Rechtliche Analyse der datenschutzrechtlichen Ausgestaltung von Gesundheits-Apps[1]

***Angelika Diarra*[2]**

Inhaltsverzeichnis

I. Ziel der Analyse

Die vorliegende rechtliche Prüfung untersucht vier verschiedene Szenarien im Hinblick auf ihre datenschutzrechtliche Ausgestaltung und mögliche Problembereiche. Dabei soll die Analyse auch mögliche datenschutzrechtliche Wege und Lösungen aufzeigen. Bei den Szenarien handelt es sich um die Anwendung von mobilen Applikationen/ Gesundheits-Apps, die teilweise als DiGA (Digitale Gesundheitsanwendung) zugelassen sind und Gesundheitsdaten von Verbraucherinnen und Verbrauchern verarbeiten. Die Szenarien wurden im Kontext des PRIMA-Projekts[3] entwickelt, um die interdisziplinären Analysen auf konkrete Anwendungsfälle zu beziehen. Anhand dieser vier Szenarien wird untersucht, inwiefern die aktuellen regulatorischen Anforderungen ausreichend sind und vorhandene Grundlagen überhaupt anzuwenden sind. Am Ende sollen typische Problembereiche mit möglichen Lösungswegen aufgezeigt werden.

---

[1] Zitiervorschlag: Diarra, Angelika (2025). Rechtliche Analyse der datenschutzrechtlichen Ausgestaltung von Gesundheits-Apps. PRIMA-Arbeitspapier. Frankfurt und Karlsruhe. Online verfügbar unter: https://prima-projekt.de/ergebnisse/

[2] Ich danke Michael Friedewald, Nils Heyen, Jana Koch, Ina Schiering, Diana Schneider und Harald Zwingelberg für ihre hilfreichen Anmerkungen und Kommentare zu früheren Versionen dieses Arbeitspapiers.

[3] https://prima-projekt.de/

II. Allgemeine Erwägungen

1. Rechtsgrundlagen

Die Rechtsgrundlagen zur datenschutzkonformen Umsetzung der Szenarien ergeben sich insbesondere aus dem allgemeinen Datenschutzrecht, der Europäischen Datenschutz-Grundverordnung (DSGVO) und dem Bundesdatenschutzgesetz sowie bereichsspezifischen datenschutzrechtlichen Vorgaben, die nachfolgend vorangestellt werden sollen, um später darauf Bezug nehmen zu können.

Jede Datenverarbeitung von personenbezogenen Daten im Sinne der DSGVO bedarf einer Rechtsgrundlage. Die Rechtsgrundlagen für die Datenverarbeitung sind in der DSGVO abschließend erfasst. Bei der Verarbeitung von Sozialdaten im Sinne des fünften Sozialgesetzbuches (SGB V) zur Regelung der gesetzlichen Krankenversicherung geht der dort geregelte bereichsspezifische Datenschutz der DSGVO vor. Bei zugelassenen DiGAs und DiPAs (Digitale Pflegeanwendung) sind die DiGAV (DiGA-Verordnung) und die DiPAV (DiPA-Verordnung) zu berücksichtigen.

In der DSGVO selbst kann neben den dort beschriebenen gesetzlichen Rechtsgrundlagen auch eine *Einwilligung* (Art. 6 Abs. 1a und Art. 9 Abs. 2a DSGVO) als Rechtsgrundlage dienen. Um die richtige Rechtsgrundlage zu ermitteln, müssen Parameter wie Art der Daten („reguläre“ personenbezogene Daten oder personenbezogene Daten besonderer Kategorien wie beispielsweise Gesundheitsdaten), Datenverarbeiter/Datenverantwortlicher, Empfänger und Art der Datenverarbeitung bekannt sein.

Art. 6 DSGVO dient als Grundlage zur Verarbeitung personenbezogener Daten. Art. 9 DSGVO hingegen ist die passende Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten besonderer Kategorien (z. B. Gesundheitsdaten). Aus juristischer Sicht muss daher immer im ersten Schritt unterschieden werden, ob „reguläre“ personenbezogene Daten (Art. 6 DSGVO) und/oder „besondere Kategorien“ personenbezogener Daten (Art. 9 DSGVO) verarbeitet werden.

Komplex wird es vor allem bei der Verarbeitung besonderer Kategorien personenbezogenen Daten (hier z. B. Gesundheitsdaten), die ausschließlich nach Art. 9 DSGVO verarbeitet werden dürfen. Nach dem Grundsatz der DSGVO für die Verarbeitung von besonderen Kategorien personenbezogener Daten dürfen diese grundsätzlich nicht verarbeitet werden, es sei denn es liegt einer der konkreten Rechtsgrundlagen aus Art. 9 DSGVO vor.

Für die vorliegenden Szenarien sind hierbei einerseits die Verarbeitung durch Ärzte (Art. 9 Abs. 2 lit. h, 3 DSGVO) und andererseits die Verarbeitung durch Dritte wie die App-Betreiber relevant. Für Ärzte gibt es eine ausdrückliche Rechtsgrundlage in Art. 9

Abs. 2 lit. h, 3 DSGVO. Dritte, wie beispielsweise die App-Betreiber, dürfen Gesundheitsdaten der Betroffenen nur dann verarbeiten, wenn eine ordnungsgemäße Einwilligung der Betroffenen (Art. 9 Abs. 2 lit. a DSGVO) vorliegt.

Aus diesem Grund ist die Einwilligung der Betroffenen und die Rechtswirksamkeit dieser Einwilligung von besonderer Bedeutung. Die Anforderungen an eine solche Einwilligung werden mithin nachfolgend zusammengefasst.

2. Anforderungen an eine Einwilligung

Für die Einwilligung kommt es darauf an, wie und mit welchem Inhalt diese eingeholt wird[4]. Bei den zu untersuchenden Szenarien werden die Daten der Betroffenen über mobile Applikationen/Apps verarbeitet, so dass insbesondere auch die Art der Einholung zu untersuchen ist.

a. Wie muss eine Einwilligung eingeholt werden?

Entscheidend bei der Einholung einer Einwilligung[5] ist die aktive Zustimmung des Betroffenen.

