzgrundverordnung ist die Verarbeitung besonderer Kategorien personenbezogener Daten durch die ausdrückliche Einwilligung der betroffenen Person gestattet. Da die in dem Projekt erhobenen Daten unter diese Kategorie fallen, erfolgt die Erhebung, Speicherung und Verarbeitung der Daten nur nach Einwilligung der Betroffenen nach Art. 7 der Datenschutzgrund-verordnung.

5.5 Lebenszyklus personenbezogener Daten

5.5.1 Erhebung

Die Datenerhebung findet direkt bei den Betroffenen (im Folgenden auch: Projekt-teilnehmer*innen, Proband*innen) oder – nach Einwilligung der Projektteil-nehmer*innen – bei Kooperationspartnern des Projektes (z.B. Angaben aus Patientenakte) statt. Hierbei werden Daten einerseits erhoben indem Fragebögen, Befragungen, Untersuchungen und Therapiemaßnahmen mit den Projekt-teilnehmer*innen durchgeführt werden und andererseits, indem Daten, die durch die Nutzung der Telepräsenzroboter gesammelt wurden, abgerufen und ausgewertet werden. Hierbei werden die Daten stets nur von den dafür zuständigen und berechtigten Mitarbeiter*innen des Projektes verarbeitet.

Jegliche Datenerhebung findet nur mit der Einwilligung der Teilnehmer*innen statt und kann jederzeit wiederrufen werden.

Im Folgenden werden die übergeordneten organisatorischen und personellen Prozesse der Datenerhebung und Datenverarbeitung aufgelistet (vgl. Haug et al. 2020, 10f.):

Phase 1 – Rekrutierung, Screening und Anfrage zur Teilnahme

- Stichprobe A
  Die Rekrutierung wird mithilfe von Kooperationspartnern des Projektes durchgeführt.
- Screening
  Das Screening der Proband*innen erfolgt durch die Kooperationspartner*innen des Projektes; diese erfragen eine Teilnahme an Erhebung t1 und vermitteln den Kontakt zu den Proband*innen.

Der Phase der Rekrutierung und des Screenings der Proband*innen der Zielgruppe A erfolgt über die gesamte Laufzeit des Projekts und erstreckt sich im Idealfall auf einen Zeitraum von 30 Monaten, bis die Ausschöpfung von n=100 Personen erreicht ist.

Phase 2 – Erhebung t1

Mittels eines standardisierten Fragebogens werden für das „ELSI"-Teilprojekt relevante Daten (soziodemographische Daten, Daten zur Lebensqualität, Daten zur Technikkompetenz, Technikakzeptanz, Einstellungsvariablen, s. Punkt 5.3) von den Proband*innen erhoben. Die Patient*innen können dem Studienpersonal ihre Kontaktdaten hinterlassen, um weiter an der Studie teilzunehmen.

Phase 3 Zuteilung der Geräte zur Stichprobe:

- Liegt eine Einverständniserklärung zur Teilnahme an der Studie vor, werden die Geräte auf die Stichprobe verteilt. Die Stichprobe wird für die Beantwortung der pflege- und therapiewissenschaftlichen Fragestellungen in drei Untergruppen eingeteilt (Ettl et al. 2020).
- Terminvereinbarung für die anschließende Installation

Phase 4: Installation und Einweisung

- Installation und Verteilung der Geräte durch die Mitarbeiter*innen des Teilprojektes eHealth
- Nutzungseinführung durch die zuständigen Mitarbeiter*innen
- Erhebung und Befundung gesundheitswissenschaftlicher Daten für die Fragestellungen in Teilprojekt 2
- Kontinuierliche technische Unterstützung und Fehlerbehebung

Phase 5: Erhebung t2

- Mittels eines standardisierten Fragebogens werden für das „ELSI"-Teilprojekt relevante Daten (Soziodemographische Daten, Daten zu Lebens-, Wohnform und Lebensqualität, Daten zur Technikkompetenz, Technikakzeptanz, Einstellungsvariablen, s. Punkt 5.3) von den Proband*innen erhoben.

Parallel zu der Erhebung bei den Probanden werden auch Daten bei Personen erhoben, die den Probanden nahestehen. Hierbei werden Daten betreffend der:

- Lebensqualität
- Technikkompetenz und Technikakzeptanz

- Akzeptanz und Nutzung von Telepräsenzrobotern
- Einstellungsvariablen
- Soziodemographische Variablen

erhoben.

Phase 6

Erheben von Daten mittels qualitativer leitfadengestützter Interviews. Die Interviews werden an einem Ort durchgeführt, der durch den Probanden gewählt werden kann.

Die erhobenen Daten werden, falls dies nicht durch Mitarbeiter*innen vor Ort geschieht, für eine Auswertung und die Speicherung von den genutzten Anwendungen oder den Projektteilnehmern selbst an die zuständigen Mitarbeiter*innen übermittelt.

Kontinuierlich findet während des Geräteeinsatzes eine Evaluation der Geräte aus therapie- und pflegewissenschaftlicher Sicht statt (Ettl et al. 2020).

- Pflegerische und therapeutische Maßnahmen, mit Unterstützung durch die Technik des Projektes
- Kontinuierliche Evaluierung therapeutisch ausgerichteter Apps
- Kontinuierliche Evaluierung therapeutisch ausgerichteter Inhalte
- Kontinuierliche Evaluation des Einsatzes der Roboter

Im Folgenden werden die übergeordneten organisatorischen und personellen Prozesse der Datenerhebung und Datenverarbeitung aufgelistet der Bereiche Physiotherapie, Logopädie und Sozialwissenschaften, (vgl. Ettl et al. 2020):

Die Datenerhebung erfolgt mithilfe von quantitativen und qualitativen Erhebungsinstrumenten. Die Erhebung der Daten erfolgt durch die Auswertung von Nutzungsdaten der eingesetzten Apps und, in dem Leitfadeninterviews durchgeführt werden.

Beim Erstkontakt mit den betroffenen Personen werden Daten bezüglich der Lebensqualität sowie der Technikakzeptanz erhoben (Fragestellungen des ELSI-Teilprojekts).

Jeder der wissenschaftlichen Teilbereiche verwendet für die im Folgenden geschilderten Datenerhebungsprozesse eine eigene Vorgehensweise und unterschiedliche Anwendungen.

Teilbereich „Pflege“:

Die Pflege erhebt in verschiedenen Phasen der Untersuchung die, durch den/die Patient*innen selbst eingeschätzte, Lebensqualität anhand einer geeigneten Methode.

Während der Teilnahmedauer werden unterschiedliche Anwendungen verwendet, um Daten über die Nutzungshäufigkeit, Nutzungsbreite und den Erfolg von Übungsprogrammen zu gewinnen. Diese Daten werden nach Beendigung der Partizipation von den Anwendungen ausgelesen und ausgewertet.

Es erfolgen während der Nutzungsdauer Telesprechstunden mittels einer durch das Projekt als geeignet eingestuften Applikation, um eine Evaluation der Telepräsenzroboter zu erlauben. Zum Ende der Erhebungsphase werden leitfadengestützte Interviews mit einigen Teilnehmer*innen und einigen Angehörigen durchgeführt

Teilbereich „Logopädie“:

Die für die Logopädie relevanten Daten werden mithilfe von verschiedenen quantitativen und qualitativen Methoden erhoben. Diese sollen die Beeinträchtigung der Teilnehmer*innen und die durch die Behandlung erzielten Erfolge in Form von auswertbaren Daten verfügbar machen. Hierbei werden unterschiedliche Testverfahren verwendet, welche mit den Patient*innen durchgeführt werden. Darüber hinaus erfolgt eine Auswertung der durch die genutzten Anwendungen gewonnenen Daten.

Im Laufe der Teilnahme der behandelten Personen werden in Abhängigkeit von individuellem Therapiebedarf Einzel- und/oder .Gruppeninterventionen durchgeführt. Hierbei werden für die Teilnahme im Vorfeld verschiedene Parameter und während der Intervention behandlungsrelevante Daten erhoben.

Mit einer Untergruppe der betroffenen Personen werden halbstrukturierte Leitfadeninterviews durchgeführt.

Teilbereich „Physiotherapie“

Die für die Physiotherapie relevanten Daten werden mithilfe von verschiedenen quantitativen und qualitativen Methoden erhoben. Diese sollen die Beeinträchtigung der Teilnehmer*innen und die durch die Behandlung erzielten Erfolge in Form von auswertbaren Daten, anhand von Indexdaten und durch die Teilnehmer*innen selbst definierten Zielen verfügbar machen. Hierbei werden unterschiedliche Testverfahren verwendet, welche mit den Patient*innen durchgeführt werden. Zudem werden die durch Anwendungen gewonnenen Daten ausgewertet.

Im Laufe der Teilnahme der behandelten Personen werden in Abhängigkeit von individuellem Therapiebedarf Einzel- und/oder Gruppeninterventionen durchgeführt. Hierbei werden für die Teilnahme im Vorfeld verschiedene Parameter und während der Intervention behandlungsrelevante Daten erhoben.

Mit einer Untergruppe der betroffenen Personen werden halbstrukturierte Leitfadeninterviews durchgeführt.

Aus diesen übergeordneten Prozessen werden konkrete Prozesse abgeleitet, wenn alle technischen Aspekte und Werkzeuge feststehen. Diese werden im Verzeichnis von Verarbeitungstätigkeiten aufgelistet.

