MKM + PARTNER
RECHTSANWÄLTE

Stellungnahme zur datenschutzrechtlichen Zulässigkeit bei der Verarbeitung von personenbezogenen Daten im Rahmen des Projektes TELE-KASPER

23.11.2021

A. Management Summary

Aufgrund der uns vorliegenden Dokumente und Unterlagen halten wir die Verarbeitung von personenbezogenen Daten innerhalb des Projekts TELE-KASPER, sowohl innerhalb der Applikation als auch außerhalb derselben für datenschutzrechtlich zulässig und damit in Einklang mit den Vorschriften der EU-Datenschutz-Grundverordnung („DSGVO"). Insbesondere werden die Grundprinzipien der DSGVO, namentlich „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz", „Zweckbindung", „Datenminimierung", „Richtigkeit", „Speicherbegrenzung" und „Integrität und Vertraulichkeit" gewahrt. Wir gehen zudem davon aus, dass die Rechenschaftspflicht erfüllt wird, sofern die erforderlichen Dokumentationen gepflegt werden. Die Grundsätze „Datenschutz durch Technikgestaltung" und „Datenschutzfreundliche Voreinstellungen" halten wir ebenfalls für erfüllt.

Im Ergebnis befinden wir das Vorhaben insgesamt daher für datenschutzkonform.

Inhaltsverzeichnis

B. Allgemeines

1. Beschreibung des Vorhabens

TELE-KASPER steht für „Telemedizinisches Kompetenznetzwerk Antibiotic Stewardship in Pediatrics“ und ist ein Projekt, das die Antibiotika-Gabe bei Kindern optimieren und den Verbrauch um mindestens 20 Prozent reduzieren soll. Beteiligt daran sind vier Universitätskliniken – das LMU Klinikum München, das Universitätsklinikum Halle (Saale), das Universitätsklinikum Essen und das Universitätsklinikum des Saarlandes in Homburg -, die als „Hubs“ für die ebenfalls am Projekt teilenehmenden umliegenden nicht-universitären Kinderkliniken bzw. Krankenhäuser mit Kinderstationen fungieren, sowie die AOK Bayern. Die statistische Auswertung wird durch das Institut für soziale Pädiatrie und Jugendmedizin an der Ludwig-Maximilian-Universität München (für die Module TELE-Info und TELE-Konsil) sowie durch das Institut für Med. Epidemiologie, Biometrie und Informatik der medizinischen Fakultät der Martin-Luther-Universität Halle-Wittenberg (im Rahmen der Punkt-Prävalenz-Erhebung und der Auswertung aggregierter Daten) übernommen.

Mittels Telemedizin und App als Kommunikationsmittel können sich Kinderärztinnen und -ärzte nicht-universitärer Krankenhäuser zum Einsatz von Antibiotika von Experten beraten lassen.

Mit der **TELE-KASPER App** wird ein zentrales Kommunikationsmittel geschaffen, das für behandelnde Ärzte als Nachschlagwerk fungiert und der direkten Kommunikation bei infektiologischen Fragestellungen, zu Fort- und Weiterbildungszwecken sowie als Plattform der Prozessevaluation zwischen Kinderklinik bzw. Krankenhäuser mit Kinderstationen und Hub dient.

2. Beteiligte

2.1. Nicht-universitäre Kliniken

Nicht-universitäre Kliniken sind in vier regionalen Netzwerken zusammengeschlossen. Jedes Netzwerk wird von einem Hub koordiniert. Ärzte der Kinderklinken können über die App in verschiedenen Behandlungssituationen Anfragen an die in den Hubs tätigen Ärzte stellen.

2.2. Hub - Universitäre Klinik mit Expertise im Bereich pädiatrisches Antibiotic Stewardship und Infektiologie

Hub-Mitarbeiter bieten den nicht-universitären Kliniken Beratungen und Konsile in Form von Kurzantworten via App (bei niedrigkomplexen Anfragen), Telemedizinische Einzelkonsile (1-2-1 Konsil oder 1-2-2 Konsil bei dringlichen oder moderat komplexen Fällen), Telemedizinische Fallkonferenzen (bei komplexeren Fällen) oder *bedside Konsile* vor Ort (wenn eine persönliche Untersuchung des Patienten unabdingbar ist) an.

2.3. LMU Klinikum München

Das LMU Klinikum München nimmt eine zentrale Stellung ein und stellt sowohl die Konsortialführung als auch die ärztliche Projektleitung für das Gesamtnetzwerk. Das LMU Klinikum München ist Inhaberin der App und somit Verantwortliche im Sinne der DSGVO für die Verarbeitung personenbezogener Daten innerhalb der App[1].

2.4. Universitätsklinikum Halle (Saale)

Auf dem Server des Universitätsklinikums Halle (Saale) werden alle pseudonymisierten Patientendaten aus der App, die pseudonymisierten Nutzerdaten (Nutzerprofil), die Daten aus der Prozessevaluation, Daten aus der Punkt-Prävalenz-Erhebung sowie aggregierte (Patienten) Daten gespeichert.

2.5. Institut für soziale Pädiatrie und Jugendmedizin

Zur Prozessevaluation erfolgt nach jeder Nutzung der App durch Arzt und Hub-Mitarbeiter eine kurze standardisierte Befragung. Informationen zur App-Nutzung und Zufriedenheit der Ärzte werden in der EDC Software erfasst und zur Auswertung an das Institut für soziale Pädiatrie und Jugendmedizin der Ludwig-Maximilian-Universität München gesendet.

2.6. Institut für Medizinische Epidemiologie, Biometrie und Informatik an der Martin-Luther-Universität Halle-Wittenberg

Das Institut erhält zur Auswertung aggregierte Daten zum Antibiotikaverbrauch.

Die Daten werden vom Krankenhauscontrolling der nicht-universitären Kliniken an die zuständigen Hubs übermittelt. Die Hubs leiten die erhaltenen Daten nach deren Validierung in aggregierter Form an das Institut weiter.

2.7. MEKmedia GmbH

Die MEKmedia GmbH ist mit der Entwicklung der TELE-KASPER-App und darüber hinaus mit der Wartung des MS SQL Datenbankservers des Universitätsklinikums Halle beauftragt.

In der Microsoft Azure Cloud der MEKmedia GmbH werden keine personenbezogenen Daten gespeichert, sondern vielmehr Nutzerdaten und nicht patientenbezogene Daten als Inhalte der App-

[1] Das LMU Klinikum München bestimmt über die Zwecke und Mittel der Datenverarbeitung im Sinne von Art. 4 Nr. 7 DSGVO. Das LMU Klinikum München geht dabei selbst – aus unserer Sicht zutreffend – von dieser Rolle aus. Bei der Prüfung konnten wir keine Anhaltspunkte identifizieren, die gegen eine Stellung als Verantwortliche sprechen. Aus Gründen der Übersichtlichkeit sehen wir von einer ausführlichen Begründung der Eigenschaft als Verantwortliche ab.

Module Information & Weiterbildung und Nachschlagewerk sowie nicht patientenbezogene Daten aus inhaltlichen Fragen zum Nachschlagewerk und aus Feedbackfragebögen im Rahmen der Prozessevaluation zum Modul TELE-Info.

Im Rahmen der Wartungsarbeiten auf dem MS SQL Datenbankserver des Universitätsklinikums Halle kann ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden. Die datenschutzkonforme Gestaltung möglicher Zugriffe ist durch den Abschluss eines Auftragsverarbeitungsvertrages zwischen MEKmedia und dem Universitätsklinikum Halle sichergestellt.

3. Beschreibung des Datenfluss

Im Projekt TELE-KASPER werden personenbezogene Daten sowohl in der TELE-KASPER App als auch außerhalb der App verarbeitet.