Der Europäische Gerichtshof (EuGH) verweist in seinem Urteil aus dem Jahr 2020 zu dieser Thematik auf Erwägungsgrund 32 der DSGVO und auch auf sein vorangegangenes Urteil aus dem Jahr 2019 zu Planet 49[6]. In den Urteilen ging es um eine Cookie-Zustimmung auf einer Website, also einer digitalen Einwilligung zur Verarbeitung von personenbezogenen Daten. Nach den Entscheidungen des EuGH wird ausdrücklich ausgeschlossen, dass bei „Stillschweigen, bereits angekreuzte[n] Kästchen oder Untätigkeit“ eine Einwilligung vorliegt. In einem solchen Fall ist es nämlich praktisch unmöglich, objektiv zu bestimmen, ob der Nutzer einer Website oder App tatsächlich seine Einwilligung in die Verarbeitung seiner personenbezogenen Daten gegeben hat, indem er die voreingestellte Markierung eines Kästchens nicht aufgehoben hat, und ob diese Einwilligung überhaupt in informierter Weise erteilt wurde.

Der Bundesgerichtshof (BGH)[7] hatte im Anschluss an das EuGH-Urteil und infolgedessen hierzu erklärt, dass es eine aktive Einwilligung des Betroffenen geben muss (*Opt-in*). Dieses Ergebnis lässt sich auch aus Erwägungsgrund 32[8] der DSGVO ableiten, der in Satz 1 eine „eindeutig bestätigende Handlung“ fordert.

---

[4] EuGH Urteil v.11.11.2020 - C-61/19
[5] Dies gilt unabhängig davon, ob es sich um personenbezogene Daten oder personenbezogene Daten besonderer Kategorien (z. B. Gesundheitsdaten) handelt.
[6] EuGH Urteil v. 01.10.2019 -C-673/17
[7] BGH, Urteil v. 28.05.2020 – I ZR 7/16
[8] https://dsgvo-gesetz.de/erwaegungsgruende/nr-32/

b. Wie kann das Opt-in umgesetzt werden?

Die aktive Einwilligung lässt sich im digitalen Kontext durch verschiedene Varianten umsetzen. Der Europäische Datenschutzausschuss (EDSA) hatte im Jahr 2020 verschiedene Beispiele aufgelistet, die eine ausdrückliche Einwilligung darstellen können[9]:

- Ausfüllen eines elektronischen Formulars,
- Senden einer E-Mail,
- Hochladen eines eingescannten, von der betroffenen Person unterzeichneten Dokuments,
- Unterzeichnen mit einer elektronischen Signatur oder
- Abgabe einer bestimmten Handlung als Bestätigung wie beispielsweise dem Drücken eines Knopfes oder einer Taste.

In der Praxis eher verbreitet ist das Anklicken einer Checkbox als aktive Form der Einwilligung. Entscheidend ist, dass der Betroffene eine Handlung durchführen muss, um die Einwilligung abzugeben. Das könnte beispielsweise auch im Rahmen einer Unterhaltung mit einem Chatbot erfolgen, solange der Betroffene Sätze hierfür eintippen muss, beispielsweise „Ja, ich willige in die Datenverarbeitung ein“ oder „Ja, ich stimme der Datenverarbeitung zu“. Die konkreten Formulierungen sind für jeden Einzelfall zu bestimmen.

c. Was bedeutet „in informierter Weise“ einwilligen?

Darüber hinaus hatte der EuGH[10] entschieden, dass Angaben zur Funktionsdauer der Cookies und dazu, ob Dritte Zugriff auf die Cookies erhalten können, zu den Informationen zählen, die der Diensteanbieter dem Nutzer einer Website vor der Abgabe einer Einwilligung mitzuteilen hat. Denn neben der Art der Einholung einer Einwilligung muss diese auch in *informierter* Weise durch den Betroffenen erfolgen. Hintergrund dessen ist die Definition der Einwilligung in Art. 4 Nr. 11 DSGVO. Danach bezeichnet der Ausdruck

> *„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;*

Das ergibt sich auch aus den Erwägungsgründen der DSGVO. Erwägungsgrund 32[11] führt zur Einwilligung auch aus, dass eine Einwilligung „für den konkreten Fall, in informierter Weise und unmissverständlich“ abgegeben werden muss. Der damit korrespondierende Erwägungsgrund 42[12] führt weiter aus: Damit die betroffene Person „in

[9] EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1., Ziff. 94.
[10] S.o.
[11] https://dsgvo-gesetz.de/erwaegungsgruende/nr-32/
[12] https://dsgvo-gesetz.de/erwaegungsgruende/nr-42/

Kenntnis der Sachlage ihre Einwilligung geben kann“, sollte sie „mindestens wissen, wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen“.

Der Betroffene muss vor und bei Abgabe seiner Einwilligung also informiert sein. Das bedeutet, ihm müssen alle notwendigen Informationen bereitgestellt werden, die eine sachliche Entscheidung zulassen. Der Betroffene muss verstehen, wofür er konkret seine Einwilligung abgibt, was mit seinen Daten passiert und welche Dritten diese Daten verarbeiten. *Nur wenn der Betroffene informiert ist, kann er eine wirksame Einwilligung abgeben* und diese zum Beispiel auch widerrufen. Damit der Betroffene als informiert gilt, erachtet die EDSA[13] folgende Informationen als mindestens notwendig an:

- Identität des Verantwortlichen
- der Zweck jedes Verarbeitungsvorgangs, für den die Einwilligung eingeholt wird,
- die (Art der) Daten, die erhoben und verwendet werden,
- das Bestehen eines Rechts, die Einwilligung zu widerrufen,
- gegebenenfalls Informationen über die Verwendung der Daten für eine automatisierte Entscheidungsfindung gemäß Art. 22 Abs. 2 lit. c DSGVO, und
- Angaben zu möglichen Risiken von Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien nach Art. 46 DSGVO

Der EuGH hat daher klargestellt, es müssten deswegen immer auch die Informationspflichten nach Art. 13 DSGVO (Name und Kontaktdaten des Verantwortlichen, Art der Datenverarbeitung, Zweck der Datenverarbeitung etc.) erfüllt sein.

Ob alleine die Informationspflichten nach Art. 13 DSGVO ausreichen, kommt letztlich darauf an, wie sie dem Betroffenen zugänglich gemacht werden. Denn die vorgenannten Mindestanforderungen an Information muss dem Betroffenen in klarer, knapper und verständlicher Form zugehen und ohne unnötige Unterbrechung des Dienstes.[14] Diese Voraussetzungen dürften beispielsweise nicht vorliegen, wenn die Informationspflichten nach Art. 13 DSGVO, wie üblich, Teil der Datenschutzerklärung sind und lediglich zu dieser verlinkt würde. Da die DSGVO jedenfalls keine konkreten Vorgaben macht, müssen bei der Bereitstellung der Informationen lediglich die vorgenannten Merkmale unter anderem erfüllt sein, die Umsetzung dabei bleibt flexibel.