5.5.2 Übermittlung und Speicherung

Personenbezogene Daten nach diesem Datenschutzkonzept werden übermittelt und gespeichert:

- Dezentral bei den Telepräsenzrobotern und assoziierten mobilen Geräten (Tablets)
- Auf Rechner und projektbezogenen mobilen Geräten (Tablets) der Therapeut*innen
- Auf Server an der OTH Regensburg / RCHST, zugangsbeschränkt nur für Mitarbeiter*innen des Projektes sowie davon beauftragte Administratoren (Mitarbeiter*innen der OTH Regensburg nach entsprechender Vertraulichkeitserklärung)
- Über Netze und Kommunikationsserver externer Anbieter (z.B. Mobilfunknetze oder Videokonferenzdienste) bei denen entweder eine Listung als Telekommunikationsanbieter bei der Bundesnetzagentur vorliegt oder eine Datenschutzerklärung haben und einen Vertrag zur Auftragsverarbeitung

unterzeichnet haben oder technisch sichergestellt ist, dass Daten durch Verschlüsselung dem Anbieter nach dem Stand der Technik nicht offenbart werden können.
- Ggf. auf Server externer Anbieter, welche in der EU ansässig sind, eine DSGVO-konforme Datenschutzerklärung haben und einen Vertrag zur Auftragsverarbeitung unterzeichnet haben (Hosting / Cloud-Plattform)
- Auf Server externer Anbieter **auch ggf. außerhalb der EU und ohne Vertrag zur Auftragsverarbeitung sofern der/die Patient*innen selbst – nach entsprechender durch Projektmitarbeiter*innen dokumentierter, objektiver, gut verständlicher Aufklärung der Umstände, Folgen und Risiken der Nutzung – sich dafür entscheidet und die Datenverarbeitung selbst (ggf. mit Hilfe von Projektmitarbeiter*innen) technisch initiiert[1]. Der Zweck dafür ist, den Effekt einer solchen damit verbundenen Verarbeitung zu erforschen. Voraussetzung für eine solche Verarbeitung ist, dass mögliche Alternativen umfassend geprüft wurden und im Ergebnis keine andere Möglichkeit ersichtlich ist, das Forschungsziel mit Hilfe einer alternativen, DSGVO-konformen Verarbeitung zu erreichen.**

Für die Erhebung, Übermittlung und Verarbeitung der Daten werden unterschiedliche technische Systeme eingesetzt. Diese Systeme sind voraussichtlich (im Laufe des Projektes könnten weitere Systeme hinzukommen, welche jedoch zu den o.g. Systemen vergleichbar sein müssen):

- Telepräsenzroboter
- Hosting-Plattformen mit Managed Security (C5-Testat oder vergleichbare Zusicherungen) unter den Bedingungen einer DSGVO-konformen Auftragsverarbeitung. Diese können die nachfolgenden Dienste und Systeme wahlweise anbieten.
- Kommunikationsserver (z.B. Signalling-Server für eine Videokommunikation, Messaging Server oder eine Nextcloud-Instanz)
- VPN-Konzentratoren, Firewalls, Netzwerkkomponenten (Router, Switches usw.)
- Datenbanken und zugehörige Anwendungen für die Speicherung, Verwaltung und Auswertung von Projektdaten
- Videokommunikationsprogramme
- Software-Anwendungen für Physiotherapie, Logopädie, Pflege, eHealth
  (1) Auf die Telepräsenzroboter und damit assoziierten mobilen Geräten
  (2) Auf Geräte bei den Therapeut*innen
- Software-Anwendungen für Sozialwissenschaften
- Statistik-Software
- Analyse-Software z.B. für Log-Auswertung und Fehlerbehebung
- Fernwartungssoftware für die Roboter
- Projektmanagement-Systeme und Office-Anwendungen (z.B. für die Planung von Hardware-Lieferungen und Terminen oder die Erstellung von Schreiben und Präsentationen)
- Cloud-Plattformen auch außerhalb der EU und ohne DSGVO-konforme Auftragsverarbeitung (z.B. für Spracherkennung oder den Einsatz bestimmter Apps), unter der Bedingung, dass der/die Patient*innen selbst – nach

[1] Ein Beispiel für solche Dienste wäre Amazon Alexa für die Spracherkennung, insbesondere unter dem Aspekt möglicher Einschränkungen durch einen Schlaganfall. Es gibt andere Forschungsprojekte, welche gezielt und ausschließlich den Effekt von weit verbreiteten nicht-EU Diensten, wie Facebook usw. wissenschaftlich untersuchen. Sie sind für die Forschung wichtig und auch durchführbar, d.h. nicht verboten. Durch die zusätzliche, freiwillige, zudem von den Patient*innen selbst initiierte Nutzung, wird der Einsatz ausreichend legitimiert.

entsprechender dokumentierter Belehrung und ggf. Hilfe durch Projektmitarbeiter*innen insb. zu möglichen Risiken – sich dafür entscheidet und die Datenverarbeitung selbst technisch initiiert (s.o. sowie Fußnote)

Für die Auswertung der Daten werden für die statistische Auswertung das Computerprogramm SPSS und für die Auswertung der Interviewdaten MAXQDA verwendet.

5.5.3 Aufbewahrungs- und Löschfristen

dieser Daten mit Personenbezug sind:

- Für administrative Daten (z.B. Leih- und Lieferscheine, Lieferantendaten, Dokumentationen, Abrechnungen, Beschäftigtendaten, personenbezogene Daten zu Geschäftszwecken im Projekt usw.): die Frist ergibt sich aus den jeweiligen gesetzlichen Vorgaben (z.B. HGB).
- Gesundheitsdaten, unmittelbar zur Dokumentation von Behandlungen: die Frist ergibt sich aus den gesetzlichen Vorgaben (z.B. 10 bis 30 Jahre für medizinische Daten unterschiedlicher Klassen)
- Daten, welche im Projekt für die Beantwortung der Forschungsfragen verarbeitet werden: nach etablierter wissenschaftlicher Praxis bzw. als Anforderung für die wissenschaftliche Verwertung dieser Daten wird eine Frist von max. 10 Jahren nach Beendigung des Projektes zugrunde gelegt.
- Liste mit Zuordnung der Pseudonyme zu den Identitätsdaten: 6 Monate nach Beendigung des Projektes.
- Datenschutzrechtliche Einwilligungen: Um die Nachweisbarkeit, dass die Datenerhebung und Verarbeitung zu dem Zeitpunkt, an dem diese durchgeführt wurden, zu gewährleisten, werden diese genauso lange aufbewahrt wie die erhobenen Daten selbst: max. 10 Jahre.

5.5.4 Migration der Daten

Eine Migration von Daten könnte stattfinden, falls Systeme aus technischen oder administrativen Gründen ausgetauscht werden müssen. In diesem Fall wird durch geeignete technische und organisatorische Maßnahmen im Projekt sichergestellt, dass geschützte Daten weiterhin demselben Schutz unterliegen, wie im ursprünglichen System.

5.6 Maßnahmen zur Zugriffsverhinderung

5.6.1 Löschung

Eine Löschung der Daten nach den Fristen aus Kap 5.5.3 wird so vorgenommen, dass die Daten tatsächlich unwiederbringlich gelöscht werden. Papierdaten werden nach den geltenden Bestimmungen geshreddert oder zur Vernichtung einem Dienstleister (mit entsprechendem Vertrag mit Zusicherungen) übergeben. Festplatten werden durch Überschreiben aller Sektoren mit einem low-level Befehl (z. B. sudo dd if=/dev/null of=/dev/sda1) gelöscht. Tablets werden nach der Anleitung des Herstellers auf Werkseinstellungen zurückgesetzt, unter der Voraussetzung, dass damit eine physikalische Löschung verbunden ist oder die Daten kryptographisch nicht mehr zugänglich gemacht werden können (Löschung des Schlüssels). Für SSD-Datenträger werden die Anweisungen des Herstellers befolgt oder die Speicherchips des Datenträgers physisch zerstört.

Bei einem Widerruf der Einwilligung seitens eines/einer Betroffenen müssen die Daten ebenfalls gelöscht werden (Ausnahmen davon s. Kap. 5.6.2). Die o.g. Maßnahmen der physikalischen Löschung sind jedoch dafür nicht selektiv genug (d.h. dadurch werden auch Daten anderer Betroffenen gelöscht), so dass eine physikalische Löschung

technisch nicht machbar bzw. verhältnismäßig ist. Es findet eine logische Löschung der Daten, die somit nicht weiter zugänglich sind. Eine Löschung anonymisierter Daten wird in dem Kontext der Widerruf einer Einwilligung nicht vorgenommen, weil sie einer Person nicht mehr zugeordnet werden können.

5.6.2 Einschränkung der Verarbeitung nach Art. 18 DSGVO (früher: Sperrung)

Eine Einschränkung der Verarbeitung findet auf Wunsch eines/einer Betroffenen oder bei einem Widerruf der Einwilligung statt, falls seine/ihre Daten bereits für Studien analysiert und ausgewertet wurden. In diesem Fall kann eine Löschung nicht mehr vorgenommen werden, weil damit die Validität der wissenschaftlichen Ergebnisse kompromittiert wird (gemäß Art. 17 Abs. 3 Punkt d DSGVO). Deshalb wird deren Verarbeitung eingeschränkt, d.h. die Daten werden nicht mehr für weitere Projekt- und Studienzwecke verarbeitet.

5.6.3 Anonymisierung

Eine Anonymisierung von Daten findet dann statt, wenn im Projekt weder Identitätsdaten noch eine Wiedererkennung (z.B. für Verlaufskontrolle oder Korrelation von Daten derselben Person) benötigt werden. Typischerweise werden bereits analysierte und aggregierte Daten z.B. vor einer Publikation anonymisiert. Die Anonymisierung findet nachfolgendem Schema statt:

- Entfernung aller persönlichen Daten sowie aller damit verbundenen Identifikatoren (Pseudonyme, Nummer mit Personenbezug usw.)

- Untersuchung, ob die damit anonymisierten Datensätze einzigartige Datenkombinationen enthalten, welche eine Re-Identifikation mit vertretbarem Aufwand ermöglichen. In diesem Fall werden nach dem Stand der Wissenschaft geeignete Techniken angewandt, um das Risiko einer Re-Identifikation zu reduzieren.

5.6.4 Pseudonymisierung

Für die im Projekt erhobenen und verarbeiteten Daten ist eine Pseudonymisierung vorgesehen, sofern die Ziele des Projektes durch eine Anonymisierung nicht erreicht werden können, z.B. sofern eine Korrelation von Datensätzen oder eine Verlaufskontrolle und somit eine Wiedererkennung von Betroffenen notwendig ist.

Die eingesetzten Roboter werden mit zufälligen Studien-IDs versehen. Diese sind eindeutig und werden jeweils einem/einer Teilnehmer*in zugewiesen. Alle Daten werden mit dieser ID erhoben. Die Zuordnung befindet sich in einer geschützten und nur durch berechtigte Mitarbeiter*innen zugreifbare Datei oder Liste. Alle Daten, die verarbeitet und gespeichert werden, beinhalten diese ID anstatt der personenbeziehbaren Daten. Die Pseudonymisierung wird detailliert im Forschungsdesign zum Teilprojekt der ELSI-Befragung (Haug et al. 2020, 12f.) beschrieben.

Auch für die pseudonymisierten Daten wird das Risiko einer unbefugten Re-Identifikation evaluiert und ggf. Maßnahmen nach dem Stand der Wissenschaft zur Reduzierung ergriffen.

6 Akteure und Beteiligte

Das Projekt und die damit verbundene Erhebung und Auswertung von Daten werden durch die Mitarbeiter*innen aus den Teilprojekten Physiotherapie, Logopädie, Pflegewissenschaften, ELSI-Begleitforschung und eHealth durchgeführt. Die jeweiligen

Teilprojekte besitzen jeweils eine/n Professor*in als Teilprojektleiter, welche/r Weisungsbefugnisse über die dort angestellten Mitarbeiter*innen haben. Daten werden bei den am Projekt teilnehmenden Pflegebedürftigen durch Betreuung und Befragung erhoben.

- eHealth: Luise Middel und Christof Popp
- Technikfolgenabschätzung und angewandte Ethik: Dr. Debora Frommeld
- Sozialforschung: Edda Currle
- Pflegeforschung: Katrin Ettl und Norbert Lichtenauer
- Logopädie: Nina Greiner
- Physiotherapie: Natalie Kudienko
- Projektmanagement: Gudrun Bahr und Vanessa Mücke

Die jeweiligen Leiter der Teilprojekte sind:

- eHealth: Prof. Dr. Georgios Raptis
- Technikfolgeabschätzung und angewandte Ethik: Prof. Dr. Karsten Weber
- Sozialforschung: Prof. Dr. Sonja Haug
- Pflegeforschung: Prof. Dr. Annette Meussling-Sentpali und Prof. Dr. Christa Mohr
- Logopädie: Prof. Dr. Norina Lauer
- Physiotherapie: Prof. Dr. Andrea Pfingsten
- Projektmanagement: Prof. Dr. Karsten Weber

Prof. Dr. Karsten Weber ist in seiner Funktion als Gesamtprojektleiter der Verantwortliche für das Gesamtprojekt.

Auftragsverarbeiter:

Sollte im Rahmen des Projektes eine Nutzung von Software mit externer Datenverarbeitung (z.B. Spracherkennungs- und Sprachsteuerungssoftware) erfolgen, wird die damit verbundene Auftragsverarbeitung mittels eines Vertrags abgesichert, so dass sichergestellt werden kann, dass die datenschutzrechtlichen Anforderungen erfüllt werden. Dasselbe gilt für die Nutzung externer Netzwerk- und Server- bzw. Cloud/Hosting-Infrastruktur. Ausnahmen s. Kap. 5.5.2.

Die zur Verfügung stehende Infrastruktur mit den eingesetzten Telepräsenzrobotern wird von allen am Projekt beteiligten Personen genutzt. Wartungsarbeiten an den internen Systemen werden durch die Mitarbeiter*innen Luise Middel und Christof Popp aus dem Bereich eHealth sowie ggf. weitere Mitarbeiter*innen des eHealth Labors durchgeführt.

Ein Zugriff der hier aufgeführten Personen auf die erhobenen Daten außerhalb der im Projekt beschriebenen Zielsetzungen ist nicht vorgesehen.

6.1 Verantwortliche Stelle

Ostbayerische Technische Hochschule Regensburg
Prüfeninger Str. 58
93049 Regensburg
Telefon +49 (0) 941 943 02
E-Mail: präsident@oth-regensburg.de

Die Ostbayerische Technische Hochschule Regensburg ist eine Körperschaft des öffentlichen Rechts gemäß Art. 11 Abs. 1 Satz 1 Bayerisches Hochschulgesetz. Die Ostbayerische Technische Hochschule Regensburg wird vom Vorsitzenden der Hochschulleitung, Herrn Präsident Prof. Dr. Wolfgang Baier, gesetzlich vertreten.

Der **Datenschutzbeauftragte** der OTH Regensburg ist:

Datenschutzbeauftragter der
Ostbayerische Technische Hochschule Regensburg
Prüfeningerstr. 58
93049 Regensburg
Tel.: 0941 / 943-02
E-Mail: datenschutz@oth-regensburg.de

Einheitlicher Ansprechpartner (Single Point of Contact, SPoC) für Anfragen von Betroffenen bzgl. ihrer Rechte aus der DSGVO:

Christof Popp
Ostbayerische Technische Hochschule Regensburg
eHealth Labor, K201
Galgenbergstr. 32
93049 Regensburg
Telefon +49 (0) 941 943 7169
E-Mail: mr.spoc@deinhaus40.de

Verpflichtung zum Datenschutz

Das Projekt TePUS, zusammen mit allen daran beteiligten Mitarbeiter*innen und vertraglich gebundenen Dienstleistern, verpflichten sich zur Einhaltung von datenschutzrechtlichen Vorschriften. Die betroffenen Personen haben eine entsprechende Datenschutzerklärung (Verpflichtungserklärung / Schweigepflicht-erklärung siehe Anhang) zur Geheimhaltungspflicht unterzeichnet.

Die Geheimhaltungspflicht für alle Mitarbeiter*innen und Dienstleister **endet nicht** mit Beendigung des Arbeitsverhältnisses oder der Dienstleistungserfüllung, sondern wirkt noch darüber hinaus.

6.2 DATENVERARBEITENDE

Die erhobenen Daten werden von den für die jeweiligen Teilbereiche zuständigen Mitarbeiter*innen und Professor*innen bearbeitet. Für die jeweiligen Teilbereiche sind dies:

- Daten betreffend der Physiotherapie werden durch Natalie Kudienko und Prof. Dr. Andrea Pfingsten erhoben und bearbeitet
- Daten betreffend der Logopädie werden durch Nina Greiner und Prof. Dr. Norina Lauer erhoben und bearbeitet
- Daten betreffend der Pflegewissenschaften werden durch Katrin Ettl, Norbert Lichtenauer, Prof. Dr. Christa Mohr und Prof. Dr. Annette Meussling-Sentpali erhoben und bearbeitet
- Daten betreffend der Technik werden durch Frau Luise Middel, Herrn Christof Popp und Prof. Dr. Georgios Raptis erhoben und bearbeitet
- Administrative Daten des Projekts werden primär durch Gudrun Bahr und Prof. Dr. Weber, können jedoch grundsätzlich von allen Mitarbeiter*innen erhoben und verarbeitet werden
- Daten betreffend der Sozialforschung werden durch Edda Currle und Prof. Dr. Sonja Haug erhoben und bearbeitet
- Daten bzgl. der Akzeptanz der Roboter und der damit verbundenen Anwendungen werden von allen Mitarbeiter*innen erhoben und bearbeitet

Aufgrund des Gesundheitsbezuges der Daten besteht eine Verschwiegenheitspflicht aller Projektbeteiligten. Für Therapeut*innen ist diese gesetzlich in §203 StGB (Schweigepflicht) geregelt. Für alle anderen Mitarbeiter*innen im Projekt wird diese entweder durch Regelungen im Arbeitsvertrag oder – falls nicht ausreichend – zusätzlich mittels der Unterzeichnung einer Verschwiegenheitserklärung bestätigt und gewährleistet.

Die Projektmitarbeiter*innen werden über die bestehenden und notwendigen Datensicherheits- und IT-Sicherheitsmaßnahmen unterrichtet.

7 DATENSCHUTZBEZOGENE ANFORDERUNGEN

In diesem Kapitel werden die Anforderungen dargelegt, die aus der DSGVO resultieren (Kap. 7.1) und wie sie durch die Gewährleistung von Datenschutzzielen erfüllt werden (Kap. 7.2).

7.1 Zentrale datenschutzrechtliche Anforderungen der DSGVO

Aus dem Standard-Datenschutzmodell werden die Anforderungen aufgelistet und die wichtigsten Aspekte bzw. Motivationen kurz übernommen.

7.1.1 Transparenz für Betroffene

Der Grundsatz der Transparenz wird in Art. 5 Abs. 1a DSGVO beschrieben. Er bezieht sich insbesondere auf die Informations- und Auskunftspflichten gemäß Art. 12ff DSGVO. Art. 12 Abs. 1 Satz 1 DSGVO fordert, dass der betroffenen Person alle Informationen gemäß der Informationspflichten aus Art. 13 und 14 DSGVO und allen Mitteilungspflichten gemäß Art. 15 – 22 sowie Art 34 DSGVO in Bezug auf die Verarbeitung beziehen, präzise, transparent, verständlich und in leicht zugänglicher Form in klarer und einfacher Sprache zugänglich gemacht werden.

7.1.2 Zweckbindung

Der Grundsatz der Zweckbindung stellt die Verpflichtung dar, Daten nur für den Zweck zu verarbeiten für den diese auch erhoben wurden. Diese Verpflichtungen sind den Verarbeitungsbefugnissen zu entnehmen, welche durch den Forschungszweck vorgegeben werden. Eine Weiterverarbeitung von erhobenen Daten, die über den ursprünglich festgelegten Zweck hinausgehen, ist zu unterbleiben.

Die Zweckbindung ist in Art. 5 Abs. 1 c sowie Art. 6 Abs. 4 DSGVO geregelt.

7.1.3 Datenminimierung

Durch die Gesetzgebung ist gefordert, dass die Erhebung und Verarbeitung von personenbezogenen Daten auf ein für den Zweck angemessenes, erhebliches und notwendiges Maß beschränkt sind (Art. 5 Abs. 1 c DSGVO).

7.1.4 Richtigkeit

Nach Art. 5 Abs. 1 d müssen personenbezogene Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Damit dies gewährleistet werden kann, ist zu gewährleisten, dass Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

7.1.5 Speicherbegrenzung

In Art. 5 Abs.1 e wird für personenbezogene Daten festgelegt, dass diese nur solange in einer Form gespeichert werden, welche die Identifizierung der betroffenen Personen ermöglicht, wie dies für die Erfüllung des Zwecks notwendig ist. Hierbei können ebenfalls die Maßnahmen der Pseudonymisierung, Anonymisierung und Löschung angewandt werden.

7.1.6 Integrität

Die Anforderung der Integrität wird in Art. 5 Abs. 1 f und in Art. 32 Abs. 1b benannt. Hierbei müssen unbefugte Veränderungen und Entfernungen, unbeabsichtigter Verlust, Zerstörung oder Schädigung durch geeignete technische und organisatorische Maßnahmen verhindert werden. Jede Veränderung an gespeicherten Daten durch unberechtigte Dritte muss ausgeschlossen werden bzw. so erkennbar gemacht werden, dass diese berichtigt werden können.

7.1.7 VERTRAULICHKEIT

Art. 5 Abs. 1 f definiert die Verpflichtung zur Wahrung der Vertraulichkeit personenbezogener Daten. Ferner wird in Art. 32 Abs. 1b die Verpflichtung zur Vertraulichkeit in Bezug auf die für die Verarbeitung eingesetzten Systeme, Dienste, Auftragsverarbeiter und Personen, die dem Verantwortlichen oder Auftragsverarbeiter unterstellt sind, vorgegeben.

Weiter gilt nach Art 28 Abs. 3 b DSGVO eine gesonderte Vertraulichkeitsverpflichtung für die Weisungen des Verantwortlichen.

Es darf Unbefugten nicht möglich sein, Zugang zu den Daten zu erlangen und weder Daten noch Geräte, die diese Daten verarbeiten, zu nutzen. (Art. 32. Abs. 1 b DSGVO)

7.1.8 RECHENSCHAFTS- UND NACHWEISFÄHIGKEIT

Art. 5 Abs. 2 DS-GVO verpflichtet den Verantwortlichen zum Nachweis der Einhaltung der in Art. 5 Abs. 1 DS-GVO formulierten Grundsätze zur Verarbeitung personenbezogener Daten.

In Art. 24 Abs. 1 S. 1 wird zudem gefordert, dass der Verantwortliche sicherstellen muss und den Nachweis dafür erbringen muss, dass die Verarbeitung gemäß der DSGVO erfolgt.

Ein Nachweis einer Einwilligung nach Art. 7 Abs. 1 DSGVO ist dann zu leisten, wenn die Verarbeitung darauf beruht.

Die DSGVO fordert in Art. 30, dass für alle Verarbeitungstätigkeiten ein Verzeichnis angelegt wird, in dem die jeweiligen Verarbeitungstätigkeiten und deren Zweck beschrieben werden.

Jegliche Verletzungen des Schutzes der personenbezogenen Daten sind nach Art. 33 Abs. 5 DSGVO für die Datenschutzaufsichtsbehörde zu dokumentieren.

Gemäß Art. 58 Abs. 1 a und e DSGVO kann die Aufsichtsbehörde die Bereitstellung aller zur Erfüllung ihrer Aufgaben erforderlichen Informationen verlangen. Die Verantwortlichen und Auftragsverarbeiter müssen die Verpflichtung erfüllen können.

Datenpannen müssen unter den in Art. 33 DSGVO geregelten Umständen an die Aufsichtsbehörden gemeldet werden.

7.1.9 IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG

Hat der/die Verantwortliche begründete Zweifel an der Identität der natürlichen Person, die einen Antrag gemäß den Artikeln 15 bis 21 stellt, so kann er unbeschadet des Artikels 11 zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind (Art. 12 DSGVO). Aus diesen Anforderungen ergibt sich die Notwendigkeit der Festlegung einer Authentifizierungsmethode für die Personen, die die Betroffenenrechte geltend machen möchten.

7.1.10 UNTERSTÜTZUNG BEI DER WAHRNEHMUNG VON BETROFFENENRECHTEN

Der Verantwortliche erleichtert der betroffenen Person die Ausübung ihrer Rechte gemäß den Artikeln 15 bis 22. In den in Artikel 11 Absatz 2 genannten Fällen darf sich der Verantwortliche nur dann weigern, aufgrund des Antrags der betroffenen

Person auf Wahrnehmung ihrer Rechte gemäß den Artikeln 15 bis 22 tätig zu werden, wenn er glaubhaft macht, dass er nicht in der Lage ist, die betroffene Person zu identifizieren.

7.1.11 Berichtigungsmöglichkeit von Daten

Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen. (Art.16 DSGVO)

7.1.12 Löschbarkeit von Daten

Gemäß Art. 17 Abs. DSGVO besitzen Betroffene das Recht auf die Löschung ihrer Daten, wenn eine der dort genannten Voraussetzungen erfüllt ist und keine Ausnahme nach Art. 17 Abs. 3 DSGVO angewandt werden kann.

Nach einer datenschutzkonformen Löschung können die betroffenen Daten nicht mehr verarbeitet werden. Hierfür sind von der verantwortlichen Stelle geeignete Vorgehensweisen festzulegen (Art. 24, 25 Abs 1 i.V.m. 5 Abs. 1e DSGVO)

Die Löschung kann nach Art. 58 Abs. 2 g DSGVO durch eine Aufsichtsbehörde angeordnet werden.

7.1.13 Einschränkbarkeit der Verarbeitung von Daten

Betroffene können nach Art. 18 DSGVO die Einschränkung der Sie betreffenden personenbezogenen Daten fordern. Die Verarbeitung ist in einem solchen Fall nur noch unter den in Art. 18 Abs 2 DSGVO genannten Bedingungen möglich. Es muss durch technische Maßnahmen sichergestellt werden, dass die betroffenen Daten nur noch begrenzt verarbeitet werden können.

Die Aufsichtsbehörde kann nach Art. 58 Abs. 2 g DSGVO eine Einschränkung der Verarbeitung anzuordnen.

7.1.14 Datenübertragbarkeit

Gemäß Art. 20 Abs. 1 DSGVO hat die betroffene Person das Recht, die betreffenden Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten.

7.1.15 Eingriffsmöglichkeit in Prozesse automatisierter Entscheidungen

Dieser Punkt findet keine Anwendung im Projekt, da keine automatisierten Entscheidungen im Projekt geplant sind.

7.1.16 Fehler- und Diskriminierungsfreiheit beim Profiling

Es ist sicherzustellen, dass für das Profiling technische und organisatorische Maßnahmen getroffen werden, welche sicherstellen, dass Faktoren, die zu unrichtigen personenbezogenen Daten oder Entscheidungen führen, die die Betroffenen diskriminieren korrigiert werden.

7.1.17 DATENSCHUTZ DURCH VOREINSTELLUNGEN

Art. 25 Abs. 2 DSGVO sieht die Verpflichtung des Verantwortlichen zur Umsetzung des Prinzips Datenschutz durch Voreinstellungen zu gewährleisten, vor. Hierfür müssen geeignete technische und organisatorische Maßnahmen getroffen werden, mit denen sichergestellt wird, dass nur personenbezogene Daten verarbeitet werden, die für den Verarbeitungszweck erforderlich sind.

7.1.18 VERFÜGBARKEIT

Art. 5 Abs. 1 e DSGVO benennt die Verfügbarkeit als einen Grundsatz der Verarbeitung personenbezogener Daten. Des Weiteren setzt Art. 32 Abs. 1 b und c DSGVO die Verfügbarkeit in einen expliziten Kontext der Sicherheit von Datenverarbeitung. Hier soll gewährleistet werden, dass die Daten für die Dauer ihrer Notwendigkeit für den Zweck verfügbar sind.

Des Weiteren findet die Gewährleistung der Verfügbarkeit Anwendung in Art. 13, 14, 15 sowie 20 der DSGVO.

7.1.19 BELASTBARKEIT

Art. 32 Abs. 1 b fordert die Belastbarkeit von Systemen und Diensten.

7.1.20 WIEDERHERSTELLBARKEIT

Art. 32 Abs.1 c fordert die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. Dies geht über den Grundsatz der Verfügbarkeit in Art. 32 Abs. 1 b DSGVO hinaus, da für eine rasche Wiederherstellbarkeit nach einem Zwischenfall zusätzliche technische und organisatorische Maßnahmen zu treffen sind.

7.1.21 EVALUIERBARKEIT

Nach Art. 32 Abs. 1d wird ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gefordert.

7.1.22 BEHEBUNG UND ABMILDERUNG VON DATENSCHUTZVERLETZUNGEN

Gemäß Art. 33 Abs. 3 d und 34 Abs. 2 DSGVO müssen technische und organisatorische Maßnahmen umgesetzt werden, welche sicherstellen, dass Datenpannen behoben werden und deren eventuelle Folgen für Betroffene abgemildert werden.

7.1.23 ANGEMESSENE ÜBERWACHUNG DER VERARBEITUNG

Damit eine wirksame Behebung und Abmilderung sichergestellt werden kann, können Verantwortliche und der Auftragsverarbeiter dazu verpflichtet werden, eine Überwachung der Verarbeitung durchzuführen. Dies kann als technische und organisatorische Maßnahme i. S. d. Art. 32 DSGVO durchgeführt werden.

7.1.24 EINWILLIGUNGSMANAGEMENT

Da die Datenverarbeitung und deren Zulässigkeit auf einer wirksamen Einwilligung der Betroffenen basiert, gilt hier Art. 6 Abs. 1 a i. V. m. Art. 4 Nr. 11 DSGVO zu beachten. Das Einwilligungsmanagement umfasst das vollständige Verfahren der Einholung, der Speicherung, der Dokumentation, des Nachweises einer Einwilligung

sowie die Umsetzung eines Widerrufs der Einwilligung. Eine Einwilligung ist nur wirksam, wenn

- eine vorherige umfassende Information des Betroffenen über die Datenverarbeitung erfolgt ist,

- der Einwilligungstext konkrete Datenverarbeitungen klar und eindeutig benennt,

- die Einwilligung freiwillig erklärt wird und

- eine unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, erfolgt.

Es muss jederzeit ein Widerruf der Einwilligung möglich sein, welcher zur Folge hat, dass die betroffenen Daten nicht mehr weiterverarbeitet werden und unter Einhaltung der bestehenden Fristen und Regelungen gelöscht werden. Der Widerruf muss nach Art. 7 Abs. 3 DSGVO genauso einfach zu erteilen sein wie die Einwilligung selbst. Hierfür müssen auf Seiten des Verantwortlichen geeignete Vorgehensweisen für die Entgegennahme und die Umsetzung festgelegt werden. Für eine elektronische Einwilligung muss eine Ausgestaltung des entsprechenden Verfahrens erfolgen.

7.1.25 Umsetzung aufsichtsbehördlicher Anordnungen

Art. 58 Abs. 2 f DSGVO erlaubt Aufsichtsbehörden die Verarbeitung zu beschränken.

Art. 58 Abs. 2 j DSGVO erlaubt Aufsichtsbehördern eine Übermittlung von Daten an Empfänger in Drittländern auszusetzen. Voraussetzung hierbei ist, dass die Empfänger lokalisiert werden können und die Datenübermittlung gesteuert werden kann.

7.2 Darstellung der Gewährleistungsziele / Schutzziele

Im Folgenden werden die für dieses Datenschutzkonzept anwendbaren Gewährleistungs- und Schutzziele dargelegt. Diese sind an den Gewährleistungszielen des SDM orientiert und dienen einer Systematisierung datenschutzrechtlicher Anforderungen. D.h. es wird dargelegt, wie das Projekt die Anforderungen des Datenschutzes sicherstellt. Da einige der nachfolgenden Aspekte erst nach der konkreten technischen Umsetzung des Projekts konkretisiert werden können, handelt es sich hierbei um eine generische Darstellung der Maßnahmen, die hierfür angedacht sind.

7.2.1 Systematisierung der rechtlichen Anforderungen durch die Gewährleistungsziele

Im Folgenden werden die in Kap. 7.1 aufgeführten datenschutzrechtlichen Anforderungen der DSGVO den Gewährleistungszielen gemäß des SDM zugeordnet. Dies dient der Systematisierung der Anforderungen in Bezug auf die technische und organisatorische Ausgestaltung der Verarbeitungstätigkeiten. Eine konkrete technische Ausgestaltung der Verarbeitungstätigkeit kann erst dann genau und explizit beschrieben werden, wenn die technische Initialisierung des Projekts vollzogen wurde. Sie wird dann diese Anforderungen und Festlegungen erfüllen.

Die folgende Tabelle ist aus dem SDM entnommen.

7.1.1	Transparenz für Betroffene (Art. 5 Abs. 1, Art. 12 Abs. 1 und 3 bis Art. 15, Art. 34 DS-GVO)	Transparenz
7.1.2	Zweckbindung (Art. 5 Abs. 1 b DS-GVO)	Nichtverkettung
7.1.3	Datenminimierung (Art. 5 Abs. 1 DS-GVO)	Datenminimierung
7.1.4	Richtigkeit (Art. 5 Abs. 1 d DS-GVO)	Integrität
7.1.5	Speicherbegrenzung (Art. 5 Abs. 1 e DS-GVO)	Datenminimierung
7.1.6	Integrität (Art. 5 Abs. 1 f, Art. 32 Abs. 1 b, DS-GVO)	Integrität
7.1.7	Vertraulichkeit (Art. 5 Abs. 1 f, Art. 28 Abs. 3 b, Art. 29, Art. 32 Abs. 1 b, Art. 32 Abs. 4, Art. 38 Abs. 5 DS- GVO)	Vertraulichkeit
7.1.8	Rechenschafts- und Nachweisfähigkeit (Art. 5 Abs. 2, Art. 7 Abs. 1, Art. 24 Abs. 1, Art 28 Abs. 3 lit. a, Art. 30, Art. 33 Abs. 5, Art. 35, Art. 58 Abs. 1 lit. a und lit. e DS-GVO)	Transparenz
7.1.9	Identifizierung und Authentifizierung (Art. 12 Abs. 6 DS- GVO)	Intervenierbarkeit
7.1.10	Unterstützung bei der Wahrnehmung von Betroffenenrechten (Art. 12 Abs. 2 DS-GVO)	Intervenierbarkeit
7.1.11	Berichtigungsmöglichkeit von Daten (Art. 5 d, Art. 16 DS-GVO)	Intervenierbarkeit
7.1.12	Löschbarkeit von Daten (Art. 17 Abs. 1 DS-GVO)	Intervenierbarkeit
7.1.13	Einschränkbarkeit der Verarbeitung von Daten (Art. 18 DS- GVO)	Intervenierbarkeit
7.1.14	Datenübertragbarkeit (Art. 20 Abs. 1 DS-GVO)	Intervenierbarkeit
7.1.15	Eingriffsmöglichkeit in Prozesse automatisierter Entscheidungen (Art. 22 Abs. 3 DS-GVO)	Intervenierbarkeit
7.1.16	Fehler- und Diskriminierungsfreiheit beim Profiling (Art. 22 Abs. 3, 4 i. V. m. ErwGr. 71)	Integrität
7.1.17	Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)	Datenminimierung, Intervenierbarkeit
7.1.18	Verfügbarkeit (Art. 32 Abs. 1 b DS-GVO)	Verfügbarkeit
7.1.19	Belastbarkeit (Art. 32 Abs. 1 b DS-GVO)	Integrität, Vertraulichkeit, Verfügbarkeit
7.1.20	Wiederherstellbarkeit (Art. 32 Abs. 1 b, c DS-GVO)	Verfügbarkeit
7.1.21	Evaluierbarkeit (Art. 32 Abs. 1 d DS-GVO).	Ein Prozess der alle Anforderungen umfasst.
7.1.22	Behebung und Abmilderung von Datenschutzverletzungen (Art. 33 Abs. 3 d, 34 Abs. 2 DS-GVO).	Integrität, Vertraulichkeit, Intervenierbarkeit, Verfügbarkeit
7.1.23	Angemessene Überwachung der Verarbeitung (Art. 32, 33, 34 DS-GVO)	Transparenz, Integrität
7.1.24	Einwilligungsmanagement (Art. 4 Nr. 11, Art. 7 Abs. 4 DS- GVO)	Transparenz, Intervenierbarkeit
7.1.25	Umsetzung aufsichtsbehördlicher Anordnungen (Art. 58 Abs. 2 f und j)	Intervenierbarkeit

7.2.2 DATENMINIMIERUNG

Der Grundsatz der Datenminimierung wird dadurch gewährleistet, indem die erhobenen Attribute bzw. Daten der betroffenen Personen auf ein für die Erfüllung des Zwecks notwendiges Maß reduziert werden. Die Optionen der Verarbeitung werden vor Beginn der Datenerhebung festgelegt und auf ein notwendiges Maß reduziert.

Im Forschungsdesign (Haug S., Currle E., 2020) wird genau festgelegt, welche Daten für die Beantwortung der Forschungsfragen im Projekt notwendig sind. Weitere Daten werden nicht erhoben und verarbeitet.

Daten werden nach den Regelungen in Kap. 5.5.3 gelöscht, wenn sie nicht mehr benötigt werden. Außerdem wird stets bei der Erhebung und Verarbeitung von Daten geprüft, ob sie anonymisiert oder – falls für die Erreichung der Forschungsziele nicht möglich – zumindest pseudonymisiert werden und dann die Anonymisierung oder Pseudonymisierung nach Kap. 5.6.3 und 5.6.4 durchgeführt.

7.2.3 VERFÜGBARKEIT

Da es sich um ein Forschungsprojekt handelt, hat ein Bruch der Verfügbarkeit (Zerstörung oder Unzugänglichkeit von Daten) grundsätzlich keine negativen Auswirkungen auf die Betroffenen, sondern nur auf die Forschungsziele (und auch dort hat sie keine Folgen bzgl. Datenschutz). Deshalb wird der Schutzbedarf zur Verfügbarkeit bzgl. des Datenschutzes als niedrig eingestuft. Ein Verlust der Verfügbarkeit wird aus diesem Grund auch nicht als meldepflichtige „Datenpanne“ eingestuft. Verfügbarkeit und Wiederherstellbarkeit werden bzgl. Datenschutz aufgrund dessen nicht zugesichert. Nichts desto trotz werden Daten möglichst redundant gespeichert und in bestehenden Backup-Konzepten der OTH Regensburg oder von externen Anbietern integriert, sofern dabei auch eine Löschung sichergestellt werden kann. Die üblichen Schutzmaßnahmen gegen Malware der OTH Regensburg (z.B. Virenschutzprogramme) werden übernommen.

Es werden ausreichend leistungsfähige Systeme und Netzwerke nach dem Stand der Technik eingesetzt oder – bei externen Anbietern – vertraglich zugesichert.

Es wird ein Notfallkonzept für die Wiederherstellung beschädigter oder verlorener Daten erarbeitet und bei Bedarf auf dieses zurückgegriffen.

7.2.4 INTEGRITÄT

Die Integrität der Daten und der technischen Systeme wird durch den Zugriffsschutz der technischen Systeme sichergestellt. Dafür werden die üblichen Mechanismen von Betriebssystemen und der Server-Infrastruktur der OTH Regensburg (z.B. Active Directory) eingesetzt; bei Einsatz von Datenbanken sowie externer Anbieter entsprechende Authentifizierungs- und Rechtemanagement-Systeme. Berechtigungen werden nach dem need to know Prinzip eingerichtet. D.h. nur Mitarbeiter*innen, welche mit den Daten arbeiten müssen, erhalten auch eine Zugriffsberechtigung.

Die Daten sowie die Systeme auf denen die Daten gespeichert und verarbeitet werden, werden vor schädlichen äußeren Einflüssen z.B. durch Einsatz von Firewalls und Virenschutzprogrammen geschützt.

Daten werden durch die Mitarbeiter*innen des Projektes bei Erhebung auf Plausibilität geprüft. Wenn Daten dabei als unrichtig erkannt wurden oder falls ein entsprechender Hinweis vom Betroffenen eingeht, sind die Mitarbeiter*innen angewiesen, die Daten genauer zu prüfen und unrichtige Daten zu löschen und nicht zu verwenden. Das Recht der Betroffenen auf Sperrung, Berichtigung oder Löschung kann durch eine Kontaktaufnahme der betroffenen Personen mit dem SPoC des Projektes wahrgenommen werden. Da es sich um eine einmalige Erhebung von Daten im Wesentlichen direkt von den Betroffenen handelt, sind Maßnahmen zur Sicherstellung der Aktualität der Daten nicht notwendig. (Richtigkeit).

Ein Profiling findet im Projekt nicht statt. Einzig die Selektion der Probend*innen erfolgt im Vorfeld auf Grundlage wissenschaftlich fundierter Kriterien, die im Forschungsdesign definiert sind.

7.2.5 VERTRAULICHKEIT

Die Vertraulichkeit wird durch eine Reihe von organisatorischen und technischen Maßnahmen sichergestellt. Organisatorisch wird sie durch gesetzliche Regelungen (Amtsgeheimnis für Professor*innen, Schweigepflicht für Therapeut*innen) oder vertragliche Regelungen (Vertraulichkeitsklausel in den Arbeitsverträgen der Mitarbeiter*innen, Verträge zur Auftragsverarbeitung mit externen Dienstleistern, Verschwiegenheitserklärungen für die Projektmitarbeiter*innen) und/oder Arbeitsanweisungen gewährleistet. Technisch werden Computersysteme durch Zugriffsschutz wie im Kap. 7.2.4 abgesichert. Netzwerkverbindungen werden verschlüsselt und authentifiziert (z.B. über TLS, IPSec). Datenträger oder Datenbestände werden bei Bedarf nach dem Stand der Wissenschaft und Technik (z.B. durch Beachtung von entsprechenden Technischen Richtlinien des BSI verschlüsselt.

7.2.6 NICHTVERKETTUNG

Durch die hier beschriebenen organisatorischen und technischen Maßnahmen wird sichergestellt, dass alle personenbezogenen / personenbeziehbaren Daten nur zu den vorgesehenen, durch die Einwilligung der Betroffenen abgedeckten Zwecken erhoben und verarbeitet werden.

7.2.7 TRANSPARENZ

Das Projekt stellt allen Betroffenen Informationsmaterial bzgl. der Datenverarbeitung zur Verfügung. Dieses wird vorher bzgl. Verständlichkeit geprüft. Es wird organisatorisch sichergestellt, dass zur Erteilung einer Einwilligung die Informationen die (künftigen) Betroffenen erreichen.

Wenn die entsprechenden technischen Aspekte (z.B. Dienstleister, eingesetzte Apps, Netzwerktopologie, Kommunikationsserver und Datenbanken, weitere Software) des Projektes feststehen, wird ein Verzeichnis von Verarbeitungstätigkeiten erstellt und laufend aktualisiert. Verträge zur Auftragsverarbeitung oder Datenschutzerklärungen oder Sicherheitszusicherungen externer Anbieter werden zur einer evtl. Prüfung durch den/die Datenschutzbeauftragte/n oder der Aufsichtsbehörde vorgehalten. Evtl. Verletzungen des Datenschutzes werden durch die Mitarbeiter*innen dokumentiert, Datenpannen werden nach den gesetzlichen Regelungen an die Aufsichtsbehörde gemeldet. Diese Pflichten werden den Mitarbeiter*innen bekanntgegeben.

Einmal jährlich, anlässlich der Erstellung des Jahresberichts des Projektes, wird eine Evaluation und Überprüfung der technischen und organisatorischen Maßnahmen durch den SPoC durchgeführt. Er befragt dafür alle Mitarbeiter*innen des Projektes und überprüft die technischen Systeme und Einstellungen.

Es wird ein Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO erstellt, sofern die technische Initialisierung des Projektes erfolgt ist. Dieses wird bei Bedarf laufend aktualisiert. Hierzu gehören Geschäftsprozesse, Datenbestände, Datenflüsse und Netzpläne, sowie die dafür genutzten IT-Systeme, Betriebsabläufe und sonstige Beschreibungen von Verarbeitungstätigkeiten.

Alle Arbeitsverträge und evtl. relevante Erklärungen (z.B. zur Vertraulichkeit im Projekt) von internen Mitarbeiter*innen sowie die Verträge mit externen Dienstleistern und Dritten, die Daten verarbeiten sowie die Zuständigkeitsregelungen werden dokumentiert.

Jegliche Einwilligungen, Widerrufe sowie Widersprüche werden von den zuständigen Projektmitarbeiter*innen dokumentiert.

Die Transparenz für die Betroffenen wird außerdem mittels der Gewährleistung der Betroffenenrechte im Kap. 7.2.8 gewährleistet.

7.2.8 INTERVENIERBARKEIT

Information

Bei der Einwilligung werden Betroffene über die Datenerhebung und -verarbeitung und über ihre Rechte gemäß DSGVO umfassend informiert. Sollten – natürlich nach erfolgter Einwilligung - Daten nicht bei den betroffenen Personen erhoben werden (z.B. Patientenakte), werden sie darüber ebenfalls informiert.

Auskunftsrecht

Auf Anfrage wird eine umfängliche Auskunft über die Daten der betroffenen Personen, die verarbeitet werden, erteilt.

Das Projekt stellt eine/n einheitliche/n Ansprechpartner*in (Single Point of Contact, SPoC) bereit. Sofern er/sie eine/n Betroffene/n sicher identifizieren und authentifizieren kann (s. Kap. 7.1.9), unterstützt er/sie den/die Betroffene/n bei der Wahrnehmung seiner/ihrer Rechte.

Eine Auskunft wird erteilt, nachdem sich die betroffene Person sich persönlich bei einem/einer Mitarbeiter*in des Projekts oder dem dafür vorgesehenen Single-Point of Contact gemeldet und authentifiziert hat (s.u.).

Identifizierung und Authentifizierung

Alle Betroffenen, dessen/deren personenbezogenen Daten im Projekt verarbeitet werden, müssen eine Einwilligung unterzeichnen. Diese enthält einerseits ihre persönlichen Daten, andererseits ist sie unterschrieben. Wenn eine betroffene Person einen Antrag bzgl. ihrer Betroffenenrechte stellt, werden die persönlichen Daten sowie

die Unterschrift auf dem Antrag gegen die Daten und Unterschrift der Einwilligung geprüft und somit eine Identifizierung und Authentifizierung durchgeführt.

Recht zum Widerspruch bzgl. der Datennutzung

Die betroffene Person wird zu Beginn der Teilnahme und bei jeglicher Äußerung von Bedenken gegenüber der Datensammlung darauf hingewiesen, dass eine sofortige Beendigung der Teilnahme ohne Nachteile möglich ist.

Durch die Mitteilung eines Widerspruchs bzw. des Widerrufs der Einwilligung werden die Daten entweder gelöscht oder ihre Verarbeitung eingeschränkt (s. Kap. 5.6.2).

Recht auf Berichtigung, Sperrung oder Löschung

Das Recht der Betroffenen auf Sperrung, Berichtigung oder Löschung kann durch eine Kontaktaufnahme der betroffenen Personen mit dem Projekt wahrgenommen werden. (siehe. Kapitel 5.6). Dazu stehen die Mitarbeiter*innen des Projektes und insbesondere der einheitliche Ansprechpartner (SPoC) zur Verfügung. Die Rechte können wie folgt wahrgenommen:

Berichtigung, Mitteilungspflicht

Der SPoC leitet Anträge auf Berichtigung von Daten an die direkt für diese Daten verantwortlichen Mitarbeiter*innen des Projektes weiter. Diese müssen den Antrag prüfen und bei Bedarf die Daten berichtigen. Diese Pflicht wird den Mitarbeiter*innen mitgeteilt. Der Betroffene wird darüber informiert.

Löschung, Mitteilungspflicht

Eine Löschung von Daten erfolgt einerseits nach Ablauf der Aufbewahrungsfristen (s. Kap. 5.5.3), andererseits bei Widerruf der Einwilligung einer betroffenen Person nach Kap. 5.6.1 (in diesem Fall wird die betroffene Person darüber informiert), sofern die Einschränkungen aus Kap. 5.6.2 nicht zutreffen. D.h. durch die in diesem Konzept beschriebenen organisatorischen und technischen Maßnahmen werden die Daten gelöscht, wenn sie nicht bereits in einer Studie ausgewertet wurde. In diesem Falle wird gemäß Art. 17 Abs. 3 Punkt d DSGVO eine Löschung nicht vorgenommen, sondern eine Einschränkung der Verarbeitung vorgenommen.

Einschränkung der Verarbeitung, Mitteilungspflicht

Eine Einschränkung der Verarbeitung erfolgt nach Maßgabe von Kap. 7.1.12, wenn eine Löschung nicht vorgenommen werden kann, oder nach Antrag des/der Betroffenen. Die Daten werden dann technisch gekennzeichnet, so dass sie nur nach Maßgabe von Art 18 Abs. 2 DSGVO verarbeitet werden. Die betroffene Person wird darüber informiert.

Aushändigung einer Kopie der Daten, Recht auf Datenübertragbarkeit (Migration der Daten)

Nach Art. 20 der Datenschutzgrundverordnung hat eine betroffene Person das Recht die sie betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten.

Eine betroffene Person kann sich persönlich an die Mitarbeiter*innen des Projekts wenden und eine Kopie der über ihn gesammelten Daten verlangen. Alle Mitarbeiter*innen werden entsprechend geschult, um bei einer entsprechenden Anfrage entsprechend zu reagieren und die notwendigen Informationen an die zuständigen Stellen weiterzuleiten.

Sobald die betroffene Person eine Anfrage auf eine Kopie dieser Daten an das Projekt übersendet, werden die angefragten Daten von den zuständigen Mitarbeiter*innen nach den oben genannten Voraussetzung zusammengestellt und dem Betroffenen ausgehändigt.

Für die Kontaktaufnahme stehen zusätzlich die Kontaktdaten des SPoC zur Verfügung.

Verpflichtung, Betroffene bzgl. Datenpannen zu informieren

Bei Vorliegen des Verdachts auf eine Datenpanne wird erst die datenschutzrechtliche Relevanz beurteilt; bei unklaren Fällen wird der Datenschutzbeauftragte konsultiert. Das Ergebnis wird dokumentiert. Stellt sich heraus, dass es sich um einen meldepflichtigen Vorfall handelt, werden die Betroffenen und die Aufsichtsbehörde innerhalb der gesetzlichen Fristen benachrichtigt.

Anspruch auf Anrufung der Datenschutzkontrollinstanz

Wer die Vermutung hat, dass er/sie bei der Erhebung, Speicherung und Verarbeitung seiner/ihrer Daten in seinen/ihren Persönlichkeitsrechten verletzt wird, hat einen Anspruch auf die Unterstützung durch die zuständige Aufsichtsbehörde. Die betroffenen Personen werden über diesen Umstand bei Teilnahme an der Studie mittels der dafür ausgehändigten Dokumente in Kenntnis gesetzt.