3.1. Verarbeitung von personenbezogenen Daten innerhalb der App

Der App-Bereich „**Kommunikation**“ ermöglicht die Erstellung allgemeiner oder patientenbezogener Anfragen.

Ärzte nicht-universitärer Kliniken haben die Möglichkeit in verschiedenen Behandlungssituationen Anfragen zu Beratungen an den lokalen Hub zu stellen. Die Anfrage erfolgt über ein Anfrageformular in der App. Niedrigkomplexe Anfragen können direkt in der App durch den Arzt oder Apotheker des jeweiligen Hubs beantwortet werden. Der zuständige Hub-Arzt hat erweiterte Rechte in der App um Anfragen bei Bedarf weiterzuleiten oder an andere Hubs zu eskalieren.

Das Kommunikations-Tool der TELE-KASPER-App beinhaltet die Module **TELE-Konsil** und **TELE-Info**.

3.1.1. Modul TELE-Konsil

Das Modul ermöglicht Beratungen mittels pseudonymisierten Patientendaten.

3.1.1.1. Welche Daten werden im Modul TELE-Konsil verarbeitet?

3.1.1.1.1. Persönliches Profil

Beim erstmaligen Gebrauch der App wird der Nutzer (Arzt oder Apotheker) aufgefordert, sein persönliches Profil anzulegen, mit Angaben zu:

> **Geschlecht, Alter in 5-Jahresspannen, Position in der Klinikhierarchie, Jahr der Approbation, Jahr der Facharztausbildung und Wochenarbeitszeit** und **optional dem Klarnamen**.

Diese Daten können vom Profilinhaber während der Projektlaufzeit angepasst werden.

Aufgrund der verschiedenen Klinikgrößen kann eine genaue Zuordnung der Nutzers anhand der Daten zu Alter, Position und Qualifikation nicht mit Sicherheit ausgeschlossen werden. Diese Daten werden deshalb als pseudonymisiert behandelt. Widerruft der Nutzer seine Einwilligung zur Verarbeitung seiner Daten, so werden alle bis dahin gespeicherten Daten anonymisiert und das Nutzerprofil gelöscht.

Die Daten zum persönlichen Profil des Nutzers werden auf dem MS SQL Datenbankserver des Universitätsklinikums Halle gespeichert.

3.1.1.1.2. Nutzercode

Für jeden Arzt wird bei der Erstnutzung der App ein Nutzercode als Benutzer-ID generiert. Der Nutzercode setzt sich aus der Klinik-ID und der Arzt-ID (fortlaufende Nummer, die innerhalb der App generiert wird) zusammen. Jeder Arzt hat somit seine eigene Kennung.

3.1.1.1.3. Nutzungsdaten

Zudem werden folgende Nutzungsdaten erfasst:

> **Art des Endgerätes** (Smartphone, Tablet oder Desktop-PC), **Art des Netzes** (z.B. mobil oder Klinik-intern), **Datum der Nutzung.**

Diese Daten dienen der Auswertung technischer Aspekte der App-Nutzung.

3.1.1.1.4. Pseudonymisierte Patienten-Daten

Im Anfrageformular in der App werden die für eine Empfehlung notwendigen Patientendaten zu

Alter, Geschlecht, Körpergröße, Gewicht

abgefragt. Es werden keine Angaben zum Namen oder dem Geburtsdatum des Patienten gemacht.

Die pseudonymisierten Patientendaten werden unter einer Patienten-ID und der zugehörigen Klinik-ID erfasst. Eine direkte Zuordnung zum Patienten innerhalb der App ist somit nicht möglich. Nur der behandelnde Arzt kann den Fall einem bestimmten Patienten zuordnen.

3.1.1.2. Rechtsgrundlage der Verarbeitung

3.1.1.2.1.1. Persönliches Profil, Nutzercode, Nutzungsdaten

Zu Beginn der Erstnutzung wird mittels einer in der App datenschutzrechtlichen Aufklärung, die Einwilligung des Nutzers zur Verarbeitung und eine mögliche Übermittlung seiner Daten in ein Drittland eingeholt. Ohne Einverständnis ist die Nutzung der App nicht möglich.

Die Einwilligung wird zudem bei Erstellung jeder neuen Anfrage eingefordert. Rechtsgrundlage der Verarbeitung ist Art. 6 Abs. 1 S. 1 lit. a DSGVO i. V. m. Art. 49 Abs. 1 lit. a DSGVO.

3.1.1.2.1.2. Pseudonymisierte Patientendaten

Patientendaten sind besonders sensible personenbezogene Daten, die einen besonderen Schutz verdienen. Zielgruppe des Projektes TELE-KASPER sind pädiatrische Patienten.

Die Verarbeitung personenbezogener Daten von Kindern, die noch nicht das sechzehnte Lebensjahr vollendet haben, ist nur rechtmäßig, sofern die/der Erziehungsberechtigte zustimmt. Eltern/Erziehungsberechtigte werden über die Verarbeitung der pseudonymisierten pädiatrischen Patientendaten im Rahmen des Tele-Konsils, der Fallkonferenzen und der Punkt-Prävalenz-Erhebung aufgeklärt. Anschließend wird deren aktive Einwilligung eingeholt.

Die Aufnahme pseudonymisierter Patientendaten in den Aufnahmebogen der App erfordert die explizite Bestätigung des behandelnden Arztes, dass die schriftliche Einwilligungserklärung der/des Eltern/Erziehungsberechtigten in die Verarbeitung dieser Daten im Rahmen eines Tele-Konsils, einer Fallkonferenzen bzw. einer Punkt-Prävalenz-Erhebung vorliegt. Rechtsgrundlage der Verarbeitung ist Art. 6 Abs. S. 1 lit. a DSGVO i.V.m. Art. 9 Abs. 2 lit. a DSGVO i.V.m. Art. 8 DSGVO

3.1.1.3. Zu welchem Zweck erfolgt die Verarbeitung im TELE-Konsil

3.1.1.3.1. Persönliches Profil, Nutzercode, Nutzungsdaten

Die App wird für Anfragen behandelnder Ärzte in verschiedenen Behandlungssituationen und für die Beratung durch Hub-Mitarbeiter genutzt.

3.1.1.3.2. Pseudonymisierte Patientendaten

Der behandelnde Arzt nimmt die pseudonymisierte Patientendaten in den Anfragebogen zu Beratungszwecken auf. HUB-Mitarbeiter können diese Informationen gemäß Rechte- und Rollenkonzept abrufen und innerhalb des TELE-Konsils Empfehlungen zur Therapie aussprechen, welche dem Nutzer der nicht-universitären Klinik nach Abruf wieder zur Verfügung stehen.

3.1.1.4. Wie lange werden die pseudonymisierten personenbezogenen Daten gespeichert?

3.1.1.4.1. Persönliches Profil, Nutzercode, Nutzungsdaten

Widerruft ein Nutzer seine Einwilligung für die Verarbeitung seiner pseudonymisierten personenbezogenen Daten, so werden alle bis dahin erfassten Daten anonymisiert. Anschließend wird das Nutzerprofil gelöscht.

3.1.1.4.2. Pseudonymisierte Daten

Im Hinblick auf die Aufbewahrung der pseudonymisierten Patientendaten konnten wir, in den uns zur Verfügung gestellten Unterlagen, keine Aussage hierzu finden. Wir gehen daher davon aus, dass diese Daten den gleichen Löschfristen unterliegen, wie dies bei der Patientenakte der Fall ist.