Das bedeutet, der Betroffene sollte bei Einwilligung über die in Erwägungsgrund 42 genannten Informationen (mindestens Kenntnis über den Verantwortlichen und die

[13] EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1., Ziff. 64 ff.
[14] Erwägungsgrund 32, DSGVO

Verarbeitungszwecke) informiert und im Übrigen auf die ausführlicheren Informationen aus der Datenschutzerklärung hingewiesen werden (durch direkte Kenntnisnahme, z. B. einen Hyperlink).

Im Hinblick auf die Übermittlung von Daten an Dritte gilt es, nicht nur auf die eigene Übermittlung hinzuweisen. Nutzen App-Betreiber/App-Hersteller bei der Entwicklung bestimmte Frameworks (z. B. auch plattformübergreifend), sind diese auf ihre eigene DSGVO-Konformität zu prüfen. Das bedeutet, enthalten die Frameworks Anbieter, die DSGVO-widrig die Daten der Betroffenen verarbeiten und hierauf nicht oder nur mangelhaft hinweisen, dürfen diese nicht eingebunden werden.

d. Weitere Merkmale einer Einwilligung

Eine Einwilligung muss entsprechend der Definition nach Art. 4 Nr. 11 DSGVO zudem freiwillig sein, für bestimmte Zwecke abgegeben werden und unmissverständlich sein.

Außerdem muss die erforderliche *Willensbekundung* „für den konkreten Fall“ erfolgen, was so zu verstehen ist, dass sie sich gerade auf die betreffende Datenverarbeitung beziehen muss und nicht aus einer Willensbekundung mit anderem Gegenstand abgeleitet werden kann. In dem Fall des EuGH war die Einwilligung innerhalb des Vertragstextes enthalten, was der EuGH mit Verweis auf Art. 7 Abs. 2 S. 1 DSGVO ablehnte.

Nach Art. 7 Abs. 2 S. 1 DSGVO muss, wenn die Einwilligung der betroffenen Person durch eine schriftliche Erklärung erfolgt, die noch andere Sachverhalte betrifft, das Ersuchen um Zustimmung in einer solchen Form erfolgen, dass es von den anderen Sachverhalten *klar zu unterscheiden* ist.

Das ist auch für das Merkmal der Freiwilligkeit relevant, weil diese nicht anerkannt wird, wenn die Einwilligung beispielsweise Teil von AGB darstellt, nicht verhandelbar oder abwählbar ist und die Einwilligung daher nicht verweigert oder zurückgezogen werden kann.[15]

Auch für die Thematik der Transparenz der Datenschutzhinweise ist diese Umsetzung relevant.

e. Berufsgeheimnis nach § 203 StGB

Ärzte, Zahnärzte, Psychologen und andere in § 203 StGB (Strafgesetzbuch) genannte Berufsgeheimnisträger sind zur Geheimhaltung offenbarter Informationen verpflichtet. Sollen solche Informationen zum Beispiel an Dritte übermittelt werden, muss der

[15] EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1., Ziff. 13 ff.

Berufsgeheimnisträger von seiner Verschwiegenheitspflicht entbunden werden. Das Berufsgeheimnis tritt insoweit neben die datenschutzrechtlichen Anforderungen. Die Regelungen des StGB sind insoweit mit denen des Datenschutzrechts im Gleichlauf, als dass eine unter der DSGVO wirksame erteilte Einwilligung oder eine andere spezialgesetzliche Erlaubnis zugleich eine Offenbarungsbefugnis nach dem StGB darstellt. Entsprechendes gilt für das berufsrechtliche Verbot der jeweiligen Kammern, vergl. § 9 Musterberufsordnung Ärzte. Mit der DSGVO-konformen Einwilligung geht also auch ohne ausdrückliche Erwähnung eine Schweigepflichtentbindungserklärung einher.

f. Zwischenergebnis zu Anforderungen an eine Einwilligung

Zusammenfassend muss eine DSGVO-konforme Einwilligung folgende Anforderungen erfüllen:

- Aktive Zustimmung/Ausdrücklichkeit
- Freiwilligkeit
- Informiertheit
- Bestimmtheit
- Zweckgebunden
- Hinweis auf Widerrufsmöglichkeit

3. Besondere Kategorien personenbezogener Daten

Ob besondere Kategorien personenbezogener Daten vorliegen, hier z. B. Gesundheitsdaten, ist nach der Definition des Art. 9 Abs. 1 DSGVO zu bemessen. Demnach sind personenbezogene Daten solche, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, *Gesundheitsdaten* oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Der EuGH hatte in seinem Urteil vom 01.08.2022[16] hierzu festgestellt, dass diese Definition sehr weit zu verstehen ist, um dem Schutz der Betroffenen gerecht zu werden. Das bedeutet, es können auch Daten hierunter fallen, die für sich genommen keine besonderen personenbezogenen Daten sind (z. B. konkrete Angaben zum Ehepartner), wenn sich hieraus aber besondere personenbezogene Daten ableiten lassen (durch konkrete Angabe des Ehepartners z. B. die sexuelle Orientierung).

Gesundheitsdaten im Sinne der Legaldefinition des Art. 4 Nr. 15 DSGVO liegen daher auch dann vor, wenn keine direkte Aussage über die Gesundheit getroffen wird,

[16] EuGH, Urteil vom 01.08.2022 - C-184/20

sondern diese lediglich abgeleitet werden kann, wie es etwa bei Medikamentenplänen, Ernährungsplänen und Daten aus Fitness-Apps und -Trackern der Fall ist.[17]

4. Was sind Sozialdaten und inwiefern sind diese relevant?

Werden Daten außerdem von Leistungsträgern der Sozialversicherung (dazu gehört auch die gesetzliche Krankenversicherung) erhoben, verarbeitet oder die Apps in die vertragsärztliche Behandlung (ärztliche Behandlung gesetzlich versicherter Patienten) integriert, stellt sich immer die Frage, ob nicht nur besondere Kategorien personenbezogener Daten verarbeitet werden, sondern gegebenenfalls auch Sozialdaten nach dem SGB V.

Sozialdaten werden nach § 67 Abs. 2 SGB X als personenbezogene Daten, die von einer in § 35 SGB I genannten Stelle verarbeitet werden, definiert:

„Sozialdaten sind personenbezogene Daten (Artikel 4 Nummer 1 der Verordnung (EU) 2016/679), die von einer in § 35 des Ersten Buches genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden.“

Diese Stellen sind zum Beispiel die gesetzlichen Krankenkassen. Allerdings wurde dies in der Vergangenheit von Gerichten auch weitläufiger verstanden, indem auch die Datenverarbeitung von Vertragsärzten hierunter gefasst wurde[18]. Dieses Verständnis wird auch von vielen Körperschaften (z. B. Kassenärztlichen Vereinigungen) und Untergerichten noch vertreten[19]. Werden also Gesundheitsdaten von Patienten durch deren behandelnden Vertragsarzt an eine App übermittelt, könnten diese nach den Ausführungen des Bundessozialgerichts (Urteil vom 10.12.2008 – B 6 KA 37/07 R) zu Sozialdaten im Sinne des SGB V werden.

Es herrscht teilweise immer noch die Auffassung, das SGB V regele den Sozialdatenschutz abschließend und lasse nur bei ausdrücklicher Verweisung in die DSGVO deren allgemeine datenschutzrechtliche Grundlagen zu.[20] Es gibt mittlerweile allerdings auch andere Rechtsauffassungen[21], die im Sozialdatenschutz ein Mehrebenensystem sehen, mit der Folge, dass zwei Regelwerke (das SGB V und die DSGVO) beachtet werden müssen.

Die Konsequenz aus der ersten Auffassung wäre, dass diese Sozialdaten (weil der Sozialdatenschutz im SGB V, jedenfalls nach dieser Auffassung, abschließend

[17] Petri in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Aufl. 2024, Art. 4 Nr. 15. DSGVO Rn. 4 f; Weichert in Kühling/Buchner, Art. 4 Nn. 15 DS-GVO Rn. 3.
[18] BSG, Urteil vom 10.12.2008 - B 6 KA 37/07 R
[19] Schifferdecker in Kasseler Kommentar Sozialversicherungsrecht, Stand März 2022, § 35 SGB I Rn. 43
[20] BSG, Urteil vom 10.12.2008 - B 6 KA 37/07 R
[21] https://www.datenschutz-bayern.de/datenschutzreform2018/SGB.pdf Rdnr. 8

geregelt wird (§ 35 Abs. 2 SGB I)), nur im Rahmen des SGB V verarbeitet werden dürfen. Das würde eine Verarbeitung von Sozialdaten durch Dritte (hier z. B. die App-Betreiber), die nicht nach dem SGB V legitimiert sind, ausschließen oder jedenfalls als problematisch erscheinen lassen.

Konkret würde das bedeuten, dass die Datenverarbeitung von Sozialdaten eine spezifische Rechtsgrundlage im Sozialrecht benötigt. Die Einwilligung nach Art. 9 Abs. 2a DSGVO würde demnach nicht ausreichen. Lässt sich keine Rechtsgrundlage im Sozialgesetzbuch finden, dann wäre die Datenverarbeitung nicht möglich.

Für eine zugelassene DiGA ist die Zulässigkeit einer Einwilligung nach Art. 9 Abs. 2a DSGVO ausdrücklich in § 4 DiGAV geregelt, weshalb die Datenverarbeitung für den DiGA-Betreiber auf Grundlage einer Einwilligung ohne Weiteres möglich wäre.

Eine nicht als DiGA zugelassene App, hier z. B. eine Gesundheits-App, die Sozialdaten verarbeitet, könnte nach der oben benannten Auffassung Sozialdaten nicht auf Grundlage einer Art. 9 Abs. 2a DSGVO Einwilligung verarbeiten, wenn es hierfür nicht eine ausdrückliche Rechtsgrundlage gibt (wie beispielsweise § 4 Abs. 2 DiGAV).

Es ist allerdings bislang noch nicht abschließend geklärt, ob die Verarbeitung durch Dritte – als Teil einer vertragsärztlichen Behandlung – dazu führt, dass die Patientendaten überhaupt als Sozialdaten im Sinne des SGB V gelten und die DSGVO als Rechtsgrundlage einer Verarbeitung ausscheidet. Hierzu sind verschiedene sozialrechtliche Verfahren anhängig. Die Einordnung der Art der Daten ist entsprechend relevant.

5. Datenverantwortlicher

Es muss weiterhin geklärt werden, wie der Datenfluss aussieht und wer tatsächlich verantwortlich ist für die Verarbeitung der Daten, wenn die App Teil einer vertragsärztlichen Behandlung ist und hier auch in Betracht käme, dass der App-Betreiber als Auftragsverarbeiter nach Art. 28 DSGVO für einen Vertragsarzt tätig würde.

Ob die Daten vom App-Betreiber nun als Auftragsverarbeiter oder als Verantwortlicher verarbeitet werden, ist auch für dessen Compliance-Pflichten relevant. Der EuGH[22] hatte festgestellt, dass eine Einwilligung jedenfalls eine Rechtsgrundlage für die Weitergabe der Daten an Dritte (Einwilligungskette) sein kann. Die Verantwortlichen haben aber erweitere Compliance-Pflichten wie zum Beispiel die Information der Verantwortlichen in der Kette über einen eingegangenen Widerruf des Betroffenen.

[22] EuGH, Urteil vom 27.10.2022 - C- 129/21

Sind diese Aspekte geklärt, lassen sich die daraus resultierenden rechtlichen Anforderungen (zum Beispiel, wer welche Informationspflichten gemäß der DSGVO umzusetzen hat) ermitteln.

III. Szenarien

1. Doku4Me

a. Funktion/Beschreibung[23]

Mit der Doku4Me-App können Angehörige von pflegebedürftigen Menschen, die in einer Wohneinrichtung leben, auf die aktuellen Vitalwerte und den Medikationsplan der zu pflegenden Menschen zugreifen. Zudem ermöglicht die App einen Austausch von pflegerischen Informationen zwischen den Angehörigen und den Pflegekräften der Einrichtung. Darüber hinaus bietet die App die Möglichkeit, Informationen über stattfindende Events und Aktivitäten in der Einrichtung zu erhalten. So sind Angehörige jederzeit darüber informiert, welche betreuerischen Leistungen angeboten werden. Ergänzend ermöglicht die App die Einsicht in die Tagesstruktur der betreuten Person und schafft damit zusätzliche Transparenz und Nachvollziehbarkeit im Alltag des pflegebedürftigen Menschen.

Die Doku4Me-App hat jedoch nicht nur für Angehörige einen Nutzen, sondern auch für die Pflegebedürftigen. In der App befindet sich ein Link zu Unterhaltungsmedien und es ist eine tägliche Einschätzung der eigenen gesundheitlichen und mentalen Verfassung möglich. Darunter fällt sowohl ein Schmerzprotokoll als auch ein Fragebogen zur Zufriedenheit. Daneben ist es möglich, das Ernährungs- und Trinkprotokoll der Fachkraft einzusehen. Eine Orderfunktion erlaubt es, den Angehörigen Getränke, Snacks oder einige Drogerieartikel über die Pflegekräfte zu bestellen. Die Orderfunktion ermöglicht auch die Bestellung von Dienstleistungen, z. B. eines Friseurbesuchs.

b. Use Case aus datenschutzrechtlicher Sicht

Die Doku4Me-App wird von pflegebedürftigen Menschen in Wohneinrichtungen (z. B. Pflegeheim, betreutes Wohnen) und deren Angehörigen gemeinsam genutzt. Die Angehörigen haben so laufend Zugriff auf die Daten (insbesondere auch Gesundheitsdaten) und können sich mit dem Pflegepersonal austauschen.

Die datenschutzrechtliche Besonderheit liegt vor allem darin, dass viele Personen Zugriff auf die personenbezogenen Daten des Betroffenen haben sollen:

[23] PRIMA 2024, Szenario Doku4Me, projektinternes Arbeitsdokument.

- Personal der Wohneinrichtung/Pflegeheim
- Angehörige
- Betroffene
- (gesetzliche) Betreuer/Bevollmächtigte

Da die Verarbeitung der personenbezogenen Daten des Betroffenen auch in diesem Fall auf Grundlage einer Einwilligung nach Art. 9 i.V.m. 6 (1) DSGVO erfolgt, entstehen im Hinblick auf den Zugriff dieser Daten durch Dritte einige Herausforderungen.

c. Rechtliche Herausforderungen/Problembereiche

Aus datenschutzrechtlicher Sicht bestehen bei Nutzung einer solchen App folgende Herausforderungen in der Umsetzung, die es zu berücksichtigen gilt:

aa. Der App-Betreiber wird in der Regel der Datenverantwortliche im Sinne der DSGVO sein. Ihm obliegen daher alle Pflichten als Verantwortlicher im Sinne von Art. 28 DSGVO, insbesondere die Sicherstellung einer Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten sowie besonderer Kategorien personenbezogener Daten. Der App-Betreiber muss entsprechend der oben dargelegten Ausführungen eine ordnungsgemäße Einwilligung (Art. 9 DSGVO) des Betroffenen einholen.

bb. Die App muss über ein Opt-in Verfahren die Einwilligung des Betroffenen in die Verarbeitung der Daten einholen und dabei auch alle Informationen zur Verfügung stellen, die eine freiwillige und informierte Einwilligung möglich machen (Art. 4 Nr. 11 i.V.m. Art. 7 DSGVO).

cc. Die Einwilligung muss auch die Information umfassen, welche Daten dem Pflegepersonal oder den Angehörigen zugänglich gemacht werden sollen.

(1) Das bedeutet, der Betroffene muss festlegen können, **wer** (aus der Wohneinrichtung, von den Angehörigen, usw.) Zugriff auf seine Daten hat und **welche** Daten aus der App zugänglich gemacht werden sollen. Der Detailgrad dieser Umsetzung muss im Weiteren festgelegt werden. Diese (wie auch im Übrigen alle anderen) Einstellungen des Betroffenen müssen elektronisch dokumentiert werden, um der Nachweispflicht gemäß Art. 5 Abs. 2 DSGVO nachzukommen.

(2) Die App sollte es möglich machen, die verschiedenen Empfänger der Daten (Pflegepersonal oder Angehörige) zu unterscheiden und unterschiedliche Berechtigungen festzulegen. Gerade bei Pflege-Apps sollte es auch die Möglichkeit geben, einen Betreuer/Bevollmächtigten der Betroffenen als Zugangsberechtigten in der App zu registrieren, damit die Nutzung durch die

einzelnen Empfänger dokumentationsfähig ist. Nach § 20 Betreuungsorganisationsgesetz (BtOG) dürfen Betreuer Gesundheitsdaten nur zur Erfüllung ihrer Aufgaben verarbeiten (diese ergeben sich aus der Betreuungsverfügung).

dd. Die gesamte Grundlage zur Verarbeitung der personenbezogenen Daten, hier insbesondere Gesundheitsdaten, durch die App basiert also auf der Einwilligung des Betroffenen (Art. 9 Abs. 2a i.V.m. Art 6 Abs. 1. lit. a DSGVO). Das bedeutet datenschutzrechtlich auch, dass der Zugriff Dritter (Pflegepersonal, Angehörige, Betreuer) von dieser Einwilligung abgedeckt sein muss.

Die Einwilligung könnte beispielsweise Kategorien von Empfängern nennen, was nach aktuellem Stand ausreichend sein kann und damit die Nennung von Namen der Mitarbeiter obsolet machen würde. Jedenfalls gibt Art. 13 Abs. 1e DSGVO vor, dass über Empfänger oder Kategorien von Empfängern informiert werden muss, und scheint dem Datenverantwortlichen durch die Nutzung des Begriffs „oder“ anheim zu stellen, ob er die Empfänger konkret benennt oder lediglich Kategorien benennt.[24]

ee. Unabhängig von den Informationen im Rahmen der Einwilligung sollte die App die verschiedenen Empfänger im Rahmen eines Rechtemanagements abbilden können. In der App muss es daher auch die Möglichkeit geben, den Zugriff auf die Daten des Betroffenen für konkrete Personen oder Personengruppen zu beschränken. Das Personal der Einrichtung besteht aus Pflegepersonal, Verwaltung und sonstigen Mitarbeitern. Nicht alle Mitarbeiter benötigen Zugriff auf die Daten der Betroffenen. Konkret besteht für die Umsetzung des Zwecks der App nur die Notwendigkeit bei dem Pflegepersonal.

Es wäre daher auch empfehlenswert, wenn die App Nutzerrollen enthält, die zugeteilt werden können mit abgestuften Freigaben. Korrelierend dazu, sollte die nutzende Einrichtung hierfür ein internes Berechtigungskonzept erstellt haben, indem dies geregelt wird. Das gilt vor allem für den Sachverhalt, dass Mitarbeiter die Einrichtung verlassen. Die App sollte aus diesem Grund auch die Möglichkeit haben, sich mit dem zentralen Verzeichnisdienst der Einrichtung (über eine API) koppeln zu können, um unbefugten Mitarbeitern über die Einrichtung automatisiert den Zugriff zu sperren.

Die datenschutzrechtliche Kernfrage ist daher, wie bei diesem Use Case das Rechtemanagement in der App ausgestaltet wird.

[24] Artikel 29-Gruppe, Leitlinien für Transparenz gemäß der Verordnung 2016/679

ff. In der App findet auch ein Informationsaustausch zwischen Pflegepersonal und Angehörigen statt. Pflegepersonal kann der Verschwiegenheitspflicht nach § 203 StGB unterliegen (z. B. so bei Ergotherapeuten (ErgThG), Hebammen und Entbindungspfleger (HebG), Krankenschwestern, Krankenpflegern, Kinderkrankenschwestern (KrPflG), medizinisch-technischen Assistenten (MTAG), Logopäden (LogopG), Masseuren, Physiotherapeuten (MPhG), Rettungsassistenten bzw. Notfallsanitätern (NotSanG), psychologischen Psychotherapeuten, Kinder- und Jugendlichenpsychotherapeuten (PsychThG[25]) und auch Altenpflegern (§ 1 AltPflG; dazu BGH[Z] VersR 13, 648, Hamm[Z] NJW 07, 850, Lips/Schönberger NJW 07, 1568)[26]. Da eine datenschutzrechtliche Einwilligung auch konkludent eine Schweigepflichtentbindungserklärung enthalten kann, sind diese Personengruppen als Empfängerkategorie im Rahmen der Einwilligung zu erwähnen.

gg. Universalentbindungserklärungen können zwar zulässig sein[27], müssen aber in regelmäßigen Abständen aktualisiert werden, da sie andernfalls ihre Zulässigkeit verlieren. In einer Einwilligung in die Empfängerkategorien kann eine solche Universalentbindungserklärung gesehen werden. Das hat zur Folge, dass die App über die Funktion verfügen sollte, die Einwilligung in regelmäßigen Abständen, beispielsweise einmal im Jahr, zu aktualisieren. Ohne Aktualisierung sollte die App dann den Zugang verweigern.

hh. Der Betroffene muss die Einwilligungen und Zugangsberechtigungen auch jederzeit widerrufen können, vgl. Art. 7 Abs. 3 DSGVO. Das muss so einfach wie möglich sein, am besten über den gleichen Weg wie die Einwilligung auch erteilt wurde. Wird der Betroffene in der Zwischenzeit einwilligungsunfähig und kann einen Widerruf nicht mehr ausüben (z. B. wegen Demenz), sollte die App über eine Funktion verfügen, die aufgrund dessen die Sperrung des Accounts für alle Personen durch einen Betreuer oder Bevollmächtigten ermöglicht. Hierbei wäre auch ein einfacher Verifikationsprozess des Betreuers oder des Bevollmächtigten empfehlenswert.

2. HelloBetter Diabetes

a. Funktion/Beschreibung[28]

HelloBetter Diabetes ist eine zugelassene Digitale Gesundheitsanwendung (DiGA). Im Kern der DiGA steht ein psychologischer Online-Therapiekurs mit sieben Trainingseinheiten von jeweils ca. 60 Minuten Länge bei Diabetes und depressiven

[25] § 203 StGB, Rdnr. 63: Eisele in Schönke/Schröder Strafgesetzbuch, 30. Auflage 2019
[26] § 203 StGB: Eisele in Schönke/Schröder Strafgesetzbuch, 30. Auflage 2019
[27] Bundesverfassungsgericht, Beschluss vom 17.07.2013 – 1 BvR 3167/08
[28] PRIMA 2024, Szenario HelloBetter, projektinternes Arbeitsdokument.

Beschwerden. Die Nutzung erfolgt über einen Internet-Browser, wobei Fortschritte zwischengespeichert werden können, so dass die Einheiten jederzeit unterbrochen und zu einem späteren Zeitpunkt fortgesetzt werden können. Die Trainingseinheiten bestehen aus Texten, Video- und Audiodateien sowie aus praktischen Übungen. Jeder Nutzer bekommt einen Coach für eine individuelle psychologische Begleitung zugewiesen. Der Coach gibt nach jeder Einheit ein individuelles, schriftliches Feedback, die als Nachrichten angezeigt werden. Darüber hinaus kann der Nutzer über eine Chat-Funktion in einen direkten schriftlichen Austausch mit dem Coach treten, auch telefonische Gespräche sind möglich. Der Nutzer ist aufgefordert, ein persönliches Stimmungstagebuch zu führen, in dem er auf einer 10-stufigen Skala einträgt, wie seine Stimmung und sein Stressempfinden am jeweiligen Tag waren. So können er und sein Coach sehen, wie sich die Werte zum Beispiel im Wochenverlauf entwickeln. Der Coach kann auch hierzu per Nachrichten-Funktion eine Rückmeldung geben. Außerdem kann der Nutzer die DiGA nutzen, um Symptome festzuhalten, positiv besetzte Aktivitäten im Alltag zu planen und sich an diese per E-Mail erinnern zu lassen.

b. Use Case aus datenschutzrechtlicher Sicht

HelloBetter ist eine zugelassene DiGA, die eine psychologische Behandlung via App anbietet. Die App kann zunächst genutzt werden, ohne dass ein Austausch mit Dritten stattfindet. Die App verarbeitet die personenbezogenen Daten, die ohne Einwilligung oder die entsprechende Funktion nicht mit Dritten, wie z. B. behandelnde Ärzte, geteilt werden.

c. Rechtliche Herausforderungen/Problembereiche

Für Digitale Gesundheitsanwendungen gilt die DiGA-Verordnung (DIGAV)[29], die auch den Datenschutz und die Datensicherheit für DiGAs regelt (§ 4 DiGAV). Es wird auf die DSGVO sowie auf das SGB V verwiesen. Verarbeitungszwecke werden hier abschließend geregelt[30]. Die DiGA muss seit 2024 und seit dem 01.01.2025 auch Zertifikate von akkreditierten Stellen gegenüber dem Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) nachweisen, aus denen die Einhaltung der Anforderungen zum Datenschutz und zur Datensicherheit hervorgehen, vgl. § 139e Abs. 10 und 11 SGB V. Damit muss die DiGA grundsätzlich hohe datenschutzrechtliche Anforderungen erfüllen, die auch überprüft werden (hier durch das BfArM), im Gegensatz zu Gesundheits-Apps, die Betroffene unabhängig von einer Kostenerstattung durch ihre Krankenkasse nutzen.

[29] https://www.gesetze-im-internet.de/digav/BJNR076800020.html
[30] Jukić/Rahn, GesR 2020, 749-756

Bei dieser DiGA findet in erster Linie eine Verarbeitung personenbezogener Daten durch die DiGA selbst statt. Dritte, wie behandelnde Ärzte, sind zunächst nicht eingebunden. Damit ergeben sich folgende datenschutzrechtliche Herausforderungen:

aa. Die Datenverarbeitung durch die DiGA muss auf einer verständlichen und vollständigen datenschutzrechtlichen Einwilligung nach Art. 9 Abs. 2a, 6 Abs. 1 lit. a DSGVO beruhen, mit einfacher Widerrufsmöglichkeit und dem Hinweis, dass im Widerrufsfalle die App dann nicht mehr nutzbar wäre.

bb. Die App muss gemäß § 4 Abs. 7 DiGAV und § 139e Abs. 10 SGB V die TR 03161[31] des Bundesamtes für Sicherheit in der Informationstechnik (BSI) beachten. Diese technische Richtlinie (TR), herausgegeben vom BSI, richtet sich speziell an Hersteller von mobilen Anwendungen im Gesundheitswesen und soll als Leitfaden für die Unterstützung zur Herstellung sicherer mobiler Applikationen im Gesundheitswesen dienen. Nach § 4 Abs. 7 DiGAV und § 139e Abs. 10 SGB V wird diese Richtlinie für DiGA-Hersteller verpflichtend.

   Somit ist der DiGA-Hersteller verpflichtet, ein Zertifikat zu beantragen, mit dem die Anforderungen an die Datensicherheit nachgewiesen werden. Die Datensicherheit wird gemäß dem BfArM durch Umsetzung der TR 06161 des BSI eingehalten und anschließend durch das Zertifikat nachgewiesen[32].

cc. Für die DiGA bedeutet das im Vergleich zu Gesundheits-Apps, die nicht verpflichtet sind, die TR des BSI umzusetzen, hohe Datenschutzanforderungen. So muss die DiGA insbesondere folgende Maßnahmen umsetzen:
   - Jeder Nutzer muss sich über ein 2-Faktor-System authentifizieren.
   - Es muss ein Rollenkonzept zur Authentifizierung geben.
   - Notwendig ist eine ständige Authentifizierung nach Unterbrechung.

3. Barmer eCare

a. Funktion/Beschreibung[33]

Die eCare-App ist die App für die elektronische Patientenakte (ePA) der Barmer Krankenkasse. Zentrale Funktion der App ist die digitale Zusammenstellung von persönlichen Gesundheitsdaten und medizinischen Behandlungs-Dokumenten wie z. B. ärztliche Befunde, Diagnosen oder Arztbriefe. Alle Dokumente und Daten sind stets verschlüsselt abgelegt und können nur von berechtigten Personen entschlüsselt

[31] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03161/tr-03161.html
[32] https://www.bfarm.de/DE/Medizinprodukte/Aufgaben/DiGA-und-DiPA/Datensicherheitskriterien/_artikel.html
[33] PRIMA 2024, Szenario Barmer eCare, projektinternes Arbeitsdokument.

werden. Nutzende können die eCare-App mit den ihnen bereits vorliegenden Daten und Dokumenten befüllen und diese jederzeit lesen, anderweitig verwenden oder auch löschen. Leistungserbringer wie Ärztinnen und Ärzte oder Krankenhäuser können die vorliegenden oder während der Behandlung neu entstehenden Dokumente in die App hochladen. Auch die Daten aus Gesundheits-Apps, die ärztlich verschrieben werden (DiGAs), können auf Wunsch in die App eingespeist werden. Für jedes Dokument können Nutzende bestimmen, wer darauf zugreifen kann: alle Leistungserbringer und/oder ausgewählte Ärzte und/oder bestimmte Personen aus dem persönlichen Umfeld. Außerdem können sie für ausgewählte Leistungserbringer allgemeine Zugriffsrechte vergeben. Die Barmer Krankenkasse selbst kann in keinem Fall Informationen in der Akte einsehen. Schließlich können Nutzende ausgewählte Daten für Forschungszwecke freigeben.

b. Use Case aus datenschutzrechtlicher Sicht

Bei der eCare-App handelt es sich um eine Krankenkassen-App für die ePA. Die Versicherten nutzen sie zunächst im Rahmen des Selbstmanagements und können, wenn sie möchten, die selbst eingespeisten Daten auch mit Leistungserbringern teilen. Die Besonderheit ist hier, dass die App zwar von der Krankenkasse bereitgestellt und betrieben wird, die Krankenkasse selbst auf diese Daten aber nicht zugreifen darf.

Die regulatorischen Anforderungen für die eCare-App ergeben sich aus dem SGB V und der DSGVO. So muss die App z. B. folgende datenschutzrechtliche Vorgaben erfüllen:

- Einwilligung nach Art. 9 DSGVO
- Widerspruchsmöglichkeit nach § 342 Abs. 2 s SGB V
- Besondere Regelungen zu Zugriffsrechten und Einwilligung nach § 342 Abs. 2 SGB V

Insgesamt weichen die datenschutzrechtlichen Regelungen für die ePA von denen einer regulären Gesundheits-App durch die besonderen Regelungen im SGB V deutlich ab.

c. Rechtliche Herausforderungen/Problembereiche

Ähnlich wie bei dem Use Case Doku4Me stellen sich hier datenschutzrechtliche Herausforderungen im Bereich der Zugriffsmöglichkeit durch Dritte (Leistungserbringer oder andere bestimmte Personen wie z. B. Vertreter, Betreuer, Angehörige). Das heißt, die App sollte es möglich machen, die verschiedenen Empfänger der Daten (Leistungserbringer oder Angehörige) zu unterscheiden und unterschiedliche Berechtigungen festzulegen. Außerdem bestehen nachfolgende rechtliche Herausforderungen:

aa. Die App muss alle Anforderungen an die ePA nach §§ 341 ff. SGB V erfüllen (z. B. Information an die Versicherten über alle relevanten Informationen durch die Krankenkasse, Widerspruchsmöglichkeit der Versicherten, Name des Anbieters der ePA usw.)

bb. Die Daten aus der ePA sollen über das Forschungsdatenzentrum (FDZ) Gesundheit[34] im Rahmen einer Sekundärnutzung anonymisiert bzw. pseudonymisiert verarbeitet werden (für Forschungszwecke). Problematisch ist das bei bestimmten Konstellationen: Wenn in einem sehr eng gefassten Kontext (bspw. bei einer Und-Verknüpfung zweier seltener Krankheitsbilder oder eines seltenen Krankheitsbildes mit einer regionalen Zuordnung des Patienten) eine zu kleine Grundgesamtheit entsteht, kann die vorher erfolgte Entfernung der Klardaten des Betroffenen durch die geringe Größe der Grundgesamtheit faktisch – wenn auch unbeabsichtigt – unterlaufen werden, was den Schutz der Patientendaten gefährdet.

cc. Nach § 341 Abs. 4 SGB V sind die Krankenkassen, die die Apps zur Nutzung der ePA zur Verfügung stellen, datenschutzrechtlich verantwortlich.

4. Emendia MS

a. Funktion/Beschreibung[35]

Emendia MS ist eine (am Markt nicht mehr erhältliche) App zur umfassenden Therapieunterstützung bei Multipler Sklerose (MS): Sie ermöglicht einen weitreichenden Überblick zum Verlauf der individuellen MS-Symptomatik. Mit der App kann der Nutzer zum Beispiel Krankheitsschübe, eigenes Befinden sowie Werte zu medizinischen Abfragen, die üblicherweise in einer ärztlichen Praxis durchgeführt werden, wie z. B. prEDSS (patient reported Expanded Disability Status Scale) oder MFIS (Modified Fatigue Impact Scale) dokumentieren. Zusätzlich kann mit der App die Medikation dokumentiert werden. Der Nutzer kann die App selbstständig zum Tracking der eigenen Symptome nutzen und gleichzeitig die Daten mit dem behandelnden Arzt teilen. Indem der Nutzer seine persönliche Emendia-ID dem Behandlungsteam mitteilt, erhält dieses Zugriff auf das Portal von Emendia.

b. Use Case aus datenschutzrechtlicher Sicht

Bei diesem Use Case geht es insbesondere um die App-Nutzung und Dokumentation eines gesundheitlichen Verlaufes durch den Patienten selbst und das Teilen dieser Informationen mit dem behandelnden Arzt. Die Besonderheit bei solchen Apps liegt

[34] https://www.forschungsdatenzentrum-gesundheit.de/
[35] PRIMA 2024, Szenario Emendia, projektinternes Arbeitsdokument.

neben den regulären datenschutzrechtlichen Anforderungen in dem „Teilen“ mit dem behandelnden Arzt oder ggf. auch weiteren an der Behandlung beteiligten Leistungserbringern. Das Ziel dieser Apps kann neben dem eigenen „Gesundheitstagebuch“ auch ein Mehrwert für die ärztliche Behandlung sein, indem der behandelnde Arzt die Daten aus der App nutzt und im Rahmen seiner Behandlung berücksichtigt.

c. Rechtliche Herausforderungen/Problembereiche

Bei der Emendia-App können datenschutzrechtliche Herausforderungen in einem Zugriff durch Dritte (z. B. die Arztpraxis) liegen:

aa. Der App-Betreiber wird in der Regel der Datenverantwortliche im Sinne der DSGVO sein. Ihm obliegen daher alle Pflichten als Verantwortlicher im Sinne von Art. 28 DSGVO, insbesondere die Sicherstellung einer Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten sowie besonderer Kategorien personenbezogener Daten. Der App-Betreiber muss entsprechend der oben dargelegten Ausführungen eine ordnungsgemäße Einwilligung (Art. 9 DSGVO) des Betroffenen einholen.

bb. Die App muss über ein Opt-in Verfahren die Einwilligung des Betroffenen in die Verarbeitung der Daten einholen und dabei auch alle Informationen zur Verfügung stellen, die eine freiwillige und informierte Einwilligung möglich machen (Art. 4 Nr. 11 i.V.m. Art. 7 DSGVO).

cc. Wenn die App die Funktion besitzt, Daten mit einem behandelnden Arzt zu teilen, muss sich die Einwilligung der Datenverarbeitung auch auf die Übermittlung an den Arzt erstrecken. Das kann für jeden Einzelfall der Übermittlung erfolgen oder vorab bei Registrierung.

dd. Je nachdem, wie die Übermittlung der Information durch die App technisch umgesetzt wurde, ist es empfehlenswert, ein Authentifizierungsverfahren für den behandelnden Arzt zu integrieren. Die App sollte zudem Sicherheitsvorkehrungen aufweisen, durch die regelmäßige Authentifizierungsverfahren der Ärzte notwendig werden, damit z. B. bei Praxisverkauf der Zugriff Unbefugter eingeschränkt wird.

ee. Ein weiteres Problemfeld ist der rechtliche Umgang mit Sozialdaten im Sinne des SGB V, der durch Sozialgerichte sehr restriktiv ausgelegt wird. Das betrifft ausschließlich die Nutzung der App durch einen gesetzlich versicherten Patienten. Nutzt der behandelnde Vertragsarzt die Gesundheitsdaten aus der App für seine ärztliche Behandlung und integriert er die Daten aus der App in seine Behandlungsakte, dann können aus diesen Daten Sozialdaten im Sinne des SGB V werden. Fraglich wird in diesem Moment die Rechtsgrundlage, auf

der die App diese Daten dann verarbeitet (s.o.). Eine Möglichkeit wäre die Verarbeitung als Auftragsverarbeiter des Vertragsarztes.

ff. Dadurch wird auch ersichtlich, dass alle verarbeitenden Stellen dargelegt und bestimmt werden müssen. Kann es z. B. eine gemeinsame Verantwortung zwischen App und behandelndem Arzt geben, vgl. Art. 26 DSGVO, wenn der Arzt in der App die Möglichkeit erhält, die vom Patienten übermittelten/ freigegebenen Daten auf eine bestimmte Weise darstellen zu lassen[36]? Oder kann die App in manchen Bereichen im Auftrag des Arztes tätig werden, vgl. Art. 28 DSGVO? Daraus resultiert immer die Frage, auf welcher Rechtsgrundlage werden von den jeweiligen Verarbeitenden die Daten des Patienten verarbeitet.

IV. Fazit

Im Ergebnis hat sich bei der Untersuchung der vier Szenarien gezeigt, dass insbesondere die Umsetzung einer datenschutzkonformen Einwilligung für jedes Szenario relevant sein wird. Das betrifft die Art der Einwilligung, die Dokumentation der Einwilligung, die Inhalte der Einwilligung und die Darstellung der Einwilligung.

Neben diesem Themenbereich ist nahezu bei allen Szenarien auch die Übermittlung von personenbezogenen Daten an Dritte bzw. der Zugriff der Dritten auf diese aus datenschutzrechtlicher Sicht einzuordnen und durch die Betroffenen-Einwilligung und Zugriffsberechtigungskonzepte umzusetzen.

Ein weiterer relevanter Themenbereich ist die DSGVO-konforme Verarbeitung von Sozialdaten im Sinne des SGB V in allen Szenarien, in denen Betroffene ihre Daten mit ihrem behandelnden Vertragsarzt teilen und dieser die entsprechenden Informationen im Rahmen seiner Behandlung verarbeitet. Hier gibt es bislang keine richtungsweisende Entscheidung eines obersten Gerichtes (Bundessozialgericht, Bundesgerichtshof, Bundesverfassungsgericht).

[36] EuGH Urteil v. 05.06.2018 – C 210/16 „Facebook Fanpage“