Einwilligungsmanagement

Jedes Teilprojekt konzipiert Einwilligungen und entsprechende Informationen für die Betroffenen, welche auf die spezielle Datenverarbeitung des Teilprojektes bzw. der konkret geplanten Intervention ausgerichtet sind. Die Begleitinformationen zur Einwilligung enthalten insbesondere klare, einfach verständliche Informationen über alle beabsichtigten Datenverarbeitungen.

Einwilligungen werden schriftlich erteilt. Sie enthalten die persönlichen Daten der Betroffenen und werden deshalb unter besonderen Sicherheitsmaßnahmen auf Papier unzugänglich für Unbefugte (abgeschlossener Schrank, Zugang nur für autorisierte Mitarbeiter*innen) zusammen mit der Liste der Pseudonymzuordnungen aufbewahrt. Muss zur Verarbeitung eines Antrags auf Ausübung eines Betroffenenrechts der/die Antragsteller*in authentifiziert werden, wird dafür die Einwilligung verwendet. Ebenfalls wird die Einwilligung zum Nachweis der Rechtmäßigkeit der Verarbeitung verwendet, wenn der/die Datenschutzbeauftragte/r oder die Aufsichtsbehörde dies verlangen.

Der Widerruf einer Einwilligung kann, genau wie die Einwilligung, schriftlich erfolgen und wird ebenfalls archiviert, elektronisch bei den betroffenen Datensätzen (falls sie nicht gelöscht werden können, sondern ihre Verarbeitung eingeschränkt wird) vermerkt und ebenfalls durch eine/n Mitarbeiter*in auf das Formular der Einwilligung inkl. Datum und Unterschrift des/der Mitarbeiter*in und auf die Pseudonymliste vermerkt.

Da im gesamten Projekt max. 100 Patient*innen als Betroffene teilnehmen werden, ist ein Einwilligungsmanagement auf Papier nach den o.g. Festlegungen angemessen.

Privacy by Design

Sofern externe Software eingesetzt wird und eine Konfiguration vorab möglich ist, wird diese Software durch das Teilprojekt eHealth entsprechend dem Prinzip Privacy by Design vorkonfiguriert oder entsprechende Instruktionen dafür an die anderen Teilprojekte weitergegeben. Bei der Etablierung von Kommunikationsvorgängen werden diese ebenfalls so konfiguriert, dass sie ohne Zutun des/der Anwender*innen datenschutzkonform arbeiten (Privacy by Default). Technische Vorgänge, welche nicht datenschutzkonform sind (z.B. Alexa Sprachsteuerung oder Apps von Anbietern außerhalb der EU nach Maßgabe des Kap. 5.5.2) sind standardmäßig deaktiviert. Die Mitarbeiter*innen werden informiert, dass solche Vorgänge nur von Betroffenen selbst aktiviert werden sollen und bieten bei entsprechendem Interesse bzw. Nachfrage Informationen insbesondere zu den damit verbundenen Datenschutz-Risiken sowie Hilfe an.

7.3 Darstellung der Rechtskonformität

Es muss zunächst geprüft werden, ob eine Datenschutz-Folgenabschätzung (DSFA) notwendig ist. Dafür wird eine Schwellwertanalyse durchgeführt.

7.3.1 Schwellwertanalyse

Die Schwellwertanalyse wird nach drei verschiedenen Vorgehensweisen durchgeführt, um die Validität zu erhöhen. Als erstes wird die Methodik aus dem Text des Standard-Datenschutzmodells ohne weitere Erläuterungen durchgeführt. Der zweite Ansatz berücksichtigt ergänzende Informationen zur Durchführung der Schwellwertanalyse aus (M. Rost, 2019) unter der Annahme eines ursprünglich hohen Risikos und Datenschutzbedarfs. Der dritte Ansatz ist eine vergleichende Analyse der Verarbeitungstätigkeit im Projekt mit der Verarbeitungstätigkeit einer Arztpraxis, welches „offiziell“ keine DSFA benötigt bzw. wofür schon Best Practices und Empfehlungen existieren.

Ziel der Schwellwertanalyse ist es, nachzuvollziehen, ob die Datenverarbeitung ein hohes Risiko bzgl. Datenschutz für die Betroffenen darstellt und deshalb eine Datenschutz-Folgenabschätzung notwendig ist.

Ansatz 1, SDM-Methodik ohne ergänzende Informationen zur Durchführung:

Es wird festgestellt, dass Gesundheitsdaten, also besondere Arten personenbezogener Daten nach Art. 9 Abs. 1 verarbeitet werden. Jedoch ist die Verarbeitung nicht umfangreich, da die Daten von max. 100 Betroffenen einmalig (zu unterschiedlichen Zeitpunkten im Laufzeit der Projektes, jedoch nicht regelmäßig oder auf Dauer angelegt) erhoben und im Projekt verarbeitet werden. Anschließend wird die Datenverarbeitung beendet. Deshalb handelt es sich nicht um eine besonders riskante Verarbeitungstätigkeit nach Art. 35 Abs. 3 DSGVO. Das Kriterium B des SDM trifft nicht zu.

Die „Muss-Liste“ der DSK (Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist) wurde geprüft. Eintrag Nr. 16 besagt:

„Verarbeitung von personenbezogenen Daten gemäß Art. 9 Abs. 1 und Art. 10 DS-GVO - auch wenn sie nicht als „umfangreich“ im Sinne des Art 35 Abs. 3 lit. b)

anzusehen ist - sofern eine nicht einmalige Datenerhebung mittels der innovativen Nutzung von Sensoren oder mobilen Anwendungen stattfindet und diese Daten von einer zentralen Stelle empfangen und aufbereitet werden. ".

Als typisches Einsatzfeld wird aufgeführt:

„Einsatz von Telemedizin-Lösungen zur detaillierten Bearbeitung von Krankheitsdaten."

Die Verarbeitungstätigkeit erfolgt tatsächlich teilweise mittels der innovativen Nutzung von Sensoren oder mobilen Anwendungen und die Daten werden von einer zentralen Stelle empfangen und aufbereitet. Jedoch ist die Datenerhebung für den Forschungszweck des Projektes einmalig. Dies wird auch durch die Auswertung des typischen Einsatzfelds unterstützt, welches so vom Projekt nicht erfüllt wird. Das Kriterium A des SDM trifft somit nicht zu.

Es wird geprüft, ob mindestens zwei Eigenschaften aus dem Working Paper 248 des Europäischen Datenschutzausschusses zutreffen. Für das Projekt wird das Kriterium

- 4. Vertrauliche Daten oder höchst persönliche Daten

sicherlich erfüllt. Es muss untersucht werden, ob auch das Kriterium

- 8. Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen

ebenfalls erfüllt wird. Aus der Analyse des Originalpapiers geht hervor, dass für dieses Kriterium neue Technologien im Kontext der Datenerhebung und -verarbeitung betrachtet werden („This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms."). Jedes Forschungsprojekt setzt sich mit Innovation auseinander. Die automatische Geltung dieser zwei Kriterien würde somit auf alle Forschungsprojekte im Gesundheitsbereich zutreffen und stets eine DSFA zur Pflicht machen. Die Innovation und die neuen Technologien werden im vorliegenden Projekt jedoch nur auf die Auswirkung von Telepräsenzrobotik auf die Versorgung von Schlaganfall-patient*innen bezogen und nicht auf Datenerhebung und Datenverarbeitung. Sie implizieren auch keine Innovation in der Datenübertragung oder Speicherung. Außerdem sind telemedizinische Verfahren inzwischen weit etabliert und keineswegs mehr neu oder besonders innovativ. Es gibt datenschutztechnische Best Practices, Empfehlungen und Zertifizierungen, sowohl in Deutschland als auch im internationalen Kontext, wie z.B. Dänemark, Estland usw. Aus diesen Überlegungen wird klar, dass das o.g. Kriterium Nr. 8 nicht erfüllt wird. Somit trifft Kriterium C des SDM nicht zu.

Es wird geprüft, ob Art, Umfang, Umstände oder Zwecke der Verarbeitungstätigkeit das Risiko für betroffene Personen erhöht. Ein solches erhöhtes Risiko kann aus dem Projekt nicht abgeleitet werden. Im Gegenteil, durch die Pseudonymisierung aller gesundheitsbezogener Daten wird das Risiko sehr deutlich reduziert. Somit trifft Kriterium D des SDM nicht zu.

Ansatz 2: Durchführung der Schwellwertanalyse nach ergänzenden Informationen zur Methodik.

Nach den Erläuterungen zur Methodik der Schwellwertanalyse aus (M. Rost, 2019) wird für ein vermutetes hohes Risiko als Risikotyp 1 „Grundrechtseingriff" und einen hohen Schutzbedarf der Betroffenen eine geeignete Gestaltung der Verarbeitungstätigkeit sowie die Implementation von Schutzmaßnahmen des

Datenschutzes (Typ 2) und Informationssicherheit (Typ 3) gegenübergestellt. Angenommen, es wird ein hohes Risiko und Schutzbedarf festgestellt. Durch die Implementierung der in diesem Dokument dargelegten Maßnahmen in Konformität zu SDM und insbesondere durch die Entfernung des Personenbezuges (Pseudonymisierung) und die Schutzmaßnahmen der Liste der Pseudonymen wird dieses Risiko auf normal oder niedrig reduziert. Grund dafür ist, dass jegliches mögliches Versagen von Schutzmaßnahmen aus Kap. 7.2 oder Maßnahmen der Informationssicherheit auf Daten ohne Personenbezug auswirkt. Also auch unter diesem Aspekt, d.h. unter der Annahme eines hohen ursprünglichen Risikos, wird dieses offensichtlich soweit reduziert, dass das Ergebnis der Schwellwertanalyse negativ ist.

Ansatz 3: Vergleichende Analyse zur Verarbeitungstätigkeit einer Arztpraxis

Eine Arztpraxis benötigt gemäß Information des Bayerischen Landesamtes für Datenschutzaufsicht (Muster 5: Arztpraxis) keine DSFA. Eine Arztpraxis verarbeitet Gesundheitsdaten von viel mehr Patient*innen (ca. 10x sowiel) als das Projekt. Sie überträgt diese Daten regelmäßig an Dritte (andere Ärzte, Abrechnungs- und Qualitätsdaten an die Kassenärztliche Vereinigung zwecks Abrechnung, auch elektronisch). Telemedizinische Verfahren vergleichbar zum Projekt werden inzwischen ebenfalls von einer großen Anzahl von Praxen eingesetzt, insbesondere anlässlich der CoVID-19 Pandemie. Die Gesundheitsdaten einer typischen Hausarzt-praxis umfassen regelmäßig auch Daten, welche von vielen Betroffenen als stigmatisierend empfunden werden, z.B. Daten zur psychischen Gesundheit oder zu sexuell übertragbaren Krankheiten. Das Projekt dagegen verarbeitet nur sehr wenige, nach o.g. Kriterien eher „harmlose“ Daten aus den Bereichen Pflege, Logopädie und Physiotherapie. Insbesondere sind alle o.g. Daten, die in der Arztpraxis verarbeitet und übermittelt werden mit klarem Personenbezug inkl. aller identifizierenden Daten. Man kann also davon ausgehen, dass Risiken des Datenschutzes und der Informationssicherheit offensichtlich weitaus höher sind als in der Verarbeitungs-tätigkeit des Projektes.

Bzgl. Informationssicherheit ist für Arztpraxen die Technische Anlage der „Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der Bundesärztekammer und Kassenärztlichen Bundesvereinigung (Bundesärztekammer, Kassenärztliche Bundesvereinigung, 2018) maßgeblich. Die zu ca. 90% inhaltsgleiche Vorgängerversion des Dokuments war mit dem BSI abgestimmt und wurde 2014 vom Düsseldorfer Kreis als geeignet bestätigt worden. Die Maßnahmen der Informationssicherheit im Projekt orientieren sich an o.g. Empfehlungen der Technischen Anlage. Demnach ist von einem vergleichbaren Sicherheitsniveau auszugehen.

Da für eine Arztpraxis nach den Erläuterungen des Bayerischen Landesamtes für Datenschutzaufsicht auf Grundlage des Risikos der Verarbeitungstätigkeit keine DSFA notwendig ist, d.h. von einem normalen Risiko ausgegangen wird, kann für das nachweislich geringere Risiko der Verarbeitungstätigkeit des Projektes – bei vergleichbaren IT-Sicherheitsmaßnahmen – erst recht keine DSFA notwendig sein.

7.3.2 Rechtssicherheit/Gerichtsverwertbarkeit der Datenverarbeitung

Da es sich um ein Forschungsprojekt handelt, ist der Aspekt der Rechtssicherheit und Gerichtsverwertbarkeit der Datenverarbeitung nicht relevant. Das Projekt entwickelt keine Rechtsfolgen für die Betroffenen, mit Ausnahme der Datenverarbeitung selbst (Datenschutz). Diese wird durch die Einwilligung und durch die Dokumentation im Projekt bzgl. Gerichtsverwertbarkeit gewahrt.

7.3.3 Revisionsfähigkeit/Beweisfestigkeit von Datenverarbeitungen

Siehe oben in Kap. 7.3.2

7.3.4 Nicht-Abstreitbarkeit von Datenübermittlungen

Siehe oben in Kap. 7.3.2

8 Implementierte bzw. zu implementierende Datenschutzmaßnahmen

Alle implementierten bzw. zu implementierenden Datenschutzmaßnahmen werden in Kap. 7.2 dargestellt.

Für einen wirksamen Datenschutz sind auch Maßnahmen zur Informationssicherheit essentiell. Da die Verarbeitungstätigkeit vergleichbar, wenngleich offensichtlich risikoärmer, zur Verarbeitungstätigkeit einer Arztpraxis ist, werden die Maßnahmen aus der Technische Anlage der Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis der Bundesärztekammer und Kassenärztlichen Bundesvereinigung (Bundesärztekammer, Kassenärztliche Bundesvereinigung, 2018) zugrunde gelegt. Wenn einzelne Maßnahmen zu spezifisch auf die ärztliche Tätigkeit sind (z.B. Einsatz eines Heilberufsausweises oder des Konnektors zum Anschluss an die Telematik-Infrastruktur) werden vergleichbare Maßnahmen gleicher Stärke implementiert. Somit wird ein vergleichbares Sicherheitsniveau erzielt.

Um angemessene Maßnahmen für Datenschutz und Informationssicherheit zu ermitteln, wurde zusätzlich ein Sicherheitskonzept nach der ISIS12-Methodik[2] angefertigt und ein ISMS initialisiert. ISIS12 ist an ISO/IEC 27001 angelehnt bzw. kompatibel und bietet in einem Risiko orientierten Ansatz einen Leitfaden und ein Überblick u.a. über die Konzeption und Umsetzung von angemessenen Sicherheitsmaßnahmen. Das Sicherheitskonzept wird ständig weiterentwickelt und kann somit zur Etablierung und Erhaltung des Sicherheitsniveaus im Projekt dienen.

Zum Zeitpunkt der Erstellung dieser Version des Datenschutzkonzeptes wird außerdem ein Data Management Plan erstellt. Dieser soll eine strukturierte Übersicht über die Datenerhebung und Verarbeitung der einzelnen Teilprojekte und effektiv über sämtliche Datenflüsse im Gesamtprojekt liefern.

Im Sinne der in 7.2.4 und 7.2.5 beschriebenen Schutzziele wurden die im Projekt eingesetzten Geräte mithilfe eines durch den Dienstleister Pegasus GmbH betriebenen Virtual Private Networks (VPN) geschützt. Das abgeschottete Netzwerk wird mittels dafür eingerichteter Router, einem VPN-Konzentrator und einer Firewall mit Advanced Threat Protection (Versorgung mit real-time Signaturen für aktuelle Angriffe) im Sinne von Managed Security realisiert. Alle Geräte, welche an Projektteilnehmer*innen gegeben werden, sowie alle zentralen Dienste des Projektes werden in diesem abgeschotteten Netzwerk betrieben. Pegasus betreibt zudem ein im Projekt genutztes Kalender- und Dateiablagesystem innerhalb des geschützten VPNs. Hierbei wird ein Nextcloud-Server von Pegasus betrieben und im Sinne von Managed Security verwaltet. Der Betreiber verfügt dabei über Zertifikate nach ISO/IEC 27001 und den für Datenschutz spezialisierten ISO/IEC 27018.

[2] vgl. https://de.wikipedia.org/wiki/ISIS12

9 RISIKOBETRACHTUNG

Die Risikobetrachtung wurde als Schwellwertanalyse in Kap. 7.3.1 durchgeführt.

10 MITGELTENDE UNTERLAGEN

- Projektantrag
- Forschungsdesign
- Pseudonymisierung im Projekt TePUS
- Liste der Apps die verwendet werden sollen und deren Verträge zur Auftragsverarbeitung
-Security Policy

11 BEREICHSSPEZIFISCHE ERGÄNZUNGEN

Es werden keine bereichsspezifischen Ergänzungen angewandt.

LITERATUR

AK Technik der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Hrsg.) (2020). *Das Standard-Datenschutzmodell: Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele. Trier:* AK Technik der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder.

Bundesärztekammer, Kassenärztliche Bundesvereinigung (2018). Technische Anlage: Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis. Online verfügbar unter https://www.kbv.de/media/sp/Technische_Anlage_Datenschutz.pdf, Köln: Deutscher Ärzte-Verlag. https://doi.org/10.3238/arztebl.2018.ds01.

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS), Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“, ZTG Zentrum für Telematik und Telemedizin GmbH (2016). Leitfaden für die Erstellung von Datenschutzkonzepten im Gesundheitswesen. Köln: Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS).

Ettl, K., Greiner, N., Kudienko, N., Lauer, N., Lichtenauer, N., Meussling-Sentpali, A. et al. (2020). Telepräsenzroboter für die Pflege und Unterstützung von Schlaganfallpatientinnen und –patienten: Forschungsdesign TP2. Unveröffentlichtes Manuskript, Ostbayerische Technische Hochschule Regensburg.

Haug, S., Currle, E., Frommeld, D. & Weber, K. (2020). *Telepräsenzroboter für die Pflege und Unterstützung von Schlaganfallpatientinnen und -patienten (TePUS): Pseudonymisierung im Projekt TePUS*, Unveröffentlichtes Manuskript, Ostbayerische Technische Hochschule Regensburg.

Rost, M. (2019). Art. 35 DSGVO: Durchführung einer Schwellwert-Analyse (Workshop). Online verfügbar unter https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Fachkongress/Fachkongress_2019/TAG1/4_IT_SIC_DatSch/Rost__Schwellwertanalyse_V2d.pdf?__blob=publicationFile&v=1, Lübeck: Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein.

Weber, K., Raptis, G:, Haug, S., Meussling-Sentpali, A., Mohr, C., Lauer, N. & Pfingsten, A. (2019). Forschungsvorhaben: Telepräsenzroboter für die Pflege und Unterstützung von Schlaganfallpatientinnen und -patienten (TePUS) im Regierungsbezirk Oberpfalz: DeinHaus 4.0. Unveröffentliches Manuskript.

IMPRESSUM

Christof Popp, Georgios Raptis: Datenschutzkonzept, Version 1.1

Projekt „Telepräsenzroboter für die Pflege und Unterstützung von Schlaganfallpatientinnen und -patienten (TePUS) im Regierungsbezirk Oberpfalz: DeinHaus 4.0“

Teilprojekt TP1, Prof. Dr. Georgios Raptis, eHealth Labor der OTH Regensburg

Stand: Dezember 2021

Erscheinungsdatum: 23.12.2021

Herausgeber:

Ostbayerische Technische Hochschule (OTH) Regensburg

Projektmanagement und Kontakt:

Gudrun Bahr, M.A.

Ostbayerische Technische Hochschule Regensburg
Postfach 12 03 27
93025 Regensburg Deutschland

E-Mail: info@deinhaus40.de
WWW: https://www.deinhaus40.de/start

Projektleitung:

Prof. Dr. Karsten Weber, Kompetenzzentrum „Institut für Sozialforschung und Technikfolgenabschätzung (IST)

http://www.oth-regensburg.de/ist