3.1.1.5. An wen werden die Daten innerhalb des Moduls TELE-Konsil übermittelt?

Sowohl das Nutzerprofil als auch die pseudonymisierten Patientendaten werden innerhalb des gesicherten Kliniknetzes des Universitätsklinikums Halle (Saale) gespeichert. Eine Weiterleitung an Dritte außerhalb des Kliniknetzes findet nicht statt.

Die Nutzerdaten werden auf dem Server der MEKmedia GmbH gespeichert. Die MEKmedia GmbH nutzt den Cloud-Dienst Microsoft Azure. Der Standort des Servers der MEKmedia GmbH ist Deutschland. Microsoft Azure ist ein Dienst von Microsoft Ireland Operations Ltd, Building 3, Sandyford Business Estate, Dublin 18, Ireland. Als US-Unternehmen fällt Microsoft unter die Section 702 des FISA (Foreign Intelligence Surveillance Act), die E.O. 12333 (Überwachungsprogramme PRISM und/oder UPSTREAM) sowie dem sog. CLOUD Act. Dieser erlaubt staatlichen Behörden in den USA Zugriff auf die von Microsoft gespeicherten Daten, auch von Unionsbürgern und auch wenn diese nicht in den USA gespeichert werden. Ein wirksamer Rechtsbehelf steht Unionsbürgern nicht zur Verfügung.

Die MEKmedia GmbH hat mit Microsoft Corporation einen Auftragsverarbeitungsvertrag geschlossen, der den Anforderungen des Art. 28 DSGVO entspricht. Ein angemessenes Datenschutzniveau ist zum einen durch den Abschluss der sog. EU-Standardvertragsklauseln garantiert. Darüber hinaus enthalten die neuen Vertragsklauseln von Microsoft Regelungen, die unmittelbar die Nutzerrechte stärken. Der Datenschutzbeauftragte der MEKmedia GmbH hat die Verwendung der Azur-Cloud und damit die theoretische Möglichkeit des Zugriffs von US-Sicherheitsbehörden oder US-Geheimdiensten im Rahmen eines Transfer Impact Assessments aus datenschutzrechtlicher Sicht bewertet und ist zu dem Ergebnis gekommen, dass mit der Speicherung der Daten in der Azure-Cloud kein erhöhtes Risiko für die Rechte und Freiheiten der Betroffenen besteht. Das Assessment ist gemäß den Anforderungen des Europäischen Gerichtshofs in der Causa „Schrems II“ und den daraus resultierenden Empfehlungen des Europäischen Datenschutzausschusses durchgeführt. Dabei wurden die sich aus dem Transfer ergebenden Risiken analysiert und mit den getroffenen vertraglichen und technischen Sicherheitsmaßnahmen bewertet.

3.1.1.6. Technische und organisatorische Maßnahmen

Die Speicherung der pseudonymisierten Patientendaten und des Nutzerprofils findet ausschließlich innerhalb des gesicherten Kliniknetzes des Universitätsklinikums Halle (Saale) mit betriebseigenen Geräten, auf denen sich die Mitarbeiter mittels persönlicher Kennung und Passwort authentifizieren müssen, statt.

Sowohl die Nutzer- als auch die Patientendaten werden in pseudonymisierter Form verarbeitet. Nur der behandelnde Arzt kann die Patientendaten (den Fall) einem bestimmten Patienten zuordnen.

Der Zugriff auf die Informationen im TELE-Konsil ist durch ein Rechtesystem auf den erforderlichen Nutzerkreis (zuständige HUB-Mitarbeiter) beschränkt.

Durch die Aufnahme von Vereinbarungen über die gemeinsame Verantwortung gem. Art. 26 DSGVO (Joint Controller Agreement/JCA) in die Konsortial- und Kooperationsverträge und darüber hinaus durch den Abschluss der erforderlichen Auftragsverarbeitungsverträge nach Art. 28 DSGVO zwischen MEKmedia und dem Uniklinikum Halle wegen der Wartung des MS SQL Datenbankservers sowie zwischen MEKmedia und dem LMU Klinikum München als Inhaberin der App und als deren Verantwortliche im Sinne der DSGVO, wird in transparenter Form festgelegt, wer welche Verpflichtungen gemäß der DSGVO zu erfüllen hat, um somit einen angemessenen Schutz der personenbezogenen Daten sicherzustellen.

3.1.2. Modul TELE-Info

3.1.2.1. Welche Daten werden verarbeitet

Im Modul TELE-Info werden die unter Punkt 3.1.1.1.2 und 3.1.1.1.3 dieser Stellungnahme genannten Daten verarbeitet. Eine Verarbeitung von (pseudonymisierten) Patientendaten erfolgt hingegen innerhalb dieses Moduls nicht.

3.1.2.2. Rechtsgrundlage der Verarbeitung

Die pseudonymisierten Nutzerdaten werden aufgrund der Einwilligung des App-Nutzers verarbeitet. Die Einwilligung wird bei Erstellung jeder neuen Anfrage eingefordert. Rechtsgrundlage der Verarbeitung ist Art. 6 Abs. 1 S. 1 lit. a DSGVO i. V. m. Art. 49 Abs. 1 lit. a DSGVO.

3.1.2.3. Zu welchem Zweck erfolgt die Datenverarbeitung

Die Verarbeitung der pseudonymisierten Nutzerdaten ist für die nicht patientenbezogenen Fragestellungen und deren Beantwortung erforderlich.

3.1.2.4. Wie lange werden die personenbezogenen Daten gespeichert?

Die Nutzerdaten bleiben für die Dauer des Projektes gespeichert.

Widerruft ein Nutzer seine Einwilligung für die Verarbeitung seiner pseudonymisierten personenbezogenen Daten, so werden alle bis dahin erfassten Daten anonymisiert. Anschließend wird das Nutzerprofil gelöscht.

3.1.2.5. An wen werden die Daten weitergegeben?

Um unnötige Doppelungen zu vermeiden wird hinsichtlich der Datenweitergabe auf die Ausführungen in Punkt 3.1.1.5 verwiesen, die auch für das Modul TELE-Info Anwendung finden.

3.1.2.6. Technische und organisatorische Maßnahmen

Das Modul TELE-Info ist innerhalb der App farblich so gekennzeichnet, dass eine optische Unterscheidung zu dem Modul TELE-Konsil gewährleistet ist.

Eine Checkbox stellt sicher, dass die allgemeine Anfrage keine patientenbezogene Daten enthält. Erst nach einer aktiven Bestätigung der Checkbox, kann die Anfrage abgesendet werden.

Durch die Aufnahme von Vereinbarungen über die gemeinsame Verantwortung gem. Art. 26 DSGVO (Joint Controller Agreement/JCA) in die Konsortial- und Kooperationsverträge und darüber hinaus durch den Abschluss der erforderlichen Auftragsverarbeitungsverträge nach Art. 28 DSGVO zwischen MEKmedia und dem Uniklinikum Halle, wegen der Wartung des MS SQL Datenbankservers sowie zwischen MEKmedia und dem LMU Klinikum München als Inhaberin der App und somit als deren Verantwortliche, wird in transparenter Form festgelegt, wer welche Verpflichtungen gemäß der DSGVO zu erfüllen hat, um somit einen angemessenen Schutz der personenbezogenen Daten sicherzustellen.

3.1.3. Prozessevaluation-App

Nach jeder Nutzung der App durch den behandelnden Arzt und Hub-Mitarbeiter erfolgt eine standardisierte Befragung anhand des Nutzercodes (Klinik- und Arzt-ID). Damit sollen Art und Frequenz der App-Nutzung und die Nutzerzufriedenheit sowie die Relevanz der App-Nutzung für die Therapieentscheidung evaluiert werden.

3.1.3.1. Welche Daten werden im Rahmen der Prozessevaluation verarbeitet?

Unter der bei Erstnutzung generierter Arzt-ID werden Daten zur Person und der genutzten Hardware (z.B. Smartphone, Tablet, Desktop-PC), der Art der Internetverbindung (z.B. mobil, privat,

Klinik-intern), dem Einsatzort (z.B. Art der Station) und studienspezifische Aktivitäten des Nutzers innerhalb der App erfasst.

3.1.3.2. Rechtsgrundlage der Verarbeitung

Rechtsgrundlage der Verarbeitung personenbezogener Daten im Rahmen der Prozessevaluation ist das berechtigte Interesse der teilnehmenden nicht-universitären und universitären Kliniken (Art. 6 Abs. 1 S. 1 lit. f DSGVO).

Das berechtigte Interesse besteht in der Evaluation der Häufigkeit der App-Nutzung, der Zeiträume zwischen abgesendeter Anfrage und abschließender Beantwortung, der Nutzerzufriedenheit und des Erfolgs der App-Nutzung für die einzelnen Anfragen.

3.1.3.3. Zu welchem Zweck erfolgt die Verarbeitung?

Um die Nutzerzufriedenheit und die Frequenz sowie die die Relevanz der App-Nutzung für die Therapieentscheidung zu evaluieren, erfolgt eine standardisierte Befragung anhand des Nutzercodes. Daten aus den Feedbackfragebögen TELE-Konsil und TELE-Info sowie pseudonymisierte Nutzerdaten dienen in aufbereiteter Form dem Institut für soziale Pädiatrie und Jugendmedizin an der Ludwig-Maximilian-Universität München zur Prozessevaluation.

3.1.3.4. Wie lange werden die personenbezogenen Daten gespeichert?

Die erhobenen Daten bleiben für die Dauer des Projektes gespeichert.

3.1.3.5. An wen werden die Daten weitergegeben?

Module TELE-Konsil und TELE-Info: Das Nutzerprofil sowie die Daten aus den Feedbackfragebögen TELE-Info und TELE-Konsil werden zur Prozessevaluation an das Institut für soziale Pädiatrie und Jugendmedizin der Ludwig-Maximilian-Universität München exportiert. Eine Weiterleitung der Daten aus dem Feedbackfragebogen TELE-Konsil außerhalb des Kliniknetzes findet nicht statt.

Modul TELE-Info: Nicht patientenbezogene Daten aus Feedbackfragebögen TELE-Info werden auf dem Server der MEKmedia GmbH gespeichert.

3.1.3.6. Technische und organisatorische Maßnahmen

Im Rahmen der Prozessevaluation werden die Daten durch strikt definierte Zugriffsrechte von anderen Datenerhebungs-Prozessen getrennt erhoben und innerhalb des Kliniknetzes durch das Institut für soziale Pädiatrie und Jugendmedizin an der Ludwig-Maximilian-Universität München ausgewertet.

Für die Erhebung und Auswertung der Daten wird die Electronic Data Capture (EDC) Software LimeSurvey eingesetzt. Anhand der Veröffentlichung unter dem Link https://www.lmu-klinikum.de/neue-technologien-internet-intranet/umfragen/2b151baa6be47371 ist von einer datenschutzrechtlichen Prüfung der Software durch das LMU Klinikum München auszugehen. Eine gesonderte Prüfung durch MKM ist nicht erfolgt, da nicht vom Auftrag erfasst.

3.2. Verarbeitung von personenbezogenen Daten außerhalb der App

Beratungen, die über eine Kurzanfrage hinausgehen (Telemedizinische Einzelkonsile oder Fallkonferenzen) und den Austausch detaillierter Informationen notwendig machen, finden außerhalb der App statt. So kann der zuständige Arzt des Hubs entscheiden, dass die Frage innerhalb des Hubs nicht beantwortet werden kann und die Anfrage an die Koordinatoren der anderen Hubs weitergeben. Komplexere Fälle können in videogestützten Telefon-Konsile (Einzelkonsile) oder telemedizinischen Fallkonferenzen behandelt werden. Auf besonderen Wunsch der anfragenden Klinik und nur für spezielle Probleme sind auch Konsile am Krankenbett (Bedside Konsil) möglich. Hub-Koordinator, Arzt und der hinzugezogene Spezialist können abschließend darüber entscheiden, ob die Anfrage in anonymisierter Form mit der entsprechender Antwort in der App als Fortbildungsangebot für alle App-Nutzer hinterlegt wird.

Über jedes Konsil bzw. jede Fallkonferenz findet außerhalb der App eine schriftliche Dokumentation unter der dazugehörigen Fall-ID statt. Diese wird anschließend der anfragenden Klinik zugesandt und kann in der Patientenakte abgelegt werden.

3.2.1. Einzel-Konsile und Fallkonferenzen

3.2.1.1. Welche Daten werden verarbeitet?

Es werden die vom behandelnden Arzt im Anfrageformular der App erfassten pseudonymisierten Patientendaten verarbeitet.

Eine direkte Zuordnung zum Patienten ist somit nicht möglich. Nur der behandelnde Arzt kann den Fall anhand der Patienten-ID und der zugehörigen Klinik-ID einem bestimmten Patienten zuordnen. Videokonferenzen werden über das Tool „Zoom“ abgehalten. Dabei werden die Nutzerdaten der Konferenzteilnehmer verarbeitet. Der Umfang dieser Daten hängt davon ab, welche Angaben zu Daten der jeweilige Teilnehmer macht.

3.2.1.2. Rechtsgrundlage der Verarbeitung?

Die Verarbeitung außerhalb der App findet nur nach vorliegender Einwilligungserklärung der Eltern/Erziehungsberechtigten statt.

Rechtsgrundlage ist Art. 6 Abs. 1 S. 1 lit. a DSGVO i. V. m. Art. Art. 8 Abs. 1 DSGVO i.V. m. Art. 9 Abs. 2 lit. a DSGVO.

3.2.1.3. Zu welchem Zweck erfolgt die Verarbeitung?

Die Verarbeitung pseudonymisierter Patientendaten innerhalb der Einzel-Konsile und Fallkonferenzen dient dem Austausch detaillierter Informationen bei komplexen Fällen.

3.2.1.4. Wie lange werden die personenbezogenen Daten gespeichert?

Die Dokumentation der pseudonymisierten Patientendaten unter der entsprechenden Fall-ID wird in der Patientenakte abgelegt und unterliegt der hier definierten Löschfrist.

Bei Widerruf der erteilten Einwilligung der Eltern/Erziehungsberechtigten werden keine weiteren Daten des betroffenen Patienten in einem Konsil oder einer Fallkonferenz besprochen.

3.2.1.5. An wen werden die Daten weitergegeben?

Die pseudonymisierten Patientendaten werden innerhalb des gesicherten Kliniknetzes des Universitätsklinikums Halle (Saale) gespeichert. Eine Weiterleitung an Dritte außerhalb des Kliniknetzes findet nicht statt.

Die unter der Fall-ID erstellte schriftliche Dokumentation der Telefon-Konsile bzw. der Fallkonferenzen werden in den Patientenakten abgelegt.

3.2.1.6. Technische und organisatorische Maßnahmen

Die Erstellung und Speicherung der Dokumentation der Konsile und Fallkonferenzen findet ausschließlich innerhalb des gesicherten Kliniknetzes mit betriebseigenen Geräten, auf denen sich die Mitarbeiter mittels persönlicher Kennung und Passwort authentifizieren müssen, statt.

Der Versand der Befunde oder der Konsil-Dokumentationen an die anfragende Klinik erfolgt auf dem Postweg oder über verschlüsselte E-Mail bzw. Fax.

3.2.2. Punkt-Prävalenz-Erhebung

Um die Verordnungsqualität von Antibiotika zu erfassen, wird durch Ärzte in den einzelnen Kliniken in Zusammenarbeit mit den Mitarbeitern der regionalen Hubs quartalsweise eine Punkt-Prävalenz-Erhebung (PPE) durchgeführt.

Die erhobenen Daten werden lokal auf Kinderklinikebene streng vertraulich behandelt und innerhalb des Projekts nur in anonymisierter Form ausgewertet.

Die Daten werden durch Fachärzte oder Facharztäquivalenz unter einer fortlaufenden Nummer online erfasst und an das zuständige Uniklinikum, an den verantwortlichen Hub-Koordinator übermittelt. Im Nachgang werden die Daten anonymisiert. Der zuständige Hub prüft die Mitteilungen und erfasst die Daten in die EDC. Anschließend leitet der Hub die anonymisierten Daten an das Institut für Epidemiologie, Biometrie und Informatik der Martin-Luther-Universität in Halle-Wittenberg weiter. Das Institut verarbeitet die Daten und wertet sie aus.

3.2.2.1. Welche Daten werden verarbeitet?

Lokal in nicht-universitären Kliniken:

Personenbezogene Daten wie ***Name – Vorname – Geburtsdatum,*** die der Identifikation des Patienten dienen, und die ***Fall-ID***, als fortlaufende Nummer werden in einer Patientenidentifikationsliste in der Klinik lokal erfasst.

Online-Fragebögen:

Die pseudonymisierten Patienten- und Behandlungsdaten, wie ***Alter – Gewicht – Körpergröße – mikrobiologische Diagnostik – erhaltene Therapie,*** werden durch Fachärzte oder Fachärzteäquivalenz unter einer Patienten-ID (zusammengesetzt aus Klinik-ID und Fall-ID) über patientenindividuelle Online-Fragebögen in den nicht-universitären Kliniken erfasst und an die zuständigen Hubs übermittelt.

3.2.2.2. Rechtsgrundlage der Verarbeitung?

Der betreuende Arzt klärt die Sorgeberechtigten und bei vorliegender Einsichtsfähigkeit auch die Patienten auf. Anschließend wird deren Einwilligung eingeholt.

Rechtsgrundlage der Verarbeitung ist Art. 6 Abs. 1 S. 1 lit. a DSGVO i. V. m. Art. 8 Abs. 1 DSGVO i. V. m. Art. 9 Abs. 2 lit. a DSGVO.

3.2.2.3. Zu welchem Zweck erfolgt die Verarbeitung?

Die Punkt-Prävalenz-Erhebung wird zum Zweck der Erfassung der Verordnungsqualität von Antibiotika in den einzelnen Kliniken durchgeführt und dient der qualitativen Analyse der antibiotischen Therapie.

3.2.2.4. Wie lange werden die personenbezogenen Daten gespeichert?

Die in den Patientenidentifikationslisten erfassen Patientendaten werden irreversibel vernichtet, sobald die Datenerfassung abgeschlossen ist.

Bei Widerruf der erteilten Einwilligung wird die Datenerhebung gestoppt und alle bis zu diesem Zeitpunkt erfassten Daten werden, soweit nicht bereits erfolgt, anonymisiert.

Die im Rahmen der Punkt-Prävalenz-Erhebung erhobenen Daten werden bis zu 15 Jahre nach Beendigung oder Abbruch der Studie verschlüsselt aufbewahrt und anschließend gelöscht.

3.2.2.5. An wen werden die Daten weitergegeben?

Die pseudonymisierten Patienten- und Behandlungsdaten werden von Fachärzten oder Fachärzteäquivalenz an das zuständige Uniklinikum weitergeleitet.

Eine Weiterleitung außerhalb des Kliniknetzes findet nicht statt.

3.2.2.6. Technische und organisatorische Maßnahmen

Die zur Re-Identifikation benötigten Patientenidentifikationslisten werden ausschließlich in den nicht-universitären Kliniken zugriffssicher aufbewahrt.

Die in der Punkt-Prävalenz-Erhebungen erfassten Daten (Alter, Gewicht, Körpergröße, mikrobiologische Diagnostik, erhaltene Therapie) werden in pseudonymisierter Form in den Online-Fragebogen erfasst. Dies ermöglicht Rückfragen bei vermeintlich fehlerhaften oder unvollständigen Angaben.

Für die Online-Erfassung der pseudonymisierten Patientendaten vor Ort durch Fachärzte oder Fachärzteäquivalenz wird die EDC Software Lime Survey eingesetzt.

Die Patientenidentifikationslisten werden nach Abschluss der Datenerfassung und der Validierung der Daten durch den zuständigen Hub irreversibel vernichtet. Erst in dieser anonymisierten Form werden die Daten an das Institut für Epidemiologie, Biometrie und Informatik an der Martin-Luther-Universität Halle Wittenberg weitergeleitet. Der Anonymisierungsprozess verhindert eine spätere patienten-individuelle Rückverfolgung.

Die in der EDC-Software erfassten Daten werden ausschließlich innerhalb des gesicherten Kliniknetzes des Universitätsklinikums Halle (Saale) gespeichert.

3.2.3. Aggregierte Daten

Für die Evaluation der Versorgungsqualität der Patienten (z.B. die Anzahl der Todesfälle und die Anzahl der stationären Fälle für jeden Monat) und für die Auswertung mikrobiologischer Befunde (um den Anteil der verschiedenen Erreger unter allen Nachweisen, sowie den Anteil sensibler, resistenter und intermediärer Befunde an allen Befunden zu bestimmen), übermitteln die nicht-universitären Kliniken aggregierte Daten an die jeweiligen Universitätskliniken. Der Hub validiert

die erhaltenen Daten und leitet sie dann an das Institut für Epidemiologie, Biometrie und Informatik an der Martin-Luther-Universität Halle Wittenberg zur Auswertung weiter.

3.2.3.1. Welche Daten werden verarbeitet?

Weder die nicht-universitären Kliniken noch das Institut für Epidemiologie, Biometrie und Informatik an der Martin-Luther-Universität Halle Wittenberg erfassen individuelle Patientendaten.

Die Daten aus Strukturfragebögen, der Apotheke, dem Krankenhauscontrolling und aus Erreger- und Resistenzstatistiken werden in aggregierter Form erfasst.

Da aggregierte Daten zum Unterschied zu pseudonymisierten Daten nicht mehr auf eine Person zurückzuführen sind, unterliegen sie nicht der DSGVO.

3.2.3.2. Technische und organisatorische Maßnahmen

Für die oben angeführten Evaluationen und Auswertungen werden keine patientenbezogenen Daten verarbeitet.

Aggregierte Daten aus den Strukturfragebögen, der Apotheke, dem Krankenhauscontrolling und aus Erreger- und Resistenzstatistiken werden von den zuständigen Hubs manuell in die EDC Software LimeSurvey erfasst.

Für alle anderen Daten wird Confluence eingesetzt. Confluence ist ein online Arbeitsbereich für das gemeinsame Projekt- und Wissensmanagement eines Teams. Die hier erfassten aggregierten Daten unterliegen nicht der DSGVO. Confluence bietet zudem die Möglichkeit definierte Seiten durch Zugriffsrechte und Verschlüsselungen zu schützen. Damit kann die Sicherheit erhöht werden. Nur die Hub-Koordinatoren und die Projekt-Mitarbeiter des Institutes für Epidemiologie, Biometrie und Informatik an der Martin-Luther-Universität Halle Wittenberg verfügen über die Berechtigung die aggregierten Daten hochzuladen und auf diese zuzugreifen.

Sowohl die Daten in der EDC Software LimeSurvey als auch die Daten in Confluence werden nur innerhalb des gesicherten Kliniknetzes des Universitätsklinikums Halle (Saale) gespeichert.

C. Fragestellung

Mit diesem Datenschutz-Gutachten soll geprüft werden, ob im Rahmen der Umsetzung des TELE-KASPER-Projektes die geltenden Regelungen zum Datenschutz eingehalten und die personenbezogenen Daten ausreichend geschützt werden. Prüfpunkte sind die Daten-Verarbeitungen innerhalb und außerhalb der TELE-KASPER App, sowie die Patienteninformationen für Jugendliche, Kinder, sowie für Eltern und Erziehungsberechtigte und die damit verbundenen Einverständniserklärungen.

Das Datenschutz-Gutachten wird im Sinne des Art. 25 DSGVO als Vorabprüfung erstellt und dient dazu, das Projekt auf Risiken für die Rechte und Freiheiten der betroffenen Personen zu untersuchen, dies umso mehr, da es bei der Verarbeitung vorwiegend um Gesundheitsdaten von Kindern und Jugendlichen als besondere Art personenbezogener Daten (Art. 8 und Art. 9 DSGVO) geht.

Unter Beachtung der in Artikel 5 DSGVO festgelegten zentralen Grundsätze soll im Ergebnis dieses Gutachtens dokumentiert werden, inwieweit die Datenverarbeitung bei der Umsetzung des TELE-KASPER-Projektes diesen Vorgaben entspricht.

D. Stellungnahme

Im Hinblick auf die Fragestellung lässt sich der geschilderte Sachverhalt im Hinblick auf die Erfüllung der sich aus Art. 5 DSGVO und Art. ergebenden Grundprinzipien wie folgt beantworten:

1. Grundsatz der Rechtmäßigkeit der Verarbeitung, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbare Weise, Art. 5 Abs. 1 lit. a DSGVO

Die Verarbeitung personenbezogener Daten ist rechtmäßig, wenn für die Datenverarbeitung eine Rechtsgrundlage vorliegt und die betroffene Person die Verarbeitung nachvollziehen kann.

Soweit im Rahmen des TELE-KASPER-Projekts personenbezogene Daten verarbeitet werden, wird die Einwilligung der Eltern/Erziehungsberechtigten eingeholt (Verarbeitung nach Art. 6 Abs. 1 S. 1 lit. a für Nutzer der App und darüber hinaus i. V. m. Art. 8 DSGVO und Art. 9 Abs. 2 lit. a für Patienten).

Für eine wirksame Einwilligung müssen die Vorgaben des Art. 7 DSGVO eingehalten werden. Auch bedarf eine datenschutzrechtlich wirksame Aufklärung einer vollständigen Information der betroffenen Personen über die Rechtsgrundlage, den Zweck der Verarbeitung, die Beteiligten, die Speicherdauer der personenbezogenen Daten und die Betroffenenrechte, insbesondere das Recht auf Widerruf für die Zukunft der Einwilligung.

Zudem stützt sich die Verarbeitung der Nutzerdaten auch auf Art. 49 Abs. 1 lit. a DSGVO. Die Speicherung der Nutzerdaten durch die MEKmedia GmbH in der Cloud von Microsoft Azure erfordert ein sogenanntes „Transfer Impact Assessment“, in dem die Risiken für die Betroffenen zu analysieren sind. Das durchgeführte Transfer Impact Assessment hat zu dem Ergebnis geführt, dass für die Nutzerdaten kein Risiko aus deren Speicherung in der Cloud von Microsoft Azure besteht.

In der Datenschutzerklärung der TELE-KASPER App werden Nutzer über die Verarbeitung ihrer personenbezogenen Daten und ihre Rechte aus der Datenschutzgrundverordnung umfassend und ausreichend informiert.

Das Gleiche trifft auch für die Aufklärung der Patienten und deren Eltern/Erziehungsberechtigten zu. Erst nach einer umfassenden Aufklärung sowohl der Patienten (Kinder und Jugendliche) als auch der Eltern/Erziehungsberechtigten wird um deren Einwilligung gebeten.

2. Grundsatz der Zweckbindung, Art. 5 Abs. 1 lit. b DSGVO

Personenbezogene Daten dürfen nur für genau festgelegte, eindeutige und legitime Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

Die Zwecke der Verarbeitung der Daten im Rahmen des TELE-KASPER-Projektes wurden bereits in der Konzeptions-Phase definiert und festgelegt. Bei Erstellung dieses Gutachtens gehen wir davon aus, dass die jeweiligen personenbezogenen Daten nur zu dem festgelegten Zweck verarbeitet werden. Vor diesem Hintergrund halten wir den Grundsatz der Zweckbindung für erfüllt.

3. Grundsatz der Datenminimierung, Art. 5 Abs. 1 lit. c DSGVO

Die Verarbeitung personenbezogener Daten muss dem Zweck angemessen und auf das für die Erreichung der Zwecke der Verarbeitung notwendige Maß beschränkt sein.

Im Rahmen des TELE-KASPER-Projektes werden personenbezogene oder anonymisierte Daten nur in dem Umfang verarbeitet, der für den definierten Zweck auch tatsächlich erforderlich ist.

Für die Authentifizierung des Nutzers und die Durchführung der Prozessevaluation werden nur die Nutzerdaten verarbeitet, die auch unbedingt benötigt werden.

Sowohl im Rahmen der Tele-Konsile und der Fallkonferenzen als auch bei der Durchführung der Punkt-Prävalenz-Erhebung und der Evaluation der Versorgungsqualität der Patienten, werden nur die Patienten- bzw. aggregierten Daten verarbeitet, die für den definierten Zweck auch unbedingt notwendig sind.

Bei der Prüfung des Sachverhalts konnten wir keine Anhaltspunkte finden, die einen Verstoß gegen das Prinzip der Datenminimierung sprechen. Nach unserer Einschätzung ist die Verarbeitung der jeweiligen Daten zur jeweiligen Zweckerfüllung notwendig.

4. Grundsatz der Richtigkeit der Datenverarbeitung, Art. 5 Abs. 1 lit. c DSGVO

Personenbezogene Daten müssen sachlich richtig sein. Darüber hinaus müssen Maßnahmen getroffen werden, damit unrichtige personenbezogene Daten unverzüglich gelöscht oder berichtigt werden. Der Grundsatz der Richtigkeit betrifft damit die Datenqualität.[2]

Patientendaten werden von den Fachärzten/behandelnden Ärzten nicht-universitärer Kliniken selbst erfasst. Dadurch wird die Wahrscheinlichkeit falsch erhobener Patientendaten auf ein Minimum reduziert. Durch deren Aufnahme in pseudonymisierter Form können bei vermeintlich fehlerhaften oder unvollständigen Angaben Rückfragen gestellt werden und die Daten, soweit erforderlich, berichtigt werden.

[2] Simitis/Hornung/Spiecker Datenschutzrecht/Roßnagel, DS-GVO Art. 5, Rn. 136.

Nutzer stellen ihre Profildaten selbst zur Verfügung, so dass hier von der Richtigkeit der verarbeiteten Daten auszugehen ist. Sofern personenbezogene Daten unrichtig sind, sind diese anschließend umgehend zu berichtigen.

5. Grundsatz der Speicherbegrenzung, Art. 5 Abs. 1 lit. d DSGVO

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie dies zur Erfüllung des Zweckes erforderlich ist. Die Speicherfrist muss auf das unbedingt erforderliche Mindestmaß beschränkt werden. Der Grundsatz der Speicherbegrenzung konkretisiert den Grundsatz der Datensparsamkeit in zeitlicher Hinsicht. [3]

Sowohl die Nutzerdaten und das Nutzerprofil als auch die Daten zur Prozessevaluation werden nur für die Dauer des Projekts gespeichert. Widerruft ein Nutzer die erteilte Einwilligung, so werden seine Daten anonymisiert und das Nutzerprofil wird anschließend gelöscht.

Die Dokumentation der pseudonymisierten Patientendaten unterliegt der Löschfrist in der Patientenakte.

Die Löschfrist der Daten aus den Punkt-Prävalenz-Erhebungen ist an die Dauer der Studie gebunden. Die erhobenen Daten werden bis zu 15 Jahre nach Beendigung oder Abbruch der Studie verschlüsselt aufbewahrt und anschließend gelöscht.

Sofern die definierten Löschfristen auch umgesetzt werden, bestehen hinsichtlich des Prinzips der Speicherbegrenzung keinerlei Bedenken.

6. Grundsatz der Integrität und Vertraulichkeit Art. 5 Abs. 1 lit. e DSGVO

Der Grundsatz der Integrität und Vertraulichkeit beschreibt zwei Ziele, denen die Gewährleistung der Datensicherheit gem. Art. 32 DSGVO dient. Integrität beschreibt in diesem Zusammenhang den Schutz der Unversehrtheit der Daten, also, dass sie nicht ganz oder teilweise gelöscht, auf andere Art vernichtet oder unbefugt verändert werden. Vertraulichkeit zielt auf den Schutz der Daten vor unbefugter Kenntnisnahme und damit vor unbefugter Verarbeitung. Auch dieser Grundsatz spielt aufgrund der pseudonymisierten Verarbeitung eine untergeordnete Rolle und ist an dieser Stelle vernachlässigbar.

Pseudonymisierte Patientendaten und das Nutzerprofil werden ausschließlich innerhalb des gesicherten Kliniknetzes des Universitätsklinikums Halle (Saale) mit betriebseigenen Geräten gespeichert. Mitarbeiter müssen sich mittels persönlicher Kennung und Passwort authentifizieren.

---

[3] BeckOK DatenschutzR/Schantz DS-GVO Art. 5 Rn. 32.

Nutzer- und Patientendaten werden in pseudonymisierter Form verarbeitet. Nur der behandelnde Arzt kann die Patientendaten einem bestimmten Patienten zuordnen.

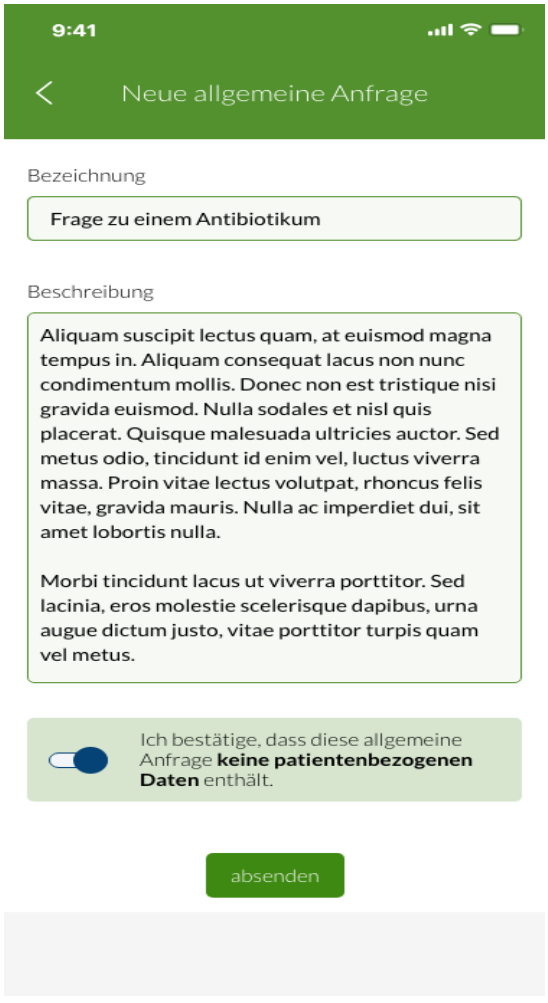
Der Zugriff auf die Informationen im TELE-Konsil ist durch ein Rechtesystem auf den erforderlichen Nutzerkreis (zuständige HUB-Mitarbeiter) beschränkt.

Die im Rahmen der Punkt-Prävalenz-Erhebung erhobenen Daten werden durch den zuständigen HUB-Koordinator nur in anonymisierter Form an das Institut für Epidemiologie, Biometrie und Informatik der Martin-Luther-Universität in Halle-Wittenberg weitergeleitet.

Technisch wird sichergestellt, dass die beiden Bereiche des Kommunikationstools der TELE-KASPER App farblich voneinander zu unterscheiden sind. Das Tele-Konsil mit pseudonymisierten Patientendaten ist mit einem blauen Balken gekennzeichnet, wogegen das Tool Tele-Info, ohne patientenbezogene Daten, über einen grünen Balken verfügt.

Um im Tool Tele-Info eine allgemeine Anfrage zu starten (Tele-Info), muss der Nutzer zudem bestätigen, dass diese allgemeine Anfrage keine patientenbezogenen Daten beinhaltet.

Screenshot hierzu:



Die getroffenen technischen und organisatorischen Maßnahmen stellen sicher, dass die Eintrittswahrscheinlichkeit eines unbefugten Zugangs zu personenbezogenen Daten zu Null tendiert. Damit wird der Grundsatz der Integrität und Vertraulichkeit gewahrt.

7. Rechenschaftspflicht, Art. 5 Abs. 2 DSGVO

Der Rechenschaftspflicht kommt eine große Bedeutung zu. So müssen Verantwortliche die Einhaltung der vorgenannten Prinzipien nachweisen können. Die Nachweispflicht des Verantwortlichen für die Einhaltung der DSGVO begründet die Darlegungs- und Beweislast des Verantwortlichen und führt damit zu einer Beweislastumkehr in dem Sinne, dass nicht der Betroffene oder die Aufsichtsbehörde eine Verletzung der DSGVO nachweisen müssen, sondern umgekehrt der Verantwortliche nachweisen muss, dass die Verarbeitung der DSGVO entspricht.[4]

Aufgrund der Rechenschaftspflicht halten wir folgende verarbeitungsspezifische, interne Dokumentationen für erforderlich:

- Dokumentation der erteilten Einwilligungen der Nutzer sowie der Eltern/Erziehungsberechtigten minderjähriger Patienten
- Führen eines Verzeichnisses der Verarbeitungstätigkeiten (Art. 30 DSGVO) in den nicht-universitären Kliniken, in den zuständigen Hubs (Universitäre Kliniken), durch das LMU Klinikum München, das Universitätsklinikum Halle und die MEKmedia GmbH als Dienstleister.
- Dokumentation der technischen und organisatorischen Maßnahmen bei der Verarbeitung von Daten im Rahmen des Projektes TELE-KASPER (Art. 32 DSGVO) (Art. 32 DSGVO)
- Aufnahme von Vereinbarungen über die gemeinsame Verantwortung gem. Art. 26 DSGVO (Joint Controller Agreement) in die Konsortial- und Kooperationsverträge
- Abschluss eines Auftragsverarbeitungsvertrages nach Art. 28 DSGVO zwischen MEKmedia und dem Uniklinikum Halle wegen der Wartung des MS SQL Datenbankservers
- Abschluss eines Auftragsverarbeitungsvertrages zwischen MEKmedia und dem LMU Klinikum München als Inhaberin der App und deren Verantwortliche im Sinne des DSGVO
- Abschluss einer Standarddatenschutzklausel durch MEKmedia mit Microsoft Corporation wegen der Nutzung der Azure-Cloud.

[4] Ehmann/Selmayr/Heberlein DS-GVO Art. 5 Rn. 30.

Hingegen halten wir die Durchführung einer Datenschutz-Folgeabschätzung nach Art. 35 DSGVO für nicht erforderlich, da in der App nur pseudonymisierte Patientendaten verarbeitet werden.

Sofern die vorgenannten Dokumentationen vollständig und aktuell sind, kann die Rechenschaftspflicht gegenüber Behörden erfüllt werden.

8. Erfüllung der Bedingungen für die Rechtmäßigkeit der Einwilligungen (Art. 7 DSGVO i. V. m. Art. 8 DSGVO)

8.1. Dokumentation der Einwilligung (Art. 7 Abs. 1 DSGVO)

Auch wenn eine Einwilligung wirksam erteilt wurde (siehe dazu Prinzip der Rechtmäßigkeit der Verarbeitung, S. 19), muss die Tatsache, dass eine Einwilligung erteilt wurde, aufgrund der Vorgabe des Art. 7 DSGVO im Zweifel (gerichtsfest) nachgewiesen werden können. Zudem ist die Verarbeitung personenbezogener Daten von Kindern, die noch nicht das sechzehnte Lebensjahr vollendet haben, nur rechtmäßig, sofern die/der Erziehungsberechtigte zustimmt (Art. 8 DSGVO).

Der Nachweis der Einwilligung ist im Rahmen des TELE-KASPER-Projekts von besonderer Bedeutung, da zum einen die Einwilligung der Eltern/der Erziehungsberechtigten eines minderjährigen Patienten und zum anderen die Einwilligung des App-Nutzers eingeholt wird.

Der Nachweis über die Einwilligung der Eltern bzw. Erziehungsberechtigten eines minderjährigen Patienten wird über die „Patienteninformation Konsile und Fallkonferenzen für Eltern und Erziehungsberechtigte“ sowie „Patienteninformation Punkt-Prävalenz-Erhebung für Eltern und Erziehungsberechtigte“ sichergestellt und dokumentiert.

Die Einwilligung der Nutzer der TELE-KASPER-App wird innerhalb der App dokumentiert.

8.2. Information der betroffenen Person über den Zweck der Verarbeitung (Art. 7 Abs. 2 DSGVO)

Um die Voraussetzungen für eine rechtmäßige Verarbeitung aufgrund der Einwilligungserklärung zu erfüllen, werden sowohl die minderjährigen Patienten als auch deren Eltern/Erziehungsberechtigte und die Nutzer der TELE-KASPER-App umfangreich über die Verarbeitung der Daten informiert. Die Information für Kinder erfolgt in einer kindgerechten Sprache.

Information der betroffenen Person, dass die Einwilligung freiwillig ist und jederzeit für die Zukunft widerrufen werden darf (Art. 7 Abs. 3 und Abs. 4 DSGVO)

Eltern/Erziehungsberechtigte und Nutzer der TELE-KASPER App werden im Rahmen der Patienteninformationen bzw. der Datenschutzerklärung zur TELE-KASPER App darüber in Kenntnis gesetzt, dass die Teilnahme an der Beratung freiwillig ist und die Einwilligung jederzeit für die Zukunft widerrufen werden kann. Zudem werden Eltern/Erziehungsberechtigte darüber informiert,

dass keine Nachteile für das jeweilige Kind entstehen, sollte die erteilte Einwilligung widerrufen werden.

Unserer Einschätzung nach werden innerhalb der TELE-KASPER App die Voraussetzungen einer rechtmäßigen Einwilligungserklärung nach Art. 7 DSGVO i. V. m. Art. 8 DSGVO erfüllt. Den betroffenen Personen wird die Kontrolle und eine echte Wahl gewährt, die angebotenen Bedingungen anzunehmen oder abzulehnen, ohne dabei Nachteile zu erleiden. Auf diesem Wege eingeholte Einwilligungen werden schriftlich oder innerhalb der TELE-KASPER App dokumentiert.

9. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Privacy by Design / Privacy by Default)

9.1. Privacy by Design

Der Grundsatz „Datenschutz durch Technikgestaltung“ (engl. „Privacy by Design“) verpflichtet das LMU Klinikum München als Verantwortliche, geeignete technische und organisatorische Maßnahmen bei der Verarbeitung der personenbezogenen Daten umzusetzen. Um unnötige Doppelungen zu vermeiden, verweisen wir an dieser Stelle auf die jeweiligen Ausführungen in diesbezüglichen Kapiteln der jeweiligen Verarbeitung.

Nach unserer Auffassung sind mit den getroffenen Maßnahmen zum Schutz der personenbezogenen Daten sämtliche, sich aus der DSGVO unmittelbar ergebenden Verpflichtungen, erfüllt.

9.2. Privacy by Default

Der Grundsatz „Datenschutz durch Voreinstellung“ (engl. „Privacy by Default“) fordert, dass durch die Voreinstellungen im technischen Verfahren nur solche personenbezogenen Daten verarbeitet werden, deren Verarbeitung für den jeweilig bestimmten Verarbeitungszweck erforderlich ist.

Die Trennung der Module TELE-Konsil und TELE-Info trägt diesem Umstand vollumfänglich Rechnung. Auch die im Bereich TELE-Info eingepflegte Abfrage, wonach der Versender nochmals Bestätigen muss, dass die Anfrage keinerlei (pseudonymisierte) Patientendaten enthält, verdeutlicht die Einhaltung dieses Grundsatzes. Im Übrigen verweisen wir auf die jeweiligen Ausführungen zur Zweckgebundenheit und Datenminimierung.

Rosemarie Popa
MKM Datenschutz GmbH
Senior Data Privacy Consultant

Fabian Dechent
MKM + PARTNER Rechtsanwälte
Rechtsanwalt

Hinweise zu diesem Gutachten

Die vorliegende, rechtliche Bewertung beruht auf den überlassenen Dokumenten und mündlich erteilten Auskünften. Alle hier getroffenen Aussagen beruhen auf diesen uns dargelegten Fakten. Sollten diese unzutreffend sein oder sich ändern, kann dies Auswirkungen auf die Bewertung des Sachverhalts haben. Diese rechtliche Bewertung trifft keine Aussage über künftige Entscheidungen von Gerichten oder Behörden in dieser Angelegenheit oder ähnlichen Sachverhalten.

Die Bewertung beruht auf dem Rechtsstand zum Zeitpunkt ihrer Erstellung. Sie stellt im Ergebnis die subjektive Interpretation der Rechtslage (Normen und Rechtsprechung) durch den Verfasser dar. Eine Anpassung nach Ablauf eines gewissen Zeitraums kann deshalb erforderlich werden. Dies erfolgt jedoch erst auf ausdrücklichen Auftrag hin und keinesfalls automatisch.

Diese Bewertung stellt ein urheberrechtlich geschütztes Werk dar. Unsere Mandanten dürfen diese Bewertung im Rahmen der geschlossenen Vereinbarung verwenden. Die ist nicht zur Weitergabe an oder zur Verwendung durch Dritte gedacht. Dritte sind nicht im Konzernverbund dem Mandanten angeschlossene Unternehmen.

MKM hält eine Vermögensschadenshaftpflichtversicherung, deren Versicherungssumme auf 10 Mio. Euro begrenzt ist. Falls im konkreten Beratungsfall eine höhere Absicherung erwünscht ist, so ist dies für den Einzelfall möglich. Der Empfänger dieses Gutachtens stellt den Ersteller von allen Ansprüchen frei, die über die von der genannten Versicherung im Schadensfall geleisteten Beträge hinausgehen. Sollte der Empfänger mit diesen Bedingungen nicht einverstanden sein, ist ihm eine Nutzung dieses Gutachtens untersagt.