Hammer, Samuel

Article

Eine datenschutzrechtliche Betrachtung der neuen elektronischen Patientenakten in Deutschland nach Einführung der DSGVO

Junior Management Science (JUMS)

Provided in Cooperation with:
Junior Management Science e. V.

Suggested Citation: Hammer, Samuel (2022) : Eine datenschutzrechtliche Betrachtung der neuen elektronischen Patientenakten in Deutschland nach Einführung der DSGVO, Junior Management Science (JUMS), ISSN 2942-1861, Junior Management Science e. V., Planegg, Vol. 7, Iss. 5, pp. 1301-1325,
https://doi.org/10.5282/jums/v7i5pp1301-1325

This Version is available at:
https://hdl.handle.net/10419/295018

Junior Management Science 7(5) (2022) 1301-1325

Junior Management Science

journal homepage: www.jums.academy

A Data Protection Law Analysis of the New German Electronic Patient Records (ePA) in the Light of the GDPR

Eine datenschutzrechtliche Betrachtung der neuen elektronischen Patientenakten in Deutschland nach Einführung der DSGVO

Samuel Hammer

FOM Hochschule für Oekonomie und Management

Abstract

A lengthy discussion about the digitization and modernization of the German healthcare system is followed by the obligation for health insurance companies to introduce electronic patient records (ePA). This regulation faces resistance from Germany's highest data protection authority (BfDI). On the basis of relevant commentary literature and considering the arguments put forward by the stakeholders this study examines, whether the criticism of the authority is justified and whether a violation of the GDPR could lie in the implementation of the ePA. As a result of the study, no such violation can be determined. Especially the conditions for the effectiveness of consent to data processing are given. The introduction of the German ePA will take place in two stages, with the second stage including improvements regarding data protection. Thus, the result of the work can also be applied ‚a maiore ad minus' to the second stage which is planned for 2022. It remains unclear whether the data protection authority (BfDI) will take further legal measures. This study affects also other research topics, such as the "right to data processing" or the role of German data protection authorities in legislative processes.

Zusammenfassung

Einer langwierigen Diskussion um die Digitalisierung und Modernisierung des deutschen Gesundheitssystems folgt 2021 die Verpflichtung der gesetzlichen Krankenkassen zur Einführung der elektronischen Patientenakte (ePA). Diese Regelung stößt bei Deutschlands oberster Datenschutzbehörde (BfDI) auf Widerstand. Anhand einschlägiger Kommentarliteratur und unter Berücksichtigung der durch die Interessenvertreter vorgebrachten Argumente untersucht diese Arbeit, ob die Kritik der Behörde begründet ist und ob ein Verstoß gegen die DSGVO mit der Einführung der ePA vorliegen könnte. Im Ergebnis lässt sich ein solcher Verstoß nicht feststellen. Insbesondere liegen die grundsätzlichen Anforderungen an die Wirksamkeit einer Einwilligung in die Datenverarbeitung vor. Die Einführung der ePA erfolgt in zwei Ausbaustufen, wobei die zweite Stufe datenschutzrechtlich relevante Verbesserungen beinhaltet. Daher gilt das Ergebnis der Arbeit „a maiore ad minus" auch für die 2022 geplante zweite Ausbaustufe. Offen bleibt, ob die Datenschutzbehörde (BfDI) weitere rechtliche Maßnahmen ergreifen wird. Die Untersuchung berührt weitere Forschungsthemen, wie beispielsweise das „Recht auf Datenverarbeitung" oder die Rolle der Datenschutzbehörden in Gesetzgebungsverfahren.

Keywords: Elektronische Patientenakte; ePA; DSGVO; Datenschutz; Telematikinfrastruktur.

1. Einleitung

1.1. Problemstellung, Erkenntnisinteresse und Forschungsfrage

Unter dem Begriff der Telematikinfrastruktur (TI) werden verschiedene Projekte und Reformen in Gesundheitswe-

Ich bedanke mich bei Herrn Professor Dr. Marcus Helfrich für die mir eingeräumte Freiheit bei der Themenwahl, sowie für die unkomplizierte Kommunikation und die konstruktive Kritik während der Betreuung dieser Arbeit.

DOI: https://doi.org/10.5282/jums/v7i5pp1301-1325

sen und -wirtschaft vornehmlich zur Digitalisierung der Prozesse und Daten zusammengefasst. Die TI soll das deutsche Gesundheitswesen vernetzen und einen sicheren Austausch von Gesundheitsdaten ermöglichen.[1] Mit über 70 Millionen Versicherten[2], etwa 100 Krankenkassen[3] und 180.000 Vertragsärzten und Psychotherapeuten[4] ist die Vernetzung des deutschen Gesundheitswesens eines der größten Digitalisierungsvorhaben in Europa. Auf die Vernetzung des Gesundheitswesens durch die Telematikinfrastruktur baut die elektronische Patientenakte (ePA) auf, welche die Krankenkassen ihren Versicherten nach geltender Sozialgesetzgebung seit dem 1. Januar 2021 anbieten müssen, § 342 Abs. 1 SGB V.[5] Die ePA soll die Digitalisierung und Vereinfachung der bisher in Papierform ablaufenden Arbeitsschritte ermöglichen. Medizinische Informationen lassen sich besser sammeln und strukturieren.[6] Davon sollen Ärzte, Apotheker, Therapeuten, anderes medizinisches Fachpersonal und vor allem der Patient selbst profitieren.

Die hohe Aktualität des Themas wird deutlich durch die Tatsache, dass das seit Jahren geplante Konzept der Telematikinfrastruktur mit dem darauf aufbauenden Element der elektronischen Patientenakte immer noch nicht umgesetzt ist und dabei ständig neue Hindernisse, wie beispielsweise Fragen zum Datenschutz oder der Informationssicherheit, auftreten.[7] Bei den Beteiligten, insbesondere bei den Leistungserbringern und den Versicherten, ist eine Unsicherheit hinsichtlich der Datenverarbeitung und deren Auswirkungen auf die datenschutzrechtliche Behandlung vorhanden.[8] Eine nachhaltige Verbesserung der Prozesse kann im Gesundheitssystem hingegen nur eintreten, wenn die – für die Versicherten freiwilligen, für die Leistungserbringer und Kassen verpflichtenden – Maßnahmen von allen Beteiligten akzeptiert werden.[9] Einen wichtigen Beitrag dafür leisten Klarheit, Transparenz und Rechtssicherheit in datenschutzrechtlichen Fragestellungen.

Mit Einführung der Datenschutzgrundverordnung (DSGVO)[10] sind möglicherweise neue datenschutzrechtliche Anforderungen an die ePA hinzugekommen, die sich auch auf ihre prozessuale oder technische Ausgestaltung auswirken könnten. Die Unklarheiten hinsichtlich der Berücksichtigung von europäischen Datenschutzvorschriften führten zu erheblicher Kritik, die den Gesetzgeber auf den Plan rief. Mit einer weiteren Novelle des SGB V, dem „Patientendatenschutzgesetz (PDSG)“, will der Gesetzgeber Abhilfe schaffen.[11]

Beispielsweise ist unklar, ob es die Möglichkeit einer differenzierten Einwilligung geben muss, i.e. die Möglichkeit zu entscheiden, welche Beteiligten am Gesundheitssystem auf welche Daten zugreifen dürfen.[12] Nach derzeitiger Lage hätte ein Physiotherapeut Zugriff auf Daten, die eigentlich nur für einen Urologen bestimmt und relevant sind. Weiterhin soll durch das PDSG festgelegt werden, wer in der Telematikinfrastruktur, respektive im Rahmen der elektronischen Patientenakte für die verschiedenen Komponenten Verantwortlicher im Sinne von Artikel 4 Nr. 7 DSGVO sein wird.[13] Ferner wurde der Umgang mit Daten bezüglich Erbkrankheiten oder anderen genetischen Informationen kritisiert. Hier sind bei der Datenverarbeitung möglicherweise nicht nur die tatsächlich Erkrankten betroffen, sondern auch nahe Verwandte. Diese müssten möglicherweise auch über die Verarbeitung der Daten informiert werden. Die Bundesregierung sieht in diesem Fall eine Ausnahme von der Informationspflicht, die in dieser Arbeit zu prüfen wäre. Veraltete Sicherheitsstandards und nicht regelkonforme Authentifizierungsverfahren stehen ebenfalls in der Kritik.[14]

Auf die zuvor genannten Aspekte wird die vorliegende Arbeit eingehen, wobei das Hauptaugenmerk auf der datenschutzrechtlichen Beurteilung der Verarbeitungsvorgänge im Rahmen der elektronischen Patientenakte nach europäischem Recht liegen wird. Insbesondere die durch den Bundesbeauftragen für Datenschutz und Informationsfreiheit vorgebrachten Bedenken, welche in einer Warnung nach Art. 58 Abs. 2 lit. a DSGVO an die Krankenkassen kulminierten, sollen näher betrachtet werden.[15] Es soll festgestellt werden, *ob diesen Bedenken Rechnung zu tragen ist oder ob die Regelungen zur elektronische Patientenakte in ihrer derzeitigen Ausgestaltung mit der DSGVO vereinbar sind.*

1.2. Forschungsstand

Nach einigen Rückschlägen wurden die Bemühungen zur Schaffung einer Telematikinfrastruktur mit der elektronischen Patientenakte unter der Regie des Bundesgesundheitsministers Jens Spahn wieder deutlich vorangetrieben.[16] Mit der Verabschiedung des „Digitale-Versorgung-Gesetz“[17] erfolgte Ende 2019 eine Novelle des SGB V, mit der die Strukturen des Gesundheitssystems der Dynamik der digitalen Transformation und der Geschwindigkeit von Innovationsprozessen angepasst werden sollten.[18] Unter anderem

[1] Vgl. Koch & Henke, 2016, S. 309.
[2] Vgl. Bundesministerium für Gesundheit (BMG), 2021, o. S.
[3] Vgl. GKV-Spitzenverband, Gesetzliche Krankenkassen, 2021, o. S.
[4] Vgl. Kassenärztliche Bundesvereinigung (KBV), 2020, S.3.
[5] Zum Verhältnis der Telematikinfrastruktur und elektronischer Patientenakte s. unten 2.2.7.
[6] Vgl. Gematik, 2021b, o. S.
[7] Den rechtlichen Ausgangspunkt setzte das „E-Health-Gesetz“ von 2015, Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen sowie zur änderung weiterer Gesetze vom 21.12.2015, BGBl. I S. 2408.
[8] Vgl. für die Versicherten Klöckner & Olk, 2021; für die ärzteschaft Bundesärztekammer, 2020a, S. 4.
[9] Vgl. auch Bundesärztekammer, Stellungnahme der Bundesärztekammer zum PDSG, 2020, S. 4.
[10] Verordnung 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016, ABl. L 119 vom 4. Mai 2016, S. 1-88.
[11] Vgl. Bundesministerium für Gesundheit, Gesetzesentwurf PDSG, 2020, S.2.
[12] Vgl. BT-Drs. 19/16228, S. 3.
[13] Vgl. a.a.O., S. 4.
[14] Vgl. a.a.O., S. 9 f.
[15] Vgl. BfDI, 2020,?.
[16] Dazu kritisch netzpolitik.org, Jens Spahn hat es eilig, netzpolitik.org (2020), o. S.
[17] Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation vom 9. Dezember 2019, BGBl. I S. 2562.
[18] Vgl. Jorzig und Sarangi (2020, S. 41).

sollten durch dieses Gesetz mehr Leistungserbringer an die Telematikinfrastruktur angeschlossen werden.[19] Mit dem „Terminservice- und Versorgungsgesetz“[20] wurden die Krankenkassen dazu verpflichtet, den Versicherten eine ePA ab spätestens 1. Januar 2021 zur Verfügung zu stellen. Mit diesen Novellen wurde versäumt, den mittlerweile durch die DSGVO geänderten Anforderungen an den Datenschutz ausreichend Rechnung zu tragen, so dass es nötig geworden war, ein weiteres Gesetz auf den Weg zu bringen: das bereits erwähnte „Patientendatenschutzgesetz“.[21] Diese Entwicklungen sind zum Zeitpunkt der Anfertigung dieser Arbeit sehr aktuell. Dementsprechend fällt der Bestand an Literatur zur konkreten Problemstellung relativ gering aus. In einem vom *health innovation hub*[22] beauftragten Gutachten wird detailliert auf die Bedenken des BfDI eingegangen.[23] Der Verfasser der vorliegenden Arbeit versucht auf die vorgebrachten Gegenargumente einzugehen, eigene Überlegungen anzustellen und eine eigene Bewertung vorzunehmen.

1.3. Forschungsmethode

Die vorliegende Arbeit wurde auf Basis einer Literaturrecherche angefertigt.[24] Zu Beginn wurde der Suchraum auf europäisches Datenschutzrecht eingegrenzt, das den Bereich des deutschen Gesundheitswesens, der die elektronischen Patientenakte beinhaltet, betreffen könnte. Der Schwerpunkt der Arbeit liegt in der Ausarbeitung der Vereinbarkeit der elektronischen Patientenakte betreffenden Regelungen, insbesondere solche des SGB V, mit der Datenschutz-Grundverordnung. Vor der Beantwortung der Forschungsfrage waren Grundlagen der elektronischen Patientenakte und der Telematikinfrastruktur zu klären, um den Rahmen der Prüfung europäischen Datenschutzrechts zu identifizieren.

Während der Ausformulierung der zuvor genannten Grundlagen, wurden parallel dazu iterative Recherchezyklen zu den Kernthemen durchgeführt, die dann zum Teil wieder neue Recherchefelder eröffneten.[25]

Die Literatursuche wurde teilweise in öffentlichen juristischen Bibliotheken mittels Bibliothekssuchmaschine und Suchmaschinen im Internet durchgeführt. Die Nutzung der öffentlichen Bibliotheken war durch die Pandemie-Situation 2020/2021 jedoch stark eingeschränkt. Daher wurde diese Arbeit überwiegend anhand im Internet elektronisch verfügbarer Dokumente angefertigt, wobei die Recherche-Plattform Beck-Online und öffentlich verfügbare Stellungnahmen der Beteiligten zur PDSG-Gesetzgebung eine zentrale Rolle einnahmen.

In die Literaturauswahl wurden neben Sachbeiträgen aus Fachzeitschriften und Kommentarliteratur zu den Vorschriften, aktuelle Gesetzgebung, Gesetzesänderungen und Spezifikationen der Gesellschaft für Telematik (gematik) mit einbezogen. Die Auswahl der Literatur erfolgte anhand der Relevanz entsprechender Literatur für das Kernthema und ihrer Aktualität.

1.4. Aufbau der Arbeit

Die Kapitel 2.1 – 2.3 bilden die theoretische Grundlage dieser Arbeit. Hier soll dargelegt werden, in welchem Umfeld die datenschutzrechtliche Betrachtung einzuordnen ist. Kapitel 2.4 behandelt die allgemeinen Voraussetzungen für die Anwendung der DSGVO. Kapitel 2.5 liefert einen Überblick über datenschutzrechtliche Kritikpunkte, die im öffentlichen Diskurs auszumachen sind. Die Kapitel 2.6 – 2.10 beschäftigen sich detailliert mit dem Spannungsverhältnis zwischen DSGVO und nationaler Sozialgesetzgebung, wobei der Schwerpunkt der Arbeit auf der Prüfung der Einwilligung nach Art. 6 Abs. 1 Satz 1 lit. a bzw. Art. 9 Abs. 2 lit. a DSGVO liegt (Kapitel 2.7.1).

2. Hauptteil

2.1. Begriff der elektronischen Patientenakte

In der Vergangenheit gab es bereits schon einzelne Vorstöße, um die digitale Kommunikation zwischen Patienten, Leistungsträger und Krankenkassen zu verbessern. Beispielsweise veröffentlichte die Techniker Krankenkasse bereits 2018 eine Anwendung mit dem Namen „TK-Safe“.[26] Allianz und DAK brachten kurze Zeit später die Anwendung „Vivy“ auf den Markt, die unter anderem Versicherten der DAK, IKK Classic, Bahn-BKK ermöglichte, Dokumente elektronisch zu speichern.[27] Solche Anwendungen werden *elektronische Gesundheitsakte* genannt.[28] Die bis dahin veröffentlichten Anwendungen haben gemein, dass sie keine umfassende Vernetzung zwischen den Akteuren im Gesundheitswesen anbieten konnten.[29] Dafür fehlten einheitliche Standards, die dann später mit dem Terminservice- und Versorgungsgesetz herbeigeführt werden sollten. Es sollte eine *elektronische Patientenakte* entwickelt werden, die die Krankenkassen ihren Versicherten zur Verfügung stellen können.[30] Die Komponenten für die ePA müssen durch gematik als zentrale Stelle geprüft und zugelassen werden. Nach derzeitigem Stand gibt es 103 Anbieter eines ePA-Aktensystems, drei Hersteller von ePA-Aktensystemen und 13 verschiedene Produkte für das Frontend, die bei der gematik zugelassen sind.[31] Daher gibt

[19] Vgl. ebd.

[20] Gesetz für schnellere Termine und bessere Versorgung vom 6. Mai 2019, BGBl. I S. 646.

[21] Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur vom 14. Oktober, BGBl. 2115.

[22] Das health innovation hub ist eine Einrichtung des Bundesgesundheitsministeriums, vgl. https://hih-2025.de/about/.

[23] Vgl. Böllhoff, Cornelius, et al. (2020).

[24] S. dazu. vom v. Brocke, Jan, Simons, Alexander, et. al. (2009).

[25] Vgl. zur Organisation der Literatursichtung und überprüfung, a.a.O., S. 9.

[26] aerztezeitung (2018, o. S).

[27] aerztezeitung.de (2018, o. S).

[28] Vgl. Wortlaut der §§68 und 351 SGB V.

[29] Es fehlt im Wesentlichen die Anbindung an die TI. Vgl. dazu unten 2.2.7.

[30] §§291a Abs. 5c Satz 4, 291b Abs. 1a Satz 1 SGB V in der vom 11.05.2019 geltenden Fassung.

[31] Gematik (2021c, o. S).

es nicht die *eine* elektronische Patientenakte, sondern verschiedene Produkte, die sich gleichwohl an denselben Standards messen lassen müssen.[32]

2.2. Aufbau und Funktionsweise der elektronischen Patientenakten

Das deutsche Gesundheitswesen setzt sich im Wesentlichen aus drei Arten von Akteuren zusammen: den Leistungsempfängern, den Leistungserbringern und den Leistungsträgern.[33] An diesem Grundgerüst muss sich auch die Architektur der ePA orientieren. Um Aufbau und Funktionsweise der elektronischen Patientenakten zu verstehen, ist es erforderlich, die Beteiligten, deren Interessen und systembedingte Komponenten zu identifizieren. Die Rolle der zuletzt genannten Beteiligten und von den Beteiligten abgeleitete Anforderungen, sowie weitere für die ePA wichtige Elemente werden im Folgenden behandelt.

2.2.1. Leistungserbringer

Zu den Leistungserbringern im Sinne des Sozialgesetzbuches, §§ 69 ff SGB V, zählen unter anderem Vertragsärzte, Vertragszahnärzte, Apotheken, Vertragspsychotherapeuten, Krankenhäuser, Erbringer von Heil- und Hilfsmittelleistungen, wie beispielsweise Physiotherapeuten, Sprechtherapeuten oder Ergotherapeuten.

Die Ärzteschaft unterstützt das grundsätzliche Vorhaben der Digitalisierung des Gesundheitswesens, sieht aber die Gefahr einer Abwälzung von Aufgaben auf die Leistungsträger, die nur unmittelbar mit der medizinischen Versorgung des Patienten verbunden seien, wie beispielsweise datenschutzrechtliche Auskunfts- oder Beratungspflichten gegenüber den Versicherten.[34]

Die ePA ist so konzipiert, dass die Leistungserbringer entsprechend ihrer Rollen mit unterschiedlichen Verarbeitungsberechtigungen auf die Patientendaten zugreifen können.[35]

2.2.2. Leistungsempfänger

Leistungsempfänger sind die Empfänger der Gesundheitsleistungen, also Patienten der Ärzte in Krankenhäusern und Arztpraxen, Therapeuten oder anderen Leistungserbringern. Von der elektronischen Patientenakte im Sinne der Sozialgesetzgebung können zunächst nur Versicherte der gesetzlichen Krankenkassen profitieren.[36]

Ein wesentliches Interesse der Leistungsempfänger dürfte eine optimale Behandlung durch die Leistungserbringer sein. Einen wichtigen Beitrag dazu leisten ein schneller Informationsaustausch und die sinnvolle Zusammenarbeit der Leistungserbringer, damit jede notwendige Expertise schnell und effizient an den richtigen Adressaten gelangt.[37] Auch eine bessere Übersicht über Dokumente und Daten und deren Strukturierung „an einem Ort“ stellen ein bedeutsames Interesse der Leistungsempfänger dar. Jedoch dürfen diese Vorteile nicht zu Lasten anderer Rechtsgüter gehen, wie beispielsweise das Recht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts, aus dem letztlich der Datenschutz erwächst.[38] Eine Auswahl an Kritikpunkten der Datenschützer werden in dieser Arbeit umrissen.[39] Auf die Bedenken des Bundesbeauftragten für Datenschutz und Informationsfreiheit wird detailliert eingegangen.[40]

Normen außerhalb der DSGVO, die auf den Schutz informationeller Selbstbestimmung abzielen, wie beispielsweise die Prüfung einer zulässigen Offenbarung gemäß § 203 StGB, werden im Rahmen dieser Arbeit nur behandelt, sofern dies im Rahmen der DSGVO nötig ist.[41]

2.2.3. gematik

Die gematik GmbH wurde von den Spitzenorganisationen des deutschen Gesundheitswesens nach gesetzlichem Auftrag gegründet, um den Aufbau der Telematikinfrastruktur als Basis für eine digitale und sichere Vernetzung im Gesundheitswesen voranzutreiben.[42] Die Geschäftsanteile sind in § 310 Abs. 2 SGB V geregelt. Aufgrund eingeschränkter Funktionsfähigkeit des Gremiums durch Patt- und Blockadesituationen, wurden Anfang 2019 die Mehrheitsverhältnisse und die Voraussetzungen für die Beschlussfähigkeit durch das Terminservice- und Versorgungsgesetz geändert.[43] Mithin hat die Bundesrepublik Deutschland mittlerweile mit 51% die Kontrolle über das Organ. Die Gesellschafter können gemäß § 310 Abs. 3 SGB V den Beitritt weiterer Spitzenorganisationen auf Bundesebene und des Verbandes der Privaten Krankenversicherung auf deren Wunsch beschließen. Die Geschäftsanteile sind innerhalb der Gruppen und Kostenträger entsprechend anzupassen. Demnach sind der Spitzenverband Bund der Krankenkassen (GKV) mit 22,05%, der Verband der Privaten Krankenversicherung (PKV) mit 2,45% und die übrigen in § 306 Abs. 1 Satz 1 SGB V genannten Organisationen der Leistungserbringer[44] mit insgesamt 24,5% beteiligt (Abbildung 1). Die gematik ist für die Einführung, Pflege, Weiterentwicklung der Telematikinfrastruktur und für datenschutzrechtlich relevante Festlegungen in Abstimmung mit dem Bundesamt für Sicherheit in der Informa-

[32] Im Verlauf der Arbeit wird der Einfachheit halber dennoch der Singular verwendet.

[33] Vgl. Jäschke und Hacks (2016, S. 7).

[34] Vgl. Bundesärztekammer (2020b, S. 1 und 7).

[35] Vgl. unten Abbildung 8.

[36] Zur Rolle der privaten Krankenkassen s. unten 2.3.

[37] Vgl. Stöferle (2016), Kooperations- und Kommunikationspartner aus Anwendersicht, S. 135.

[38] Vgl. BVerfGE 65, 1, Volkszählung.

[39] S. unten 2.5.

[40] S. unten 2.6 f.

[41] Vgl. ausführlich dazu Stöferle, Kooperations- und Kommunikationspartner aus Anwendersicht, S. 141.

[42] Vgl. Gesellschaft für Telematik (gematik) (2021e, o. S).

[43] Vgl. Bundesministerium für Gesundheit (BMG) (2019, o. S).

[44] Dies sind im Einzelnen: Die Kassenärztliche Bundesvereinigung (7,35%), die Kassenzahnärztliche Bundesvereinigung (2,45%), die Bundesärztekammer (2,45%), die Bundeszahnärztekammer (2,45%), die Deutsche Krankenhausgesellschaft (5,88%) sowie der Deutsche Apothekenverband (3,92%).

tionstechnik und mit der oder dem Bundesbeauftragten für den Datenschutz durch gesetzlichen Auftrag verantwortlich, § 311 SGB V. Die gematik ist weiterhin für die Zulassung der für die ePA benötigten Komponenten (§§ 341 Abs. 3, 325 SGB V) und für die Zulassung der von den Betreibern entwickelten Anwendungen und Services (§§ 311 Abs. 1 Nr. 4 und Nr. 5, 324, 325 SGB V) zuständig.

2.2.4. Hersteller ePA-Aktensysteme

Die Betreiber sind die Beteiligten, die einen wesentlichen Teil der Infrastruktur und des Backends für den Betrieb der digitalen Services bereitstellen. Die gematik bezeichnet diese Betreiber als Hersteller für „ePA-Aktensysteme“.[45] Der Markt wird unter drei Unternehmen oder Unternehmenskonsortien aufgeteilt: *IBM* wird Services für die ePA im Backend für die Techniker Krankenkasse, die Barmer, die Knappschaft, die Hanseatische Krankenkasse und Viactiv BKK anbieten. Der zweite Anbieter ist ein Zusammenschluss des Unternehmens *Bitmarck* und dem österreichischen Unternehmen *Research Industrial Systems Engineering (RISE)*.[46] Die Unternehmensverbindung wird die Services für 87 Krankenkassen unterschiedlicher Größe, darunter Betriebskrankenkassen (BKK), DAK und IKK, anbieten.[47] Das Unternehmen *x-tention Informationstechnologie GmbH* wird zusammen mit internationalen Partnern die Services für die Allgemeinen Ortskrankenkassen (AOKen) bereitstellen.[48] Die Aktensysteme sind die Serverseite der Fachanwendung ePA und besteht aus folgenden Komponenten (Abbildung 2)[49]:

- „Authentisierung von Nutzern“: Wird von anderen Komponenten verwendet, um die Authentifizierung von Versicherten und deren berechtigten Vertretern zu erstellen.
- Zugangsgateway des ePA-Aktensystems: Ermöglicht den Zugang des Versicherten auf das jeweilige Aktensystem über das Internet und dient dem Netzabschluss in Richtung Internet.
- Autorisierung und Schlüsselverwaltung: Stellt für den authentifizierten Nutzer eines Aktenkontos bei gegebener Autorisierung das jeweilige Schlüsselmaterial bereit.
- Dokumentenverwaltung: Dient dem sicheren Speichern und Auffinden von Dokumenten des Versicherten in seiner Akte. Diese Funktion können Versicherte selbst oder von ihm benannte Vertreter, Leistungserbringer und Kostenträger nutzen.

[45] Vgl. Gesellschaft für Telematik (gematik) (2021a, o. S).
[46] Vgl. aerzteblatt.de Elektronische Patientenakte (2020, o. S).
[47] Vgl. ebd.
[48] Vgl. ebd.
[49] Vgl. Gematik (2021a, o. S).

2.2.5. Leistungsträger als Anbieter der ePA

Die im Kontext der elektronischen Patientenakten relevanten Leistungsträger sind die gesetzlichen Krankenkassen, § 12 i.V.m. § 18 ff. SGB I. Die Krankenkassen sind die Kunden der oben beschriebenen Betreiber. Für Vertrieb und Teile der Frontendgestaltung der Smartphone Apps sind die Krankenkassen verantwortlich.[50] Die Anbieter der ePA sind damit in der Regel die gesetzlichen Krankenkassen.[51] Die Gestaltungsmöglichkeiten des Designs (customizing) hängen vom Angebot der Betreiber ab. Das Frontend kann beispielsweise mit unterschiedlichen Farben, Logos und Verweisen auf die Webseiten der jeweiligen Krankenkasse gestaltet werden.[52] Auch der Produktname wird von den Krankenkassen bestimmt. So wird die App bei der Barmer „eCare“, bei der Techniker Krankenkasse „TK-Safe“ und bei der AOK „Mein Leben“ heißen.[53]

Der GKV-Spitzenverband unterstützt die Einführung und Weiterentwicklung der ePA, sieht aber eine Hürde in der vom BfDI geforderten Information des Versicherten über die im ersten Jahr fehlende Möglichkeit einer selektiven Rechtevergabe auf Dokumentenbasis vor jeder Speicherung eines Dokuments.[54] Unnötig sei auch das Festhalten einer Sanktionierung der Krankenkassen, wenn keine ePA angeboten werde.[55] Ablehnend steht der Spitzenverband auch der Neuaufnahme einer öffnenden Regelung zur Bereitstellung der ePA durch andere Anbieter als Krankenkassen gegenüber.[56] Dies führe zu erheblichen Rechtsunsicherheiten bei allen Beteiligten. Der GKV-Spitzenverband lehnte auch die Einrichtung einer Ombudsstelle bei der gematik für Betroffene im Sinne datenschutzrechtlicher Normen ab[57] und steht der Einrichtung von sogenannten Terminals kritisch gegenüber.[58]

2.2.6. ePA Frontend des Versicherten (ePA-FdV)

Das ePA Frontend des Versicherten bezeichnet die Client-Software auf einem mobilen Endgerät des Versicherten, mit dem dieser auf die ePA zugreifen kann (Abbildung 3).[59] Die Frontends wurden für bestimmte Krankenkassengruppen von verschiedene Herstellern entwickelt.[60] Beispielsweise wurde die „AOK Mein Leben“ App von Ernst & Young entwickelt. Andere Frontends wurden von IBM, RISE, der Hanseatischen Krankenkasse und der Techniker Krankenkasse entwickelt.

2.2.7. ePA als Fachanwendung in der Telematikinfrastruktur

Die Telematikinfrastruktur (TI) ist die bevorzugte Informations-, Kommunikations- und Sicherheitsinfrastruktur des deutschen Gesundheitswesens mit allen technischen

[50] Vgl. aerzteblatt.de Elektronische Patientenakte (2020, o. S).
[51] Vgl. Gematik (2021c, o. S.): „Anbieter-ePA-Aktensystem“; nichtamtliche überschrift des §342 Abs. 1 SGB V.
[52] Vgl. ebd.
[53] Vgl. aerzteblatt.de Elektronische Patientenakte (2020, o. S).
[54] Vgl. GKV-Spitzenverband (2020b, S. 7); siehe dazu unten 2.7.1.3.
[55] Vgl. GKV-Spitzenverband (2020b, S. 7).
[56] Vgl. ebd.
[57] Vgl. a.a.O., S. 9.; §307 Abs. 5 Satz 2 und 3 SGB V.
[58] S. dazu unten 2.5.4.
[59] Gesellschaft für Telematik (gematik) (2021b, o. S).
[60] Vgl. Gematik (2021c, o. S).

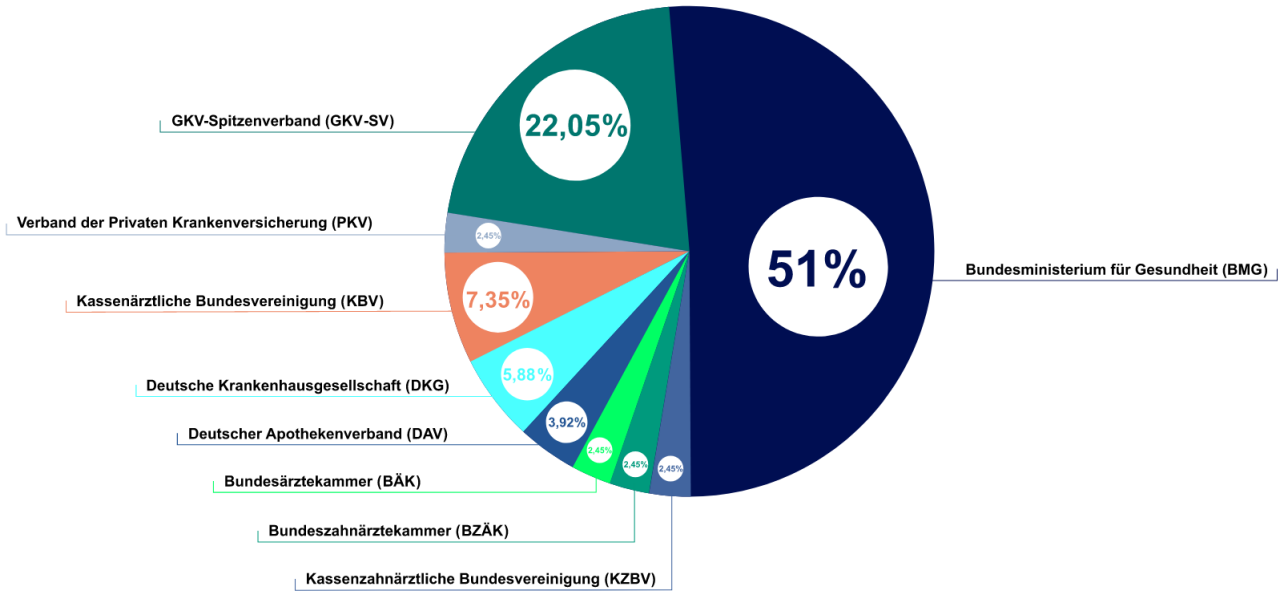

Abbildung 1: Gesellschafteranteile der gematik

Quelle: *gematik*, Gesellschafteranteile, 2021

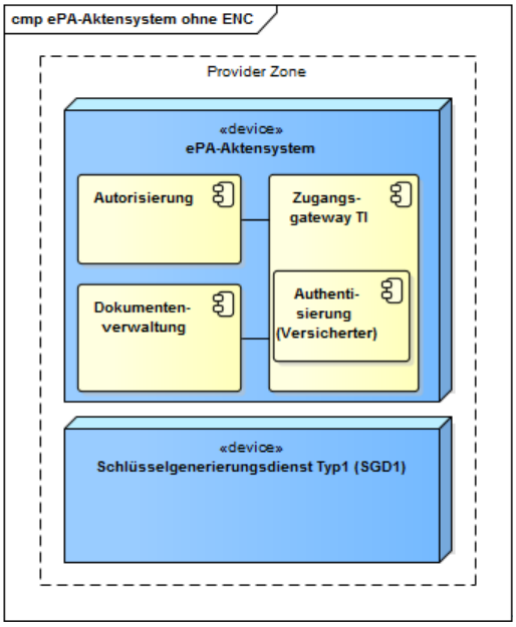

Abbildung 2: High Level Diagramm – ePA Aktensystem

Quelle: Gesellschaft für Telematik (gematik) (2021g, S.9).

und organisatorischen Anteilen.[61] Die TI unterstützt die Anwendungen der Versicherten gemäß § 306 Abs. 1 SGB V. Die ePA ist eine Fachanwendung der Telematikinfrastruktur gem. § 306 Abs. 1, § 327 SGB V und nutzt Teile der Telematikinfrastruktur, wie beispielsweise die Verbindung zu den „Konnektoren“ der Leistungserbringer oder den „KTR-Consumern“, die den Kostenträgern den Zugang zur TI ermöglichen (unten Abbildung 5).[62]

Die obligatorischen Anforderungen an die Fachanwendung ePA ergeben sich aus § 341 Abs. 2 i.V.m. § 342 Abs. 2 SGB V. Enthalten sind unter anderem die „Einstellung“ von

[61] Vgl. Gesellschaft für Telematik (gematik) (2021i, o. S).

[62] Vgl. Gesellschaft für Telematik (gematik) (2021f, o. S).

Medikationsplänen, Notfalldaten, Daten zu Befunden, Diagnosen, Therapiemaßnahmen, und Daten der Impfdokumentation.

2.2.8. Angebot nicht vorgeschriebener Services

Das ePA-FdV kann über die gesetzlichen Vorschriften hinaus zusätzliche Funktionalitäten enthalten. Diese werden dann allerdings nicht der Fachanwendung ePA zugeordnet und unterliegen somit nicht der Regelungshoheit der gematik (Abbildung 4).[63] Die Techniker Krankenkasse bietet beispielsweise ein persönliches Arztverzeichnis, Impf- und Vorsorgeempfehlungen, Übersicht zur Arbeitsunfähigkeit und Informationen über Arztbesuche und Krankenhausaufenthalte an.[64] Die Barmer will Gesundheitsinformationen, Prävention und saisonale Ratschläge anbieten.[65] Einige Krankenkassen möchten sogenannte Gesundheitshistorien, die auf Abrechnungsdaten basieren, bereitstellen.[66] Diese Zusatzfunktionen müssen für den Nutzer von den Funktionalitäten der Fachanwendung ePA jedoch unterschieden werden können.[67] Weiterhin muss das Design des Frontends sicherstellen, dass der Nutzer dem Verarbeiten der ePA-Daten in zusätzlichen Funktionalitäten bezüglich Umfang, Art und Dauer der Verarbeitung vor dem Zugriff der Zusatzfunktionen auf die ePA-Daten zustimmen muss und diese Zustimmung wiederrufbar ist.[68] Darüber hinaus enthalten die Spezifikationen des ePA-FdV weitere Pflichten, die die *Sicherheit* betreffen. Die Zusatzfunktionen werden vom Produktgutachter in seinem Produktgutachten hinsichtlich ihrer Sicherheit mitberücksichtigt.[69] Der Begriff Sicherheit meint im Rahmen der Produkt- und Sicherheitsgutachten die Informationssicherheit, die den „Datenschutz“ implizit mit einschließt.[70] Nach Ansicht des Verfassers wird der Datenschutz zwar nicht durch die Informationssicherheit impliziert,[71] sofern aber im Ergebnis den datenschutzrechtlichen Vorgaben entsprochen wird, ist diese Diskussion hinfällig.

2.2.9. Übersicht der technischen Komponenten der ePA

Schließlich ergibt sich ein komplexes Bild des Geflechts zwischen den Beteiligten unter Einbeziehung der verschiedenen technischen Komponenten (Abbildung 5).

2.3. Ausbauphase der ePA

Die Krankenkassen sind aus § 342 Abs. 1 SGB V verpflichtet, spätestens ab dem 1. Januar 2021 jedem Versicherten eine ePA mit den dort in Abs. 2 genannten Anforderungen zur Verfügung zu stellen. Mit der Bereitstellung zum 1. Januar 2021 begann eine „Testphase“, die für die Dauer des ersten Quartals des Jahres geplant war und in der die Anbindung einiger ausgewählter Leistungserbringer erprobt werden sollte.[72] Im zweiten Quartal soll nach erfolgreicher Testphase mit dem Rollout der Konnektoren begonnen werden, um eine flächendeckende Anbindung der Leistungserbringer bis zum Ende des Jahres fertigzustellen (Abbildung 6). Die Leistungserbringer sind dementsprechend aus § 341 Abs. 6 SGB V dazu verpflichtet, bis zum 30. Juni 2021 nachzuweisen, dass sie über die für den Zugriff auf die ePA erforderlichen Komponenten und Dienste verfügen. Aus Sicht des Verfassers ist es zumindest fragwürdig, dass eine Anwendung für über 70 Millionen Versicherte zur Verfügung gestellt wird, deren Anbindung an dezentrale Komponenten sich noch in der Testphase befindet.

Bis 2022 sind weitere Funktionalitäten in der ePA obligatorisch aufzunehmen, § 342 Abs. 2 Nr. 2 SGB V. Hinzukommen wird unter anderem ein feingranulares Rechtemanagement und das E-Rezept.[73] 2023 wird die ePA mit weiteren Modulen aufgerüstet, wie beispielsweise Daten pflegerischer Versorgung oder der Arbeitsunfähigkeitsbescheinigung, § 342 Abs. 1 Nr. 3 SGB V. Spätestens dann sollen Daten der ePA auch zu Forschungszwecken durch den Versicherten zur Verfügung gestellt werden können, § 342 Abs. 1 Nr. 4 SGB V.

Seit April 2020 ist auch wieder der Verband der Privaten Krankenversicherung (PKV) Gesellschafter der gematik.[74] Die privaten Krankenversicherungen wollen die ePA erst 2022 in ihrer erweiterten Form anbieten.[75] Darüber hinaus möchten sich einige private Versicherer mit weiteren digitalen Angeboten in der App hervorheben.[76] Diese Zusatzfunktionen müssten hinsichtlich Informationssicherheit und Datenschutz ebenfalls durch von der gematik beauftragte unabhängige Gutachter geprüft werden.

2.4. Allgemeines zur Anwendbarkeit der DSGVO im Kontext der ePA

Die Verordnung 2016/679 (DSGVO) hat kraft EU-Gesetzgebung allgemeine Geltung; sie ist in allen Teilen verbindlich und gilt unmittelbar in jedem Mitgliedsstaat der europäischen Union, Art. 288 UAbs. 2 AEUV.[77] Weiterhin sind bei der Auslegung einer Vorschrift des Unionsrechts neben ihrem Wortlaut und ihrem verfolgten Ziel auch der Kontext und das gesamte Unionsrecht zu berücksichtigen. Die Entstehungsgeschichte einer Vorschrift des Unionsrechts sowie deren Erwägungsgründe können ebenfalls Hinweise für ihre Auslegung geben.[78]

[63] Vgl. Gesellschaft für Telematik (gematik) (2021h, S. 11).
[64] Vgl. aerzteblatt.de Elektronische Patientenakte (2020, o. S).
[65] Vgl. ebd.
[66] Vgl. ebd.
[67] Vgl. Gesellschaft für Telematik (gematik) (2021h, S. 24).
[68] Vgl. Gesellschaft für Telematik (gematik) (2021h, S. 25).
[69] Vgl. Gesellschaft für Telematik (gematik) (2020b, S. 2).
[70] Vgl. Gesellschaft für Telematik (gematik) (2020c, S. 6).
[71] Vgl. Hof (2020, S. 477 Rn. 2).
[72] Vgl. Gesellschaft für Telematik (gematik) (2021c, o. S).
[73] Daten elektronischer Verordnungen nach §360 Abs. 1 SGB V.
[74] Vgl. Gesellschaft für Telematik (gematik) (2020a, o. S). Der PKV war bereits Gesellschafter trat aber 2012 wieder aus der Organisation aus, vgl. Olk, Private Krankenversicherung will wieder an gesetzlicher Digitalisierung teilhaben, handelsblatt.com, 2020, o. S.
[75] PKV Verband der Privaten Krankenversicherung (2020, o. S).
[76] Vgl. aerztezeitung (2020, o. S.): Signal Iduna möchte Mehrwertdienste anbieten, die „deutlich über die gesetzlichen Funktionen hinausgehen“.
[77] Vgl. nur Ehmann/Selmayr/Selmayr/Ehmann, DSGVO, Einführung, A. Einl. Bemerkungen, Rn. 1.
[78] Vgl. EuGH NVwZ 2019, 143 Rn. 47 m.w.N.

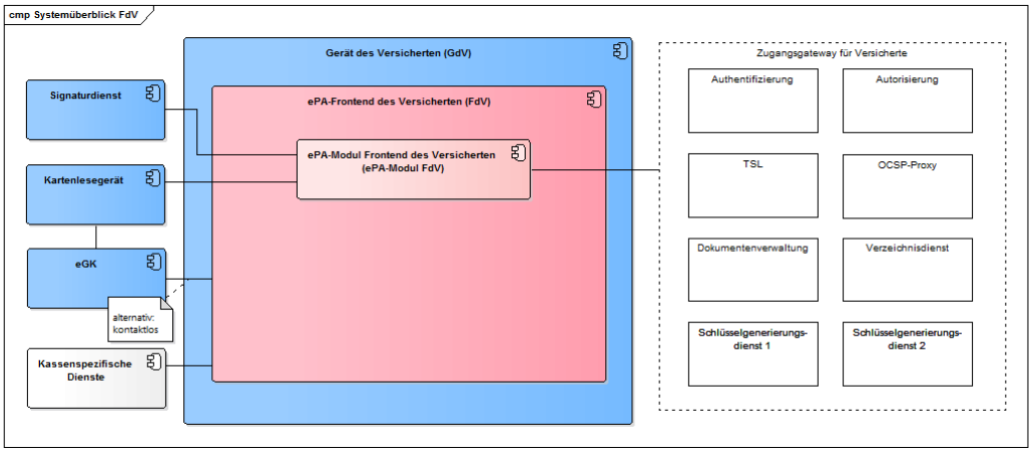

Abbildung 3: High Level Design – ePA-Frontend des Versicherten

Quelle: Gesellschaft für Telematik (gematik) (2021h, S. 13).

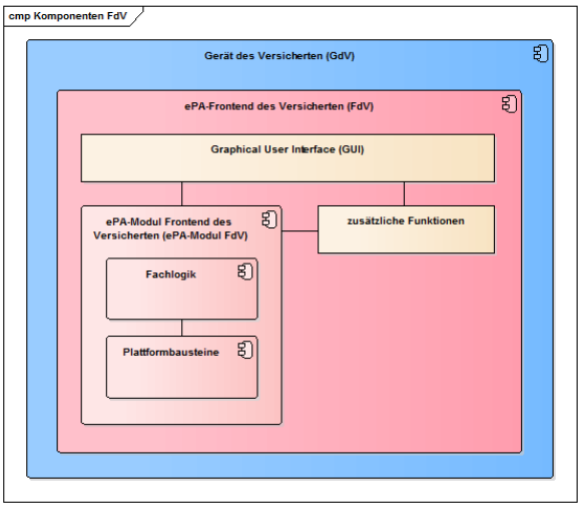

Abbildung 4: Komponenten ePA-Frontend des Versicherten

Quelle: Gesellschaft für Telematik (gematik) (2021h, S. 16).

2.4.1. Sachlicher Anwendungsbereich

Der sachliche Anwendungsbereich der DSGVO ist in Art. 2 Abs. 1 DSGVO geregelt. Die Daten müssen personenbezogen sein, Art. 4 Nr. 1 DSGVO.[79] Die betroffenen Versicherten sind identifizierbare natürliche Personen.

Es muss eine Verarbeitung der Daten vorliegen, Art. 1 Abs. 1, Art. 2 Abs. 1, Art. 4 Nr. 2 DSGVO. Erfasst sind unter anderem automatisierte oder teilautomatisierte Verarbeitungen personenbezogener Daten. Automatisierte Verarbeitungen sind solche, welche mit automatisierten Mitteln bewerkstelligt werden.[80] Darunter sind die meisten rechnergestützten Verarbeitungen personenbezogener Daten zu verstehen.[81]

Im Rahmen der elektronischen Patientenakte werden unterschiedlichste Patientendaten auf den Servern der Betreiber erhoben, gespeichert und verfügbar gemacht. Insbesondere das Ermöglichen des Zugriffs Dritter auf die personenbezogenen Daten ist ein zentrales Element der ePA.[82] Verarbeitet werden beispielsweise Stammdaten und Daten, die wegen ihres Gesundheitsbezugs durch Art. 9 Abs. 1 DSGVO besonderen Schutz genießen. Ein Anwendungsausschluss der Verordnung nach Art. 2 Abs. 2 und 3 DSGVO kommt bei den regelmäßigen Verarbeitungsvorgängen im Bereich der deutschen elektronischen Patientenakte nicht zum Tragen.

[79] S. auch ErwG 1 DSGVO.
[80] Vgl. Ehmann/Selmayr/Zerdick, DSGVO, Art. 2 Rn.3.
[81] Vgl. ebd.
[82] Vgl. weiter unten Abbildung 8.

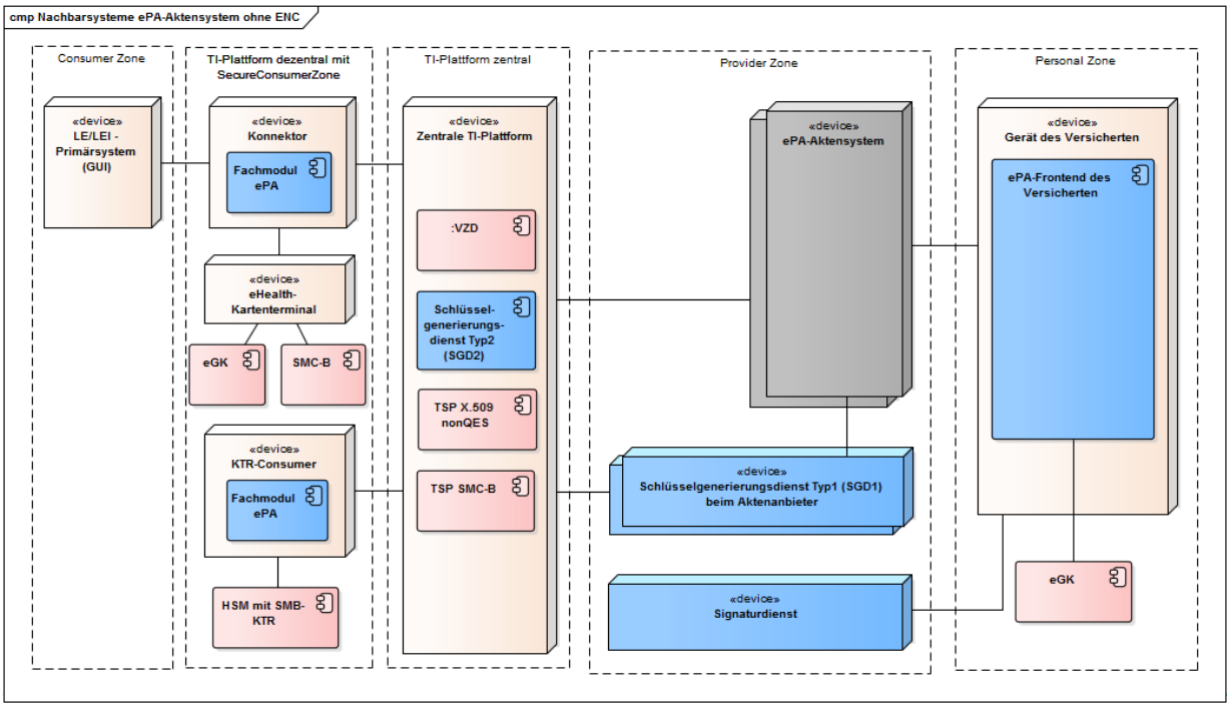

Abbildung 5: Gesamtübersicht der ePA

Quelle: Gesellschaft für Telematik (gematik) (2021g, S. 11).

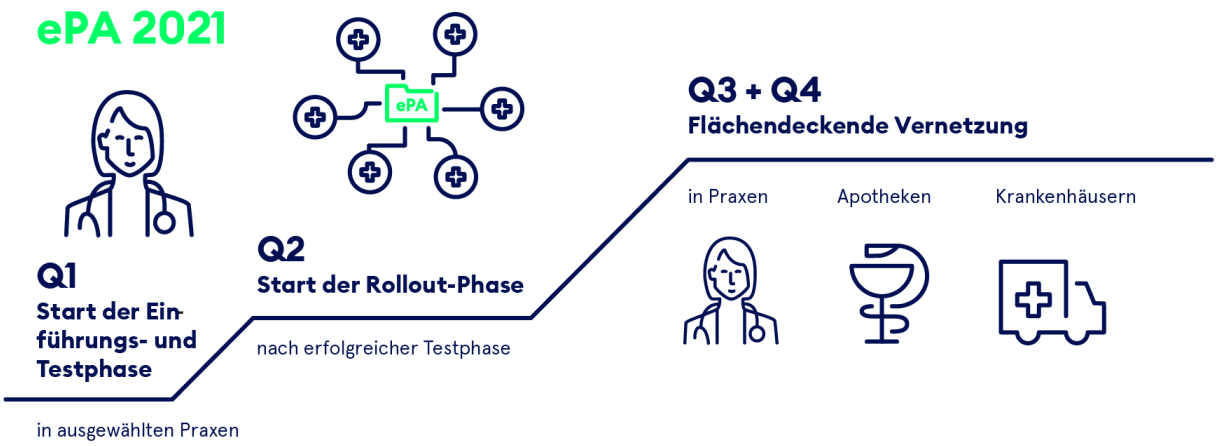

Abbildung 6: Ausbauphase ePA 2021

Quelle: Gesellschaft für Telematik (gematik) (2021c).

2.4.2. Räumlicher Anwendungsbereich

Der räumliche Anwendungsbereich ist in Art. 3 DSGVO geregelt. Die Verarbeitung personenbezogener Daten im Rahmen der deutschen elektronischen Patientenakte fallen in den räumlichen Bereich der DSGVO, da unabhängig vom Ort der Niederlassung der Verantwortlichen, gem. Art. 3 Abs. 1 DSGVO sich ein räumlicher Zusammenhang aus Art. 3 Abs. 2 lit. a DSGVO ergibt. Denn die betroffenen Personen, nämlich die deutschen Patienten, befinden sich in der Europäischen Union und die Datenverarbeitung erfolgt im Kontext des Angebots von Dienstleistungen im Gesundheitsbereich, wie beispielsweise Heilbehandlungen durch Ärzte und andere Leistungserbringer bzw. die Bereitstellung der ePA selbst.

2.4.3. Verantwortlicher

Den Verantwortlichen nach Art. 4 Nr. 7 DSGVO treffen verschiedene Pflichten, die sich aus der Verordnung ergeben, beispielsweise die Umsetzung technischer und organisatorischer Maßnahmen, um sicherzustellen, dass die Datenverar-

beitung mit der Verordnung konform abläuft, Art. 24 Abs. 1 DSGVO. Er ist darüber hinaus auch Adressat direkter Ansprüche einer betroffenen Person, unter anderem des Auskunftsrechts nach Art. 15 DSGVO oder des Schadensersatzes nach Art. 82 DSGVO.[83] Gemäß Art. 4 Nr. 7 1. HS DSGVO ist Verantwortlicher eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Gemäß Halbsatz 2 des Art. 4 Nr. 7 DSGVO kann der Verantwortliche oder die Kriterien seiner Benennung nach dem Recht eines Mitgliedsstaats festgelegt werden, sofern auch die Zwecke und Mittel der Verarbeitung durch das Recht des Mitgliedsstaats vorgegeben sind. Während zuvor noch unklar war, wer Verantwortlicher im Rahmen der elektronischen Patientenakte sei[84], schafft das PDSG nun Abhilfe. Mit Einfügen des 11. Kapitels in das fünfte Buch des Sozialgesetzbuchs, liegt nun eine solche nationalstaatliche Regelung vor. Nach § 307 SGB V ergibt sich sinngemäß die Verantwortlichkeit aus der konkreten Zuständigkeit des Beteiligten und der Entscheidungskompetenz in den für ihn überblickbaren und beherrschbaren Strukturen.[85] Der für die Verarbeitung der Daten zum Zweck der *Nutzung* der elektronischen Patientenakte Verantwortliche ist gem. §§ 307 Abs. 4, 341 Abs. 4 SGB V der jeweilige Anbieter. Für die Nutzung von Komponenten der dezentralen Infrastruktur (vgl. oben Kapitel 2.2.1) sind die jeweiligen Nutzer dieser Komponenten verantwortlich, sofern sie „über die Mittel der Datenverarbeitung mit entscheiden“, § 307 Abs. 1 SGB V. Diese Verantwortlichkeit soll sich im Wesentlichen auf die bestimmungsgemäße Nutzung der Komponenten, deren ordnungsgemäßen Anschluss und die Durchführung der Wartung beziehen.[86] Die Regelung in § 307 Abs. 5 Satz 1 SGB V soll eine durchgehende datenschutzrechtliche Verantwortlichkeit sicherstellen, in dem die gematik als Verantwortliche benannt wird, sofern keine speziellere Verantwortlichkeit vorliegt und soweit sie im Rahmen ihrer Aufgaben über die Mittel der Datenverarbeitung bestimmt.[87] Damit wird der in Art. 26 Abs. 1 Satz 3 DSGVO zum Ausdruck kommende Gedanke aufgegriffen.

Das bedeutet beispielsweise, dass ein Arzt für die Patientendaten in der Praxis verantwortlich ist und der TI-Konnektor vor Missbrauch geschützt wird. Die Verantwortung für die bestimmungsgemäße Funktionsweise des Konnektors liegt hingegen bei dessen Hersteller. Die Datenübertragung und Verarbeitung in der Telematikinfrastruktur fallen in den Verantwortungsbereich der gematik. Die Verantwortung für den Datenschutz im ePA-Aktensystem (s.o. Kapitel 2.2.4) obliegt der jeweiligen Krankenkasse.

Auch wenn die koordinierende Stelle der gematik gem. § 307 Abs. 5 Satz 2 SGB V als Auffangbecken für datenschutzrechtliche Anliegen dient, wird es durch die Aufteilung der Verantwortlichkeit an so viele einzelne Beteiligte, deren Ineinanderwirken kaum vollständig getrennt werden kann, möglicherweise im konkreten Fall zu weiteren Diskussionen kommen.

2.5. Aktuelle Fragestellungen im Gesundheitsdatenschutz

Ein potenziell großer Teil der in der ePA gespeicherten Daten bezieht sich auf den Gesundheitszustand, die Gesundheitsgefährdungen von betroffenen Personen oder lässt zumindest Schlüsse auf eine dieser beiden Eigenschaften zu. Gesundheitsdaten betreffen den höchstpersönlichen Bereich eines Menschen. Mit Gesundheitsdaten können Menschen diffamiert, unter Druck gesetzt oder direkt gefährdet werden. Manchmal möchte eine Person auch gar nicht wissen, wie es um den eigenen Gesundheitszustand bestellt ist. Gesundheitsdaten können für das Individuum ein Leben lang relevant sein.

Der individuelle Schutz von Leben und Gesundheit ist gesetzlich garantiert.[88] Der besondere Schutz von Gesundheit und Leben kommt im europäischen Datenschutzrecht durch das Verbotsprinzip nach Art. 9 Abs.1 DSGVO zum Ausdruck. Danach ist die Verarbeitung von Gesundheitsdaten generell untersagt. Für die Verarbeitung ist das Vorliegen eines in Art. 9 Abs. 2 DSGVO genannten Erlaubnistatbestands erforderlich. Der Katalog in Abs. 2 ist zwar abschließend[89], enthält aber zahl- und weitreichende Ausnahmetatbestände, die zu einer weitgehenden Egalisierung des Verarbeitungsverbots führen.[90]

Im Folgenden wird eine Auswahl aktueller Fragen mit datenschutzrechtlichem Bezug im Rahmen der ePA ausgeführt[91].

2.5.1. Erbkrankheiten

Nur auf den ersten Blick problematisch erscheint die Verarbeitung von Daten über Krankheiten, die durch Vererbung von Vorfahren auf ihre Nachkommen übertragen werden können. Zwar enthalten die Daten Informationen sowohl über den direkt Betroffenen, als auch über dessen Nachkommen, i.e. die Möglichkeit des Vorhandenseins der Krankheit, – insofern könnte den Verarbeiter solcher Daten eine Informationspflicht aus Art. 14 DSGVO treffen – allerdings greifen in solchen Fällen die in Abs. 5 lit. c und lit. d DSGVO formulierten Ausnahmen einer einschränkenden nationalen Regelung[92]: Gemäß § 11 GenDG darf das Ergebnis einer genetischen Untersuchung grundsätzlich „nur der betroffenen Person und nur durch [...] die Ärztin oder den Arzt [...] mitgeteilt werden.“ Auch kommt eine Anwendung des § 203 StGB in Betracht. Ob eine Befugnis zur Weitergabe von Geheimnissen vorliegt, ist im Einzelfall zu prüfen. Schließlich

[83] Vgl. nur Ehmann/Selmayr/Nemitz, DSGVO, Art. 82 Rn. 4.
[84] Vgl. BT-Drs. 19/16228, S. 4.
[85] Vgl. BR-Drs. 164/20, Gesetzentwurf der Bundesregierung, S. 108.
[86] Vgl. BR-Drs. 164/20, Gesetzentwurf der Bundesregierung, S. 108 f.
[87] Vgl. a.a.O., S. 109.
[88] Art. 2, Art. 3, Art. 35 GRCh; Art. 2 Abs. 2 S. 1 GG.
[89] Vgl. Sydow/Kampert, DSGVO, Art. 9. Rn. 5 f; Paal/Pauly/Frenzel, DSGVO, Art. 9 Rn. 18 f.
[90] Vgl. Gola/Schulz, DSGVO, Art. 9 Rn. 1 f.
[91] Vgl. vor allem BT-Drs. 19/6628 und die Stellungnahmen des BfDI zum PDSG.
[92] Vgl. Antwort der Bunderegierung auf eine kleine Anfrage, BT-Drs. 19/6628, S. 4.

dürfte in diesem Bereich das Recht auf Nichtwissen relevant sein. Zur informationellen Selbstbestimmung gehört nämlich auch, dass der Betroffene darüber entscheiden kann, ob er sich mit dem Wissen um seine genetischen Besonderheiten belasten möchte.[93]

2.5.2. Aspekte der Datensicherheit

Kriterien der Datensicherheit[94] sind in Art. 32 DSGVO benannt. Sowohl Verantwortlicher als auch Auftragsverarbeiter sind dazu angehalten geeignete technische und organisatorische Maßnahmen zu treffen, um eine sichere Verarbeitung zu gewährleisten.[95] Die Datensicherheit ist außerdem als Grundsatz in Art. 5 Abs. 1 lit. f DSGVO benannt.

Im Zusammenhang mit Gesundheitsakten wurde in der Vergangenheit immer wieder Kritik hinsichtlich ihrer Datensicherheit geübt. Beispielsweise wurden in der Anwendung „Vivy“ diverse Sicherheitsmängel identifiziert[96], hier einige Beispiele:

- Dokumente wurden mit einer 5-stelligen Session ID aus Kleinbuchstaben veröffentlicht
- Wurde eine Session gefunden, konnten Metadaten, wie Name, Versichertennummer, Adresse, Alter, Geschlecht, Bild, Arzt und Spezialisierung des Arztes ausgelesen werden
- Um das Dokument einzusehen musste eine 4-stellige PIN eingegeben werden (10000 Versuche mit der Brute Force Methode)
- In die App konnte HTML-Code, zum Beispiel Verlinkungen auf Phishing Seiten, eingeschleust werden
- Die 2-Faktor-Authentifizierung konnte mit Brute Force geknackt werden

Solche Mängel sind eine eklatante Gefahr für die Nutzer der Anwendung und eine Katastrophe für den Anbieter.

Auch bei der ePA bzw. der TI wurde hinsichtlich der Datensicherheit an einigen Punkten Kritik geäußert, z.B.:

- Der Einsatz des veralteten Verschlüsselungsprotokolls TLS 1.1 im Versichertenstammdatenmanagement. Mit dem Update der Konnektoren wurde die Unterstützung von TLS 1.1 entfernt. In den Spezifikationen der TI sind Vorgaben zur Verwendung von TLS 1.2 und TLS 1.3 festgeschrieben.[97]
- Alternative Authentifizierungsverfahren[98]: Der BfDI fordert beispielsweise, dass die Authentifizierungsverfahren der Sicherheitsstufe „hoch“ im Sinne der BSI-Richtlinie TR-03147 genügen.[99] Der Bezug zur DSGVO und die Prüfung der Konformität der Authentifizierungsverfahren erfolgt unten in Kapitel 2.9.
- Schwachstelle Mensch: Im Dezember 2020 wurde bekannt, dass Konnektoren in Arztpraxen öffentlich über das Internet erreichbar waren.[100] Die sei darauf zurückzuführen, dass diese Konnektoren fehlerhaft angeschlossen wurden. Die Schwachstelle wurde dem Hersteller mitgeteilt. Eine Richtlinie der Kassenärztlichen Bundesvereinigung soll Sicherheitsstandards in Praxen verbindlich festlegen, § 75b Abs. 1 SGB V.[101] Des Weiteren wird der Einsatz von zertifizierten Fachleuten vorgeschrieben, § 75b Abs. 5 SGB V.[102]
- Gutachter der TU Graz fanden Schwachstellen im sogenannten VAU-Protokoll.[103] Nach Aussage der gematik führen diese Schwachstellen ohne weitere Folgen zu keinem praktisch durchführbaren Angriff.[104] Die Schwachstellen seien mit einer neuen Version umgehend ausgebessert worden.[105]

Bei Betrachtung dieser Probleme ist zu bedenken ist, dass ein System niemals vollständig sicher sein kann. Je komplexer, desto anfälliger ist es für Schwachstellen. Wichtig ist jedenfalls, dass die vorgeschriebenen Standards eingehalten und kontrolliert werden. Immerhin lässt die Aussage des IT-Experten Christoph Saatjohann hoffen: Auf die verschlüsselte Datenbank im Internet und die entsprechenden Server sei ein sehr hoher Wert gelegt worden.[106] Er sei vorsichtig optimistisch; die bekannten Probleme seien angegangen worden.

2.5.3. Datenschutz-Folgenabschätzung

Fraglich ist, ob vor der Verarbeitung von Daten besonderer Kategorien, wie den Gesundheitsdaten, grundsätzlich die Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO angezeigt ist.[107] Der Maßstab des Art. 35

[93] Vgl. dazu Kühling/Buchner/Weichert, Art. 9 Rn. 34.

[94] Im Kontext des Datenschutzes ist oft von Datensicherheit die Rede, auch wenn weitgehende überschneidungen mit der Informationssicherheit bestehen.

[95] Vgl. Hof, Datenschutz mittels IT-Sicherheit, S. 477 Rn. 2.

[96] Vgl. Tschirsich, Martin, All Your Gesundheitsdaten Are Belong To Us, 2018, o. S.

[97] Vgl. BT-Drs. 19/16228, S. 10.

[98] i.e. Authentifizierungsverfahren ohne elektronische Gesundheitskarte. Vgl. BfDI (2020a, o. S).

[99] Bundesamt für Sicherheit in der Informationstechnik (BSI) (2018).

[100] Vgl. tagesschau.de (2020, o. S).

[101] S. auch KBV, Richtlinie nach §75b SGB V Anforderungen, 2020.

[102] S. auch KBV (2020).

[103] i.e. Vertrauenswürdige Ausführungsumgebung. Vgl. Slany (2020, S. 4).

[104] Vgl. Gesellschaft für Telematik (gematik) (2020d, S. 2).

[105] Vgl. ebd.

[106] Vgl. sueddeutsche.de (2020, o. S).

[107] Vgl. die Ansicht der Freien ärzteschaft, Gelten die Datenschutzgesetze nicht für Gesundheitsminister Spahn?, 2020, o. S. Die Freie ärzteschaft steht der Digitalisierung des Gesundheitswesens grundsätzlich kritisch gegenüber. Weiterhin wurde a.a.O. auch behauptet, der BfDI hätte die Durchführung einer Datenschutz-Folgenabschätzung einfordert. Tatsächlich hat der BfDI in einer ersten Stellungnahme zum Entwurf des PDSG (vgl. BfDI, 2020b, S. 2) lediglich dazu angeregt von der Gestaltungsmöglichkeit in Art. 35 Abs. 10 DSGVO Gebrauch zu machen und eine Datenschutz-Folgenabschätzung verbindlich vorzusehen. In der Stellungnahme hinsichtlich der öffentlichen Anhörung einen Monat später ist dieser Vorschlag nicht mehr enthalten (vgl. BfDI, 2020a).

Abs. 1 DSGVO ist ein „voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen“.[108] Die Beurteilung ob eines solches Risiko vorliegt, ergibt sich aus einer Synthese der in Abs. 1, 3, 4, 5 genannten Kriterien und auch aus den Erwägungsgründen 71, 75, 76, 89, 91.[109] Es genügt nicht, dass eines der beschriebenen Risiken oder Schadensszenarien möglich erscheint, es ist vielmehr erforderlich, dass das konkrete Risiko *im Einzelfall* über die allgemeinen Gefahren hinausgeht. Eine pauschale Verpflichtung zu einer Datenschutz-Folgenabschätzung aufgrund nur eines dieser Merkmale ist durch den EU-Gesetzgeber nicht vorgesehen. Allerdings könnte sich eine Verpflichtung aus Art. 35 Abs. 3 lit b DSGVO ergeben, nach der eine Datenschutz-Folgenabschätzung gemäß Abs. 1 erforderlich ist, wenn eine *umfangreiche* Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DSGVO erfolgt. Im Parlamentsentwurf der DSGVO wurde in einem ähnlichen Zusammenhang davon ausgegangen, dass bei einem Richtwert von 5.000 betroffenen Personen innerhalb von zwölf aufeinanderfolgenden Monaten ein „konkretes Risiko“ erreicht sei.[110] Da die Verordnung in ihrer jetzigen Fassung aber keinen konkreten Richt- oder Schwellwert angibt, ist davon auszugehen, dass ein „voraussichtlich hohes Risiko“ auch mit einem deutlich niedrigeren Wert vorliegen kann. Die Aufteilung der Verantwortlichkeiten im Rahmen der ePA erschwert eine Beurteilung der Sachlage. Konkretisiert werden kann die Norm durch eine Positivliste der Aufsichtsbehörde, Art. 35 Abs. 4 DSGVO. Der BfDI hat eine solche Liste veröffentlicht. Allerdings ergeben sich daraus keine besonderen Erkenntnisse: Am Ende des knappen Dokuments wird auf eine grundsätzliche Einzelfallprüfung verwiesen.[111] Für die Krankenkassen und Ärzte wären die Listen der entsprechenden LfDI zu berücksichtigen, deren Prüfung den Rahmen dieser Arbeit sprengen würde.

Schließlich ist davon auszugehen, dass stets im Einzelfall zu betrachten ist, welcher Verantwortliche eine Datenschutz-Folgenabschätzung durchführen muss. Auf der Hand liegt, dass eine einzelne Arztpraxis eher weniger dazu verpflichtet sein wird als eine Krankenkasse oder die gematik mit der gesamten TI im Rücken.[112] Im Angesicht der wenig greifbaren Norm und, zumindest auf deutscher Bundesebene, auch wenig greifbaren Konkretisierung, bleibt abzuwarten, inwiefern hier die Judikative Abhilfe schaffen muss. Gegen die Befugnisse einer Aufsichtsbehörde aus Art. 58 DSGVO, kann sich der Verantwortliche gem. Art. 78 Abs. 1 DSGVO gerichtlich wehren. Die Pflichten aus Art. 35 DSGVO betreffen übrigens nicht die Rechtmäßigkeit des einzelnen Verarbeitungsvorgangs.[113]

2.5.4. Ausschließlicher Zugang über Mobile Devices in 2021

Der Zugang zur elektronischen Patientenakte erfolgt in der ersten Ausbaustufe der ePA bis 1. Januar 2022 ausschließlich über Apps für iOS oder Android („Frontend-Nutzer“). In der zweiten Ausbaustufe ab 1. Januar 2022 sollen die Krankenkassen verpflichtet sein, auch „Frontend-Nichtnutzern“ mit anderen Mitteln den Zugriff auf die ePA ermöglichen, § 338 Abs. 1 SGB V.[114] Ursprünglich war hierfür eine flächendeckende Bereitstellung von entsprechenden Terminals vorgesehen.[115] Diese Regelung wurde aber später wieder verworfen.[116] Nun soll von der gematik nur noch evaluiert werden, ob ein Bedarf für eine flächendeckende Bereitstellung solcher Einrichtungen besteht, § 338 Abs. 2 SGB V.

Der BfDI sieht in der mangelnden Ausstattung für Frontend-Nichtnutzer eine Ungleichbehandlung im Grundrecht auf informationelle Selbstbestimmung.[117] Er bemängelt einen Wertungswiderspruch zu § 336 SGB V der den Versicherten garantiert, auf die Daten ihrer ePA zugreifen zu können.[118]

Ob ein solcher Wertungswiderspruch in der Sozialgesetzgebung besteht, muss hier nicht geprüft werden, da der Wertungsmaßstab dieser Arbeit sich nur aus der DSGVO ergibt.[119]

2.5.5. Berechtigungsmanagement

Die Einführung der ePA erfolgt wie bereits dargestellt in mehreren Ausbaustufen mit unterschiedlichen Möglichkeiten in der Berechtigungsverwaltung für Dokumente. Ein wesentliche Kritikpunkt des BfDI ist das Ausbleiben eines differenzierten Berechtigungsmanagements, das den Zugriff der Leistungserbringer und anderer berechtigter Personen regelt.[120] Der allgemeine Zugriff auf Daten des Versicherten ist in § 339 SGB V und der Zugriff durch Leistungserbringer auf Daten der elektronischen Patientenakte ist in § 352 SGB V geregelt. Voraussetzungen an die Einwilligung des Versicherten bezüglich des Zugriffs anderer sind in § 342 Abs. 2 Nr. 1 lit. c, sowie Nr. 2 lit. b und speziell in § 353 SGB V festgelegt. Die ePA wird unter diesem Aspekt in zwei Schritten eingeführt. Mit dem Start der ePA ab 1. Januar 2021 gibt es noch kein ausdifferenziertes Rechtemanagement, während spätestens ab 1. Januar 2022 die Versicherten eine Einwilligung auf den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen erteilen können sollen. Dies ergibt sich aus den Formulierungen in § 342 Abs. 2 Nr. 1 lit. c und Abs. 2 Nr. 2 lit. b SGB V.

[108] Art. 35 Abs. 1 DSGVO „aufgrund“.
[109] Vgl. Ehmann/Selmayr/Baumgartner, DSGVO, Art. 35 Rn. 24; Sydow/Schwendemann, DSGVO, Art. 35 Rn. 10.
[110] Vgl. ErwGe 63 und 75, Art, 25 Abs. 2 lit. b, Art. 32a Abs. 2 lit. a und Art. 35 Abs. 1 lit. b des Beschlusses des Europäischen Parlaments vom 12.3.2014, COM(2012)0011 – C7 – 0025/2012 – 2012/0011 (COD).
[111] Vgl. BfDI (2019, S. 2).
[112] Vgl. ähnlich auch Ehmann/Selmayr/Baumgartner, DSGVO, Art. 35 Rn. 39.
[113] Vgl. nur Ehmann/Selmayr/Baumgartner, DSGVO, Art. 35 Rn.78.
[114] Vgl. BR-Drs. 164/20, S. 119.
[115] Vgl. BR-Drs. 164/20, S. 33.
[116] Vgl. Verbraucherzentrale (2020, o. S).
[117] Vgl. BfDI (2020a, o. S).
[118] Vgl. BfDI (2020b, S. 3).
[119] Vgl. unten 2.7.1.1 zur Frage, ob diese potentielle Diskriminierungslage einen Einfluss auf die Einwilligung i.S.v. Art. 4 Nr. 11 DSGVO hat.
[120] Vgl. zuletzt BfDI (2020b, S. 3).

Damit die Berechtigungserteilung einer Einwilligung im Sinne der DSGVO entspricht, müssen die Voraussetzungen nach Art. 4 Nr. 11 DSGVO gegeben sein. Die technische Erteilung der Zugriffsberechtigung ist von der Einwilligung gemäß Art. 4 Nr. 11 DSGVO zu trennen, so dass eine Einwilligung widerrufen werden kann, auch wenn technisch der Zugriff noch möglich wäre. Die Grundlage der Verarbeitung würde dann dennoch wegfallen.

Die folgenden Abbildungen geben einen Überblick über die verschiedenen Möglichkeiten des Zugriffs durch die Leistungserbringer.

Die DSGVO-Konformität des Berechtigungsmanagement wird unten in Kapitel 2.7 f. näher betrachtet.

2.5.6. Erkenntnis für die vorliegende Arbeit

Im Rahmen der ePA gibt es eine Vielzahl von Ansatzpunkten zur Prüfung datenschutzrechtlicher Vorgaben. Auch eine abstrahierte – vom Einzelfall losgelöste – Prüfung der DSGVO-Konformität müsste, sofern sie den Anspruch an ihre Vollständigkeit genügen sollte, im Grunde für jede Art von Verarbeitungsvorgang gesondert erfolgen. Angenommen jeder unten abgebildete Anwendungsfall repräsentierte einen Verarbeitungsvorgang, so wird deutlich, dass die Prüfung der einzelnen Verarbeitungsvorgänge im Rahmen dieser Arbeit nicht möglich ist (Abbildung 9). Eine detaillierte Prüfung soll im folgenden Kapitel abschließend für die zuletzt vorgebrachten Kritikpunkte des BfDI hinsichtlich der ePA erfolgen, deren Relevanz derzeit am höchsten sein dürfte.

2.6. Spannungsverhältnis zwischen DSGVO und SGB V

Seit Oktober 2020 gilt das PDSG zur näheren Ausgestaltung der ePA und verpflichtet die gesetzlichen Krankenkassen zum Angebot der ePA ab 1. Januar 2021. Der BfDI kritisierte schon frühzeitig einige Aspekte des PDSG und in seinen Stellungnahmen zum PDSG wurden diese erneut formuliert.[121] Am 16. November 2020 übermittelte der BfDI eine Warnung an die gesetzlichen Kassen in seinem Zuständigkeitsbereich.[122] Aus Sicht des BfDI verstießen die Krankenkassen gegen die DSGVO, sofern sie die ePA nur nach den Vorgaben des PDSG umsetzten. Kritisiert werden zwei Eigenschaften der ePA: zum einen das Fehlen eines feingranularen Rechtemanagements[123], zum anderen die Verwendung sogenannter alternativen Authentifizierungsverfahren[124]. Der Aufsicht des BfDI unterliegen derzeit 63 gesetzliche Krankenkassen mit ca. 44 Millionen Versicherten.[125] Diese Krankenkassen müssten Zusatzfunktionen anbieten, die ein feingranulares Rechtemanagement ermöglichen und sie müssten von den alternativen Authentifizierungsverfahren absehen. Der BfDI behielt sich vor weitere Maßnahmen nach Art. 58 Abs. 2 DSGVO zu prüfen.[126]

In der Antwort auf eine kleine Anfrage ging die Bundesregierung auf die Auffassung des BfDI ein.[127] Die Bundesregierung teilt die Bedenken des BfDI nicht. Das PDSG sei von den Verfassungsressorts umfassend auf die Vereinbarkeit mit übergeordnetem Recht geprüft worden. Der BfDI sei fortlaufend in die fachliche Diskussion mit eingebunden und hätte maßgeblich an der Erarbeitung der Regelungen im Gesetzesentwurf zum PDSG mitgewirkt.

Das Bundesamt für Soziale Sicherung (BAS) formulierte seine Ansichten in einer Stellungnahme zur Warnung des BfDI und stärkte den Krankenkassen den Rücken.[128] Die Vereinbarkeit des PDSG mit übergeordnetem Recht sei geprüft worden. Die Nutzung der ePA sei freiwillig und die Verarbeitung geschehe aufgrund einer wirksamen Einwilligung (Art. 4 Nr. 11 DSGVO). Darüber hinaus seien die Informationspflichten der DSGVO auch in der Sozialgesetzgebung berücksichtigt worden (§ 343 Abs. 1 Nr. 3 SGB V). Das Diskriminierungsverbot in § 335 SGB V garantiere eine echte Wahlfreiheit. Auch allgemeine Grundsätze der DSGVO seien nicht verletzt worden (Art. 5, 25 und 32 DSGVO).

Zutreffend ist, dass die geforderten Maßnahmen des BfDI bis zum Einführungstermin der ePA nicht umsetzbar sind, da die Spezifikationen bei der gematik noch nicht definiert waren und erst eine Zulassung der gematik erfolgen müsste.[129] Das BAS müsste als Ausführungsbehörde die Sanktionen ohne Ermessen vollziehen, sofern dies der GKV-Spitzenverband in einem entsprechenden bestandskräftigen Bescheid feststellt, § 342 Abs. 5 S. 2 SGB V.[130]

Damit wurden die Krankenkassen vom Gesetzgeber und oberster Datenschutzaufsichtsbehörde in ein Dilemma bugsiert, das diese nicht auflösen können.

Im Dezember 2020 wurde ein Gutachten der Kanzlei Redeker Sellner Dahs veröffentlicht, das durch das *health innovation hub* des Bundesgesundheitsministeriums beauftragt wurde. Die Verfasser des Gutachtens gelangen zum Ergebnis, dass die Umsetzung der Sozialgesetzgebung nicht gegen das europäische Datenschutzrecht verstößt.[131]

Aufgrund des oben beschriebenen Konfliktpotentials der Normen und der dargelegten allgemeinen Anwendbarkeit der DSGVO (s.o. Kapitel 2.4), soll im Folgenden eine ausführliche Prüfung der Hauptkritikpunkte des BfDI – i.e. das Fehlen eines ausdifferenzierten Berechtigungsmanagements und die Sicherheit der alternativen Authentifizierungsverfahren – nach Maßgabe der DSGVO erfolgen.

2.7. Berechtigungsmanagement ab 1. Januar 2021, § 342 Abs. 2 Nr. 1 SGB V

Die allgemeine sachliche und räumliche Anwendbarkeit und das grundsätzliche Vorhandensein von Verarbeitungsvor-

[121] BfDI (2020b); BfDI (2020a); BfDI (2020a, o. S).
[122] BfDI (2020b).
[123] Vgl. a.a.O., S. 1 ff.
[124] Vgl. BfDI (2020a, o. S.); BfDI (2020a, S. 7).
[125] BfDI (2021, o. S.); BfDI (2020a, o. S).
[126] BfDI (2020b, S. 3).
[127] Vgl. BT-Drs. 19/23243, S 2 f.
[128] Vgl. Bundesamt für Soziale Sicherung, Stellungnahme zur elektronischen Patientenakte, 2020.
[129] Vgl. Bundesamt für Soziale Sicherung, Stellungnahme zur elektronischen Patientenakte, 2020, S. 2 f.
[130] Vgl. a.a.O., S. 3.
[131] Vgl. Böllhoff, Cornelius, et al. (2020, S. 4 f.)

Berufsgruppe	Mögliche Verwendung medizinischer Informationen über Versicherte	Mögliche Verwendung der von Versicherten zur Verfügung gestellten Gesundheitsinformationen
Ärztinnen/Ärzte, Zahnärztinnen/Zahnärzte, Psychotherapeutinnen und -therapeuten, Krankenhäuser, Rehakliniken	Verarbeitung	Verarbeitung
Apothekerinnen/Apotheker	Auslesen, Speicherung und Verwendung sowie Verarbeitung des elektronischen Medikationsplans	Auslesen, Speicherung und Verwendung
Gesundheits- und Krankenpflegerinnen und -pfleger, Gesundheits- und Kinderkrankenpflegerinnen und -pfleger, Altenpflegerinnen und -pfleger, Pflegefachfrauen und Pflegefachmänner sowie deren Helferinnen und Helfer	Auslesen, Speicherung und Verwendung	Auslesen, Speicherung und Verwendung
Hebammen/Entbindungspfleger	Auslesen, Speicherung und Verwendung	Auslesen, Speicherung und Verwendung
Physiotherapeutinnen/Physiotherapeuten	Auslesen, Speicherung und Verwendung sowie Verarbeitung von Daten zu Befunden, Diagnosen, durchgeführten und geplanten Therapiemaßnahmen oder Früherkennungsuntersuchungen, von Behandlungsberichten und sonstigen untersuchungs- und behandlungsbezogenen medizinischen Informationen, die sich aus der physiotherapeutischen Behandlung ergeben	Auslesen, Speicherung und Verwendung
Arbeitsmedizinerinnen/Arbeitsmediziner, Betriebsärztinnen/Betriebsärzte	Auslesen, Speicherung und Verwendung	Auslesen, Speicherung und Verwendung
Öffentlicher Gesundheitsdienst	Verarbeitung, soweit für Aufgabenerfüllung erforderlich	Verarbeitung, soweit für Aufgabenerfüllung erforderlich

Abbildung 7: Zugriff der Leistungserbringer auf die ePA ab Januar 2021

Quelle: GKV-Spitzenverband (2020a, S. 15).

Kontrolle	Ausbaustufe	Berechtigung für	auf	wie
undifferenziert	1. Januar 2021	zugriffsberechtigte Leistungserbringer	Dokumente von Leistungserbringern UND ODER Dokumente vom Versicherten	App/eGK
differenziert	1. Januar 2022	zugriffsberechtigte Leistungserbringer	Vertraulichkeitsstufe ▪ normal UND ODER vertraulich UND ODER streng vertraulich	App/eGK/Vertreter
			Mittlere Granularität ▪ eine oder mehrere Kategorien einer Vertraulichkeitsstufe	App/eGK/Vertreter
			Feine Granularität ▪ einzelne Dokumente	App/eGK/Vertreter

Abbildung 8: Zusammenfassung Berechtigungsmanagement

Quelle: In Anlehnung an GKV-Spitzenverband (2020a, S. 15 ff).

gängen wurden oben dargelegt (oben 2.4). Im weiteren Verlauf der Prüfung sei stets von der Verarbeitung von Gesundheitsdaten, als Daten einer besonderen Kategorie im Sinne des Art. 9 Abs. 1 DSGVO, ausgegangen. Insofern wird die Einwilligung bezüglich der Registrierung bzw. Authentifizierung hier nicht berücksichtigt, weil dabei ausschließlich Stammdaten betroffen sind, die in der Regel keine Daten besonderer Kategorien enthalten.[132] Insofern sei auf Verarbeitungsvorgänge im Rahmen der Nutzung der ePA, i.e. die Verarbeitung von gesundheitsbezogenen Dokumenten und Datensätzen, abgestellt.

[132] Zur Frage, ob die personenstandsrechtliche Geschlechtsangabe ein sensibles Datum sein kann: Ehmann/Selmayr/Schiff, Art. 9 Rn. 30 dort Fn. 80.

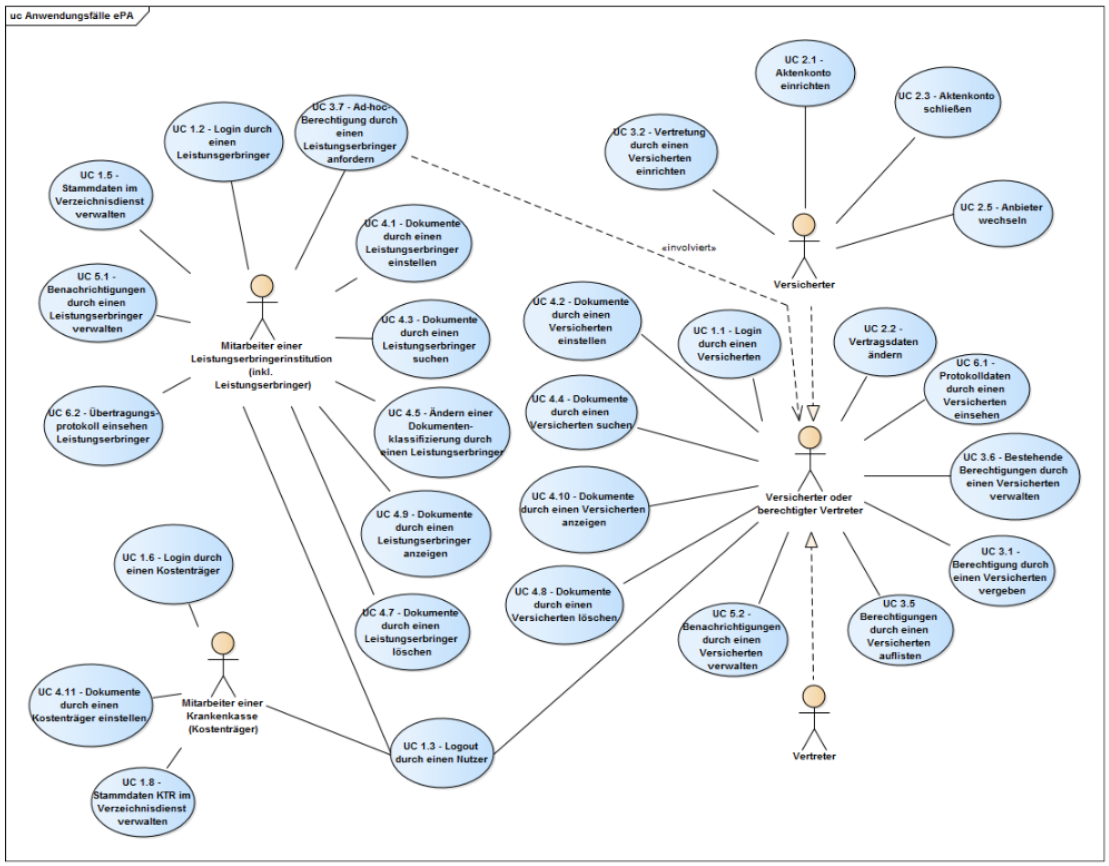

Abbildung 9: Anwendungsfälle der ePA

Quelle: Gesellschaft für Telematik (gematik) (2019, S. 37)

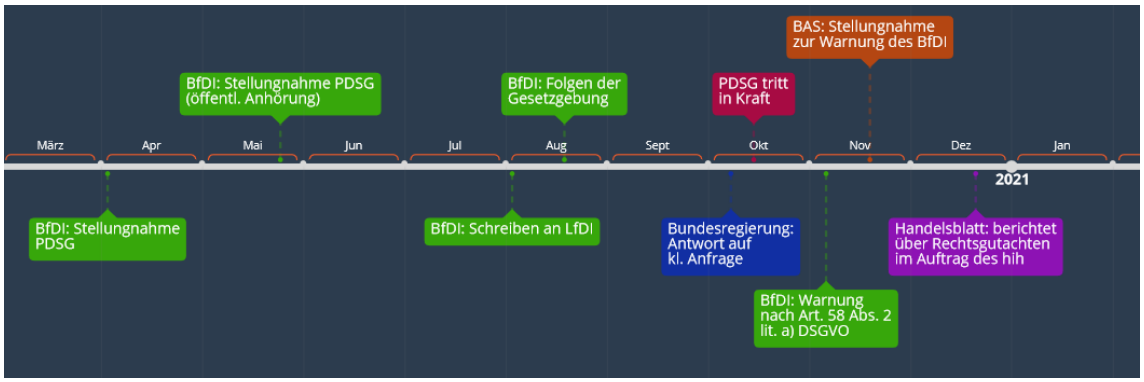

Abbildung 10: Zeitstrahl – BfDI vs ePA

Quelle: Eigene Darstellung

2.7.1. Rechtmäßigkeit der Datenverarbeitung aufgrund einer Einwilligung

Die Rechtmäßigkeit der Datenverarbeitung ergibt sich aus den Bestimmungen des Art. 6 Abs. 1 Satz 1 bzw. Art. 9 Abs.2 DSGVO.

Die Regelungen der Sozialgesetzgebung, insbesondere §§ 339 Abs. 1, 342 Abs. 2 Nr. 1 lit. c, 353 SGB V, verlangen für die Verarbeitung der in der ePA gespeicherten Gesundheitsdaten eine Einwilligung im Sinne des Art. 6 Abs. 1 lit. a bzw. Art. 9 Abs. 2 lit. a DSGVO.[133] Insofern besteht keine eigene Rechtsgrundlage in der Sozialgesetzgebung, die Verarbeitungsvorgänge in der ePA legitimieren könnten. Mithin scheidet eine

[133] Vgl. Böllhoff, Cornelius, et al. (2020, S. 23 f.)

Verarbeitung aufgrund von Art. 9 Abs. 2 und lit. h DSGVO aus.

Eine Verarbeitung aufgrund von Art. 9 Abs. 2 lit. c DSGVO kommt gegebenenfalls in Ausnahmefällen in Betracht. Beispielsweise, wenn in der ePA überlebenswichtige Informationen abgerufen werden können und die betroffene Person außer Stande ist, eine Einwilligung nach Art. 4. Nr. 11, Art. 7, Art. 9 Abs.2 lit. a DSGVO abzugeben.[134] Allerdings ist das nicht der Regelfall und taugt daher nicht als Gegenstand einer vom Einzelfall losgelösten Prüfung.

Eine Verarbeitung nach Art. 9 Abs. 2 lit. g und lit. i DSGVO scheidet in Ermangelung entsprechender Gesetzgebung aus.[135]

Fraglich ist aber, ob eine Datenverarbeitung auch gem. Art. 6 Abs. 1 lit. b DSGVO nicht schon aufgrund eines Nutzungsvertrag rechtmäßig ist. Dafür muss die Verarbeitung für die Vertragserfüllung erforderlich sein.[136] Hier könnte zwischen den Backend-seitigen und Frontend-seitigen Verarbeitungsvorgängen zu unterschieden werden. Wenn beispielsweise einem Leistungserbringer eine Berechtigung erteilt wird (nicht erforderlich), ist es zwingend notwendig, dass entsprechende Parameter im ePA-Aktensystem im Verantwortungsbereich der Krankenkasse gespeichert werden (erforderlich). Diese Speicherung der Einstellung können auch – zumindest mittelbare – Gesundheitsdaten enthalten, und zwar Metadaten wie die Art der Freigabe, der zugriffsberechtigter Arzt und dessen Fachrichtung. Die Erfüllung eines Vertrags ist allerdings kein Ausnahmetatbestand des Art. 9 Abs. 2 DSGVO. Insofern ist Art. 6 Abs. 1 lit. b DSGVO nicht auf Gesundheitsdaten anwendbar.[137] Grundlage einer Datenverarbeitung von Gesundheitsdaten in der ePA kann daher ausschließlich eine *Einwilligung gemäß Art. 6 Abs. 1 lit. a bzw. Art. 9 Abs. 2 lit. a, Art. 7 und Art. 4 Nr. 11 DSGVO* sein. Diese Einwilligung kann gleichwohl für den Zweck eingeholt werden, um Funktionalitäten bereitstellen zu können, die der Durchführung eines Nutzungsvertrages dienen.[138] Die Einwilligung bezieht sich im oben angeführten Beispiel daher auf das Auslesen der Daten durch den Leistungserbringer, und auch auf die Speicherung der Einstellung, dass diese Daten gelesen werden dürfen.

Im Sinne des Art. 4 Nr. 11 DSGVO ist eine Einwilligung jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, Art. 4 Nr. 11 DSGVO. Weitere Anforderungen an die Einwilligung werden in Art. 7 DSGVO aufgeführt.

Freiwilligkeit, Art. 4 Nr. 11, Art. 7 Abs. 4 DSGVO

Freiwilligkeit liegt vor, wenn die betroffene Person über eine echte Wahl und die Kontrolle bei der Abgabe der Einwilligung verfügt.[139] Die Einwilligung ist nichtig, sofern die betroffene Person keine echte Wahl hat, sich zur Einwilligung gedrängt fühlt oder negative Auswirkungen erdulden muss, wenn sie nicht einwilligt.[140] Dies ist beispielsweise der Fall, wenn die betroffene Person die Einwilligung nicht verweigern oder zurückziehen kann, ohne Nachteile zu erleiden.[141] Unangemessener Druck oder Einflussnahme auf die betroffene Person, die diese von der Ausübung ihres freien Willens abhalten, können demnach zur Unwirksamkeit der Einwilligung führen.[142]

Letztlich muss die Einwilligung zwar im konkreten Fall betrachtet werden, eine systematische Beeinflussung in der Willensbildung ist bei der ePA aber nicht erkennbar. Insbesondere die für den Vertrieb zuständigen Krankenkassen treten bezüglich der ePAen eher verhalten auf. Insbesondere wird auf intensive Bewerbung verzichtet.[143] Zudem könnte das Diskriminierungsverbot gem. § 335 SGB V zur Wahrung der Freiwilligkeit, auch im konkreten Fall, beitragen. Dem Versicherten dürfen keine Nachteile entstehen, wenn er die Nutzung der ePA oder den Zugriff auf Daten in der ePA ablehnt oder nachträglich widerruft. Demnach soll es sich bei der ePA um ein zusätzliches Angebot an den Versicherten handeln. Die Leistungen der Leistungserbringer sollen mit oder ohne Zugriff auf die ePA in der gleichen Güte erbracht werden.[144] Fraglich ist aber, ob diese gesetzliche Kodifizierung eine tatsächliche Ungleichgewichtslage zu verhindern vermag. Maßgeblich ist die tatsächliche Gestaltung der ePA und damit verbundene objektive feststellbare Vorteile und deren Wirkung auf die Zielgruppe. Dabei müssen Nutzen und Kosten gegeneinander abgewogen werden. Es wird kaum zu bestreiten sein, dass die Nutzung der ePA über mobile Endgeräte Vorteile mit sich bringt, beispielsweise den schnellen und unkomplizierten Zugriff und eine bes-

[134] Vgl. Forgó/Helfrich/Schneider/Arning/Born, Betrieblicher Datenschutz, Teil X. Kapitel 2 Rn. 47.

[135] Vgl. a.a.O., Rn. 48.

[136] Ehmann/Selmayr/Heberlein, DSGVO, Art. 6 Rn. 13; Paal/Pauly/Frenzel, DSGVO, Art. 6 Rn. 14; Kühling/Buchner/Buchner/Petri, DSGVO, Art. 6 Rn. 38 ff.

[137] Vgl. Forgó/Helfrich/Schneider/Arning/Born, Betrieblicher Datenschutz, Teil X. Kapitel 2 Rn. 52 dort Fn. 39; Engler, ZD 2018, 55, 58. Ungenau: DAK (2021, o. S.), Punkt 6.: „Die Rechtsgrundlage für die Datenverarbeitung im Rahmen der Nutzung der ePA ist Art. 6 Abs. 1 lit. b DSGVO, da diese Datenverarbeitungsvorgänge für die ordnungsgemäße Erfüllung des Nutzungsvertrags mit dem Nutzer über die ePA erforderlich sind."

[138] Vgl. so z.B: Die Techniker, Datenschutzerklärung für die elektronische Patientenakte und „TK-Safe", 2021, o. S.

[139] Vgl. ErwG 42 DSGVO; Artikel-29-Datenschutzgruppe, Leitlinien in Bezug auf die Einwilligung, S.6; Paal/Pauly/Ernst, DSGVO, Art. 4 Rn. 69; Sydow/Ingold, DSGVO, Art. 7 Rn. 29.

[140] Vgl. Böllhoff, Cornelius, et al. (2020, S. 26).

[141] ErwG 42 DSGVO, BeckOK Datenschutzrecht/Stemmer, 33 Art. 7 Rn. 38.

[142] Vgl. Gola/Schulz, DSGVO, Art. 7 Rn. 21.

[143] Vgl. aerzteblatt.de Elektronische Patientenakte (2020). Dies entspricht auch dem Eindruck des Verfassers: Auf den Internetauftritten der größten gesetzlichen Krankenkassen (AOKen, Techniker, BARMER, DAK) wird auf der Hauptseite nicht direkt auf die Verfügbarkeit einer elektronischen Patientenakte verwiesen. Auf der Internetpräsenz der KKH findet man überhaupt keine Verlinkung zu den App Distributionen von Google und Apple (Stand: Mai 2021).

[144] Vgl. Böllhoff, Cornelius, et al. (2020, S. 27).

sere Strukturierung und Sammlung von gesundheitsrelevanten Dokumenten (vgl. oben Kapitel 2.2.2). Ohne diese Vorteile wäre die Entwicklung und Bereitstellung der ePA allerdings auch nicht wirtschaftlich und überhaupt notwendig. Die Möglichkeit der Nutzung dieser Vorteile begründet keine Diskriminierungslage. Es wird insbesondere kein unbilliger emotionaler oder wirtschaftlicher Druck ausgeübt.

Insofern besteht auch keine Zwangslage bei Frontend-Nichtnutzern. Es ist kaum vorstellbar, dass Versicherte, die kein mobiles Endgerät nutzen können oder wollen, einem derartigen Druck unterliegen, dass sie sich zur Verwendung eines mobilen Endgeräts gezwungen fühlen. Mithin ist eine potentielle Ungleichbehandlung allenfalls innerhalb der Sozialgesetzgebung gegebenenfalls unter der Berücksichtigung von grundrechtlichen Garantien zu prüfen.[145]

Auch ein latentes Ungleichgewicht in der Arzt-Patienten-Beziehung, das je nach Schwere einer Erkrankung unterschiedlich sein dürfte und sich auch bei der Zugriffserteilung in der ePA auswirken könnte, schließt nicht von vornherein die Freiwilligkeit einer Einwilligung aus.[146] Eine von der Literatur teilweise geforderte Kompensation des Ungleichgewichts durch weitere Voraussetzungen dürfte bei der ePA erfüllt sein[147]:

- Umfassende Aufklärung des Patienten darüber, zu welchem spezifischen Zweck seine Daten verarbeitet werden sollen

Art. 13 Abs. 1 lit. c DSGVO und entsprechende Regelungen in der Sozialgesetzgebung beinhalten diese Anforderung (vgl. unten Kapitel 2.7.1.3).

- Behandlungsnachteile dürfen nicht an die Entscheidung des Patienten geknüpft werden

Hier greift das Diskriminierungsverbot nach § 335 SGB V.

- Die Ergebnisse der Datenverarbeitung können dem Patienten zu Gute kommen

- Die Datenverarbeitung selbst erfolgt zu nichtkommerziellen Zwecken

Auch das ist der Fall.

Unter dem Aspekt der Freiwilligkeit muss weiterhin das in Art. 7 Abs. 4 DSGVO und ErwG 43 S. 2 2. Alt. DSGVO zum Ausdruck kommende *Kopplungsverbot* geprüft werden.[148] Ein gewisser Druck könnte auf die betroffene Person einwirken, sofern keine Alternativen auf dem Markt verfügbar sind.[149] Weil letztlich aber schwierig festzustellen ist, ob eine Leistung substituierbar ist, wird der Schutzzweck des Art. 7 Abs. 4 DSGVO eng auszulegen sein, nämlich insofern, dass geprüft werden muss, ob die Daten für den Vertragszweck erforderlich sind und die Verweigerung der Einwilligung nicht ohne Nachteil für die betroffene Person erfolgt.[150] Im Kern soll verhindert werden, dass Daten für vom Vertragsgegenstand „vollkommen losgelöste Zwecke“ erhoben werden.[151] Wie oben festgestellt wird zum einen kein unbilliger emotionaler oder wirtschaftlicher Druck auf die betroffene Person ausgeübt. Zum anderen sind die Verarbeitungsvorgänge für die Erfüllung des Nutzungsvertrag des Versicherten mit der Krankenkasse unbedingt erforderlich, damit die Funktionalitäten vertragsgemäß bereitgestellt werden können.[152]

Auch eine Kopplung an das Grundverhältnis des Versicherten mit der Krankenkasse besteht nicht, da die Erteilung der Zugriffsmöglichkeit auf die Gesundheitsdaten der Versicherten an die Leistungserbringer demselben *Zweck* dient wie das Grundverhältnis.[153] Beides erfolgt zur Gewährleistung der Gesundheitsversorgung des Versicherten.[154] In § 352 SGB V ist zusätzlich festgeschrieben, dass der Zugriff auf Daten durch Personen in der ePA nur dann erfolgen darf, wenn er für die Versorgung des Versicherten erforderlich ist.

Ferner wird in der Literatur ein *horizontales Kopplungsverbot* genannt. Dieses soll verhindern, dass zu verschiedenen nebeneinander bestehenden Verarbeitungsvorgängen nicht gesondert eine Einwilligung des Betroffenen eingeholt wird, obwohl dies im Einzelfall angebracht wäre.[155] Wegen des fehlenden ausdifferenzierten Berechtigungsmanagements kann es im Kontext der ePA, beispielsweise durch das parallele Abfragen von Dokumenten durch verschiedene Leistungsträger zu nebeneinander bestehenden Verarbeitungsvorgängen kommen, die möglicherweise eine gesonderte Einwilligung des Betroffenen erfordern. Diese Frage soll jedoch nicht an dieser Stelle, sondern vielmehr nachfolgend im Rahmen des Merkmals des „bestimmten Falls“ geprüft werden.

Bestimmtheit

Die Einwilligungserklärung muss gem. Art. 4 Nr. 11 DSGVO weiterhin „für den bestimmten Fall“ abgegeben werden, damit der Betroffene die Reichweite seiner Erklärung überblicken kann und der Verantwortliche Grenzen für die Verarbeitung der personenbezogenen Daten vorfindet.[156] Die Bestimmtheit der Einwilligung ergibt sich de facto aus

[145] Vgl. dazu ausführlich, in ähnlichem Zusammenhang: Böllhoff, Cornelius, et al. (2020, S. 39).

[146] Vgl. Otto und Rüdlin (2017), 519, 521 m.w.N.

[147] Vgl. ebd. mit Verweis auf Lodzig, ZD-Aktuell 2012, 02952.

[148] Vgl. beispielsweise Ehmann/Selmayr/Heberlein, DSGVO, Art. 6 Rn. 7; Taeger/Gabel/Taeger, DSGVO, Art. 6 Rn. 29.

[149] Vgl. Teager/Gabel/Taeger, DSGVO, Art. 7 Rn. 85; Plath/Plath, DSGVO, Art. 7 Rn. 15; Albrecht, CR 2016, 88, 91; Paal/Pauly/Frenzel, DSGVO, Art. 7 Rn. 20; Gola/Gola, DSGVO Art. 4 Rn. 85.

[150] Vgl. Teager/Gabel/Teager, Art. 7 Rn. 93; Golland (2018), 130, 132; Laue/Kremer/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, §2 Rn. 22 f.

[151] Vgl. Gola/Schulz, DSGVO, Art. 7 Rn. 24 f.

[152] Vgl. beispielsweise BKK, Nutzungsvertrag, o. S. Punkt 2: „Die ePA ermöglicht dem Nutzer die sichere Speicherung, übermittlung und Verwaltung ihrer Gesundheitsdaten (z.B., Befunde, Laborberichte, Arztbriefe, etc).“

[153] Vgl. Böllhoff, Cornelius, et al. (2020, S. 32).

[154] Vgl. a.a.O., S. 33.

[155] Vgl. Gola/Gola, DSGVO, Art. 4 Rn. 85; ErwG 43 S. 2 2. Alt. DSGVO.

[156] Vgl. BeckOK Datenschutzrecht/Stemmer, Rn. 74; Forgó/Helfrich/Schneider/Arning/Born, Teil X. Kapitel 2 Rn.53.

dem Zusammenspiel der Informationen an den Betroffenen und der Einwilligungserklärung, womit sich folglich das Bestimmtheitserfordernis mit der Informationsplicht überschneidet (s. nachfolgendes Kapitel).[157] Umfasst vom Bestimmtheitsgrundsatz sind der Verantwortliche, die Art der Verarbeitung, die Verarbeitungszwecke und letztlich die zu verarbeitenden Daten selbst.[158]

Insbesondere hinsichtlich des zuletzt genannten Kriteriums, könnten sich im Rahmen der elektronischen Patientenakte Probleme ergeben. Denn in der ersten Ausbauphase der ePA ist kein ausdifferenziertes Berechtigungsmanagement vorgesehen. Die Dokumente lassen sich in dieser Ausbaustufe in zwei Kategorien einteilen (s.o. 2.5.5). Der Versicherte kann entscheiden, ob ein Leistungserbringer auf eine oder beide Kategorien zugreifen kann. Der Leistungserbringer kann technisch auf alle Dokumente dieser Kategorie zugreifen.

Der BfDI sieht in diesem Zusammenhang die Freigabe nach einem „Alles-oder-nichts-Prinzip".[159] An dieser Stelle muss bereits festgehalten werden, dass selbst in der ersten Ausbaustufe der ePA kein „Alles-oder-nichts-Prinzip" besteht, da eine Differenzierung nach den einzelnen Leistungserbringern und nach den Kategorien „Dokumente des Leistungserbringers" und „Dokumente des Versicherten" erfolgen kann. Außerdem kann eine zeitliche Befristung des Zugriffs erfolgen.[160]

In der DSGVO ist die Ausgestaltung der Einwilligung hinsichtlich ihrer Granularität nicht definiert. So kann die Einwilligung auch generell zweckbezogen erteilt werden, anstatt bezogen auf jeden einzelnen Verarbeitungsvorgang für denselben Zweck.[161] Dies kommt auch insbesondere in ErwG 32 S. 4 zum Ausdruck. Mithin sind an die Festlegung des Zweckbegriffs in der DSGVO keine klaren Anforderungen festgelegt. So können die Zwecke in ihrem Abstraktionsgrad variieren.

Auch die Zusammenfassung mehrerer Zwecke unter einer Einwilligung ist möglich, sofern diese bestimmt und abschließend bezeichnet sind und die Einwilligung insgesamt nicht gegen das Kopplungsverbot verstößt.[162] Ob dabei besondere Kriterien an die Spezifizierung des Zwecks anzulegen sind, kann letztlich dahinstehen, denn die Einwilligung in der ePA bezieht sich auf *einen* Zweck, nämlich der *gesundheitlichen Versorgung* des Versicherten.

Gegen eine restriktive Auslegung der Bestimmtheit spricht auch die Informationspflicht aus Art. 14 Abs. 1 lit. c DSGVO. Der Gesetzgeber geht davon aus, dass die betroffene Person nicht alle Daten konkret kennen muss, um wirksam einzuwilligen.[163]

Ebenfalls ist in einem Arbeitspapier zu elektronischen Patientenakten der Artikel-29 Datenschutzgruppe kein datenschutzrechtliches Gebot zur Gewährleistung eines granularen Zugriffsberechtigungsmanagements zu erkennen.[164] Es wird vielmehr empfohlen, dass unterschiedliche Module nach verschiedenen Vertraulichkeitsstufen mit unterschiedlichen Zugangsvoraussetzungen eingerichtet werden sollen.[165]

Im Kontext der ePA ist weiterhin nicht ersichtlich, warum ein derart besonderer Sachverhalt vorliegen sollte, der die Voraussetzungen eines horizontalen Kopplungsverbots erfüllt, ErwG 43 S. 2 1. Alt. DSGVO. Dass die Daten einer besonderen Kategorie nach Art. 9 Abs. 1 DSGVO besonders schutzbedürftig sind reicht dafür allein nicht aus. Außerdem sollte auch keine vollständige Entmündigung der Person betrieben werden, indem ihr trotz maximaler Transparenz die Möglichkeit einer Einwilligung genommen wird.[166] Insofern sei hier teilweise auf die Erfüllung der Informationspflichten und des Transparenzgebots der DSGVO verwiesen.

Ein Minus in der Granularität der Einwilligung könnte durch ein Plus in Information und Transparenz ausgeglichen werden.

Informiertheit und Transparenzgebot

Die Einwilligung muss weiterhin dem Grundsatz der Informiertheit entsprechen, Art. 4 Nr. 11 DSGVO. Dafür muss die betroffene Person im Vorfeld abschätzen können, welche Auswirkungen die Erteilung einer Einwilligung für sie hat und sie muss die Umstände der Datenverarbeitung sowie die Tragweite ihrer Einwilligung eindeutig und klar erkennen können.[167] Die Person muss darüber in Kenntnis gesetzt werden, welche Arten von Daten zu welchem Zweck verarbeitet werden, wer die verantwortliche datenverarbeitende Stelle ist und wie diese zu erreichen ist, sowie an welche Dritten die Daten im Falle der Übermittlung weitergeben werden.[168]

Weiterhin muss die betroffene Person über die Widerrufbarkeit der Einwilligung und die Rechtmäßigkeit der bis zum Widerruf erfolgten Verarbeitung unterrichtet werden, Art. 7 Abs. 3 DSGVO.[169] In der Literatur ist umstritten, ob das Ausbleiben dieser Informationspflicht die Unwirksamkeit der Einwilligung nach sich zieht.[170]

[157] Vgl. BeckOK Datenschutzrecht/Stemmer, Art. 7 Rn. 75; Kugelmann, DuD 2016, 566, 568.

[158] Vgl. BeckOK Datenschutzrecht/Stemmer, Art. 7 Rn. 75.

[159] BfDI (2020b, S. 2).

[160] Diese ist standardmäßig auf 7 Tage festgelegt, kann vom Nutzer aber auch kürzer (ab 1 Tag) oder länger (bis 540 Tage) eingestellt werden. Vgl. dazu: GKV-Spitzenverband (2020a), Kapitel 5.4, S. 16.

[161] Vgl. BeckOK Datenschutzrecht/Stemmer, Art. 7 Rn. 77.

[162] Vgl. ebd.; ErwG 43 DSGVO.

[163] Vgl. Böllhoff, Cornelius, et al. (2020, S. 29).

[164] Vgl. Artikel-29-Datenschutzgruppe (2007, S. 18).

[165] Vgl. ebd.

[166] Vgl. in ähnlichem Zusammenhang: Gola/Schulz, DSGVO, Art. 7 Rn. 35. In diese Richtung auch Schantz, Wolff, DSGVO, 2017, D II Rn. 517: Es hinge von der Komplexität der Einwilligung ab, ob eine differenzierte Einwilligung angebracht ist. Mit der Granularität der Einwilligung steigt auch ihre Komplexität. Man könnte befürchten, dass der Betroffene überfordert sein dürfte, wenn er eine Vielzahl zusätzlicher Entscheidungen treffen müsste.

[167] Vgl. Kühling/Buchner/Buchner/Kühling, DSGVO, Art. 4 Nr. 11 Rn. 8, Art. 7 Rn. 59.

[168] Vgl. a.a.O., Art. 7 Rn. 59.

[169] Vgl. Taeger/Gabel/Taeger, DSGVO, Art. 7 Rn. 57: Die Informationspflicht bezieht sich sowohl auf Satz 1 als auch auf Satz 2.

[170] Bejahend: Taeger/Gabel/Taeger, DSGVO, Art. 7 Rn. 5; verneinend: Eh-

Weitere Informationspflichten ergeben sich aus Art. 13 und 14 DSGVO und aus den allgemeinen Anforderungen in Art. 12 DSGVO.

Im Rahmen der ePA finden sich konkretisierende Vorschriften in § 343 SGB V und in § 353 Abs. 2 SGB V. § 343 SGB V regelt eine allgemeine Informationspflicht der Krankenkassen mit einer Auflistung zahlreicher Gesichtspunkte, die als nicht abschließend anzusehen sind.[171] Gemäß Absatz 2 der Vorschrift soll den Krankenkassen entsprechendes Informationsmaterial durch den Spitzenverband Bund der Krankenkassen im Einvernehmen mit dem BfDI zur Verfügung gestellt werden. Dieses Material findet man beispielsweise auf den Webseiten der Krankenkassen.[172] Gemäß § 353 Abs. 2 SGB V werden zusätzlich die Leistungserbringer verpflichtet, die Frontend-Nichtnutzer über die fehlende Granularität der Zugriffserteilung zu informieren.

Im Verhältnis zur DSGVO „extensivere Informationspflichten“ sind mit Schaffung der genannten Vorschriften nicht von vornherein impliziert.[173] Beispielsweise ist nach europäischer Vorschrift über den Umstand zu informieren, dass es sich bei den zu verarbeitenden Daten um Daten einer besonderer Kategorie im Sinne des Art. 9 Abs. 1 DSGVO handelt, bereits weil die betroffene Person gem. Art. 9 Abs. 2 lit. a DSGVO „ausdrücklich“ in die Verarbeitung einwilligen muss.[174] Der Regelkatalog in § 343 Abs. 1 SGB V enthält diesbezüglich beispielsweise keine ausdrückliche Regelung, wobei sich dieser Umstand aus dem Kontext der Norm ergeben sollte. Ob die Informationsübermittlung den Pflichten aus der DSGVO entspricht ist unabhängig von der Normierung im Sozialgesetzbuch für den konkreten Einzelfall zu prüfen.

Hinsichtlich der Präsentation von Informationen gibt es in der DSGVO keine konkreten Vorschriften. Neben den weitgehend unspezifischen Kriterien Art. 12 Abs. 1 S. 3 und 4 DSGVO (präzise, transparente, verständliche und leicht zugängliche Form; klare, einfache Sprache) ist Art. 12 Abs. 7 DSGVO zu nennen, der auf die Möglichkeit der Verwendung von unterstützenden Bildsymbolen verweist. Bislang hat sich keiner der verfügbaren Symbolsätze am Markt durchgesetzt.[175] Um das oben erwähnte Minus der Granularität der Einwilligung auszugleichen, hätte der Gesetzgeber von seinem Gestaltungsspielraum Gebrauch machen können und präzisere Anforderungen an die Präsentation der Informationen formulieren können. Eine spielerische, gestalterisch intelligente Auseinandersetzung, gegebenenfalls in Verbindung mit einer Anleitung zur Verwendung der Anwendungen, hätte einen viel höheren Wirkungsgrad als die bloße Text-Information über eine Website, die nicht einmal direkt mit der Anwendung verknüpft ist.[176] Eine anschauliche Vermittlung der datenschutzrelevanten Informationen würde auch das Vertrauen der Versicherten in das Produkt ePA stärken.

Fraglich ist darüber hinaus, ob auch über die *Bedenken* des BfDI informiert werden muss.[177] Der BfDI plante die Krankenkassen anzuweisen ihren Versicherten einen „von ihm vorgegebenen Warntext“ zukommen zu lassen.[178] Diese Forderung wurde den Krankenkassen bis jetzt nicht offiziell übermittelt.[179]

Unmissverständlichkeit und Form

Die Einwilligung muss gem. Art. 4 Nr. 11 DSGVO eine „unmissverständlich abgegebene Willensbeurkundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung“ sein. Die größte Rechtssicherheit gewährleistet die ausdrückliche Einwilligungserklärung, wobei keine Schriftform erforderlich ist.[180] Es genügt demnach auch eine elektronisch zum Ausdruck gebrachte Einwilligung, beispielsweise durch Auswählen von Checkboxen und Bestätigung durch einen weiteren Klick auf einen Bestätigungs-Button. Der Verantwortliche muss gem. Art. 7 Abs. 1 DSGVO nachweisen können, dass eine dem Verarbeitungsvorgang entsprechende Einwilligung vorliegt. Diese Nachweispflicht erfordert, dass die Einwilligung in einer durch die Norm nicht näher spezifizierten Art dokumentiert werden kann.[181] Damit liegt in der Regel eine unmissverständliche Willensbekundung vor.[182] Sofern die Krankenkassen dieser Dokumentationspflicht, beispielsweise durch die Protokollierung der Einwilligungsparamater, nachkommen können, sind die Willensbekundungen als unmissverständlich zu betrachten.

Widerrufbarkeit

Nach Art. 7 Abs. 3 DSGVO muss die Einwilligung jederzeit widerrufbar sein. Die Widerrufbarkeit stellt sicher, dass der Betroffene nicht unwiederbringlich seines Selbstbestimmungsrechts beraubt wird, sondern ihm ein „Weg zu-

mann/Selmayr/Heckmann/Paschke, DSGVO, Art. 7 Rn. 89: Die ausdrückliche Unwirksamkeitsregelung in Absatz 2 spräche gegen eine entsprechende Auslegung für Absatz 3; Ernst, ZD 2017, 110, 112; Differenzierung, ob die Datenverarbeitung bereits begonnen hat oder nicht Simitis/Hornung/Spiecker/Klement, DSGVO, Art. 7 Rn. 95.

[171] Vgl. §343 Abs. 1 Satz 3 SGB V „insbesondere“.

[172] So z.B. AOK https://www.aok.de/pk/fileadmin/user_upload/Universell/05-Content-PDF/RS_2020-852_Anlage_01_-_mit_AOK_Anpassung_ITSG_GKV-SV.pdf.

[173] So. z.B. Böllhoff, Cornelius, et al. (2020, S. 31).

[174] Vgl. Kühling/Buchner/Buchner/Kühling, DSGVO, Art. 7 Rn. 60a.; s. auch Böllhoff, Cornelius, et al. (2020, S. 31).

[175] Vgl. Kühling/Buchner/Bäcker, DSGVO, Art. 12 Rn. 20.

[176] So jedenfalls bei der AOK App „Mein Leben“. Die Informationen nach §343 SGB V sind nicht direkt in der App enthalten. Vgl. zum Thema Medienbruch: Kühling/Buchner/Buchner/Kühling, DSGVO, Art. 7 Rn. 60a; Lüdemann, Pokrant, DuD 2019, 365, 368.

[177] z.B. Borchers, Detlef, Diagnose: digital!, c't 2021, 116, 118: „Zunächst werden sie [die Kassen] auf jeden Fall ihre Versicherten anschreiben und die Bedenken des obersten Datenschützers übermitteln.“.

[178] Vgl. BfDI (2020a, S. 2); BfDI (2020b).

[179] Dementsprechend enthält die AOK App „Mein Leben“ auch keinen Warntext.

[180] Vgl. BeckOK Datenschutzrecht/Stemmer, Art. 7 Rn. 80.

[181] Vgl. BeckOK Datenschutzrecht /Stemmer, Art. 7 Rn. 80, Rn. 88.

[182] Vgl. BeckOK Datenschutzrecht /Stemmer, Art. 7 Rn 80; Paal/Pauly/Frenzel, DSGVO, Art. 7 Rn. 6.

rück“ offenbleibt.[183] Der Widerruf hinsichtlich der Nutzung der gesamten Anwendung ist in der Information des GKV-Spitzenverbands geregelt.[184] Die technische Rückabwicklung einzelner Zugriffsberechtigungen der Leistungserbringer ist für Frontend-Nichtnutzer derzeit über das erneute Setzen einer Zugriffsberechtigung mit der Mindestdauer (1 Tag) zu realisieren.[185] Das ist nicht elegant, aber zumutbar.

Zwischenergebnis

Damit sind die Voraussetzungen einer wirksamen Einwilligung nach Art. 6 Abs. 1 Satz 1 lit. a bzw. Art. 9 Abs. 2 lit. a DSGVO gegeben. Insbesondere die fehlende Granularität der Zugriffserteilung steht der Wirksamkeit der Einwilligung nicht entgegen.

2.7.2. Grundsätze des Datenschutzes gem. Art. 5 DSGVO

Fraglich ist, ob über die Rechtmäßigkeit der Verarbeitung hinaus, die in Art. 5 DSGVO benannten Grundsätze des Datenschutzes verletzt werden. Implikationen dieser Grundsätze wurden teilweise schon im Rahmen der Wirksamkeit der Einwilligung geprüft. Der BfDI stellt Verstöße gegen Art. 5 Abs. 1 lit. b, c und f DSGVO fest.[186]

Grundsätze der Datenminimierung und Erforderlichkeit

Gemäß Art. 5 Abs. 1 lit c DSGVO dürfen nur solche Daten verarbeitet werden, die auf den Zweck bezogen, der Datenverarbeitung *angemessen*, *erheblich*, und für den Zweck *erforderlich* sind.[187] Der Grundsatz der Erforderlichkeit ist damit eine Ausprägung des Grundsatzes der Datenminimierung.[188] Die Angemessenheit des Verhältnisses der Datenverarbeitung mit dem Zweck ist gegeben, wenn ihre Zuordnung zu dem Zweck nicht beanstandet werden kann.[189]

Es bestehen keine Anhaltspunkte, dass die Verarbeitung der Daten in der ePA dem Zweck der Gesundheitsversorgung nicht *angemessen* wäre.

Die *Zweckerheblichkeit* ist dann gegeben, wenn die Verarbeitung der Daten geeignet ist, ein legitimes Ziel zu erreichen.[190] Die Datenverarbeitung in der ePA ist geeignet einen bestimmten Grad der Gesundheitsversorgung zu erreichen und die Gesundheitsversorgung ist ein legitimes Ziel.

Die Prüfung, ob bei der ersten Ausbaustufe der ePA durch das grobgranulare Dokumentenmanagement nicht erforderliche Datenverarbeitungen vorgenommen werden könnten, muss nicht durchgeführt werden, weil die Verarbeitung nicht erforderlicher Daten durch die Einwilligung legitimiert wäre.[191] Dafür spricht insbesondere, dass der *Erforderlichkeitsgrundsatz* in beinahe allen Rechtsgrundlagen der DSGVO genannt wird, nur nicht im Wortlaut der Rechtsgrundlage der Einwilligung in Art. 6 Abs. 1 lit. a oder Art. 9 Abs. 2 lit. DSGVO.[192] Die bewusste und informierte Entscheidung für die Nutzung von Diensten, die potentiell nicht dem Erforderlichkeitsgrundsatz entsprechen, muss gerade aufgrund der informationellen Selbstbestimmung möglich sein.[193] Diese Garantie beinhaltet auch, dass der einzelne mit seinen Daten verfahren kann, wie er möchte. Eine weitere Erforderlichkeitsprüfung würde den Sinn einer freiwilligen und informierten Einwilligung völlig konterkarieren. Der Umstand auf einen möglichen Verzicht der Erforderlichkeit von Datenverarbeitungen sollte in der Einwilligung aber entsprechend zum Ausdruck kommen.[194] Die Einwilligung erfolgt im Rahmen der ePA unter der Information, dass das Berechtigungsmanagement bis 1. Januar 2022 nicht auf Dokumentenebene steuerbar ist.[195]

Grundsatz der Integrität und Vertraulichkeit

Nach Art. 5 Abs. 1 lit. f DSGVO müssen Daten so verarbeitet werden, dass sie eine angemessene Sicherheit der Daten gewährleisten. Dafür sollen insbesondere geeignete technische und organisatorische Maßnahmen zum Einsatz kommen um vor etwaigen Risiken zu schützen. Etwas näher konkretisiert wird der Grundsatz in Art. 32 Abs. 1 und 2 DSGVO.[196] Die geeigneten technischen und organisatorischen Maßnahmen müssen ein dem Risiko angemessenes Schutzniveau gewährleisten. Die Maßnahmen sind vom Verantwortlichen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs der Umstände, und der Zwecke der Verarbeitung, sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu treffen.

Art. 32 Abs. 1 und 2, sowie Art. 25 Abs. 1 DSGVO schreiben dem Verantwortlichen jedoch keine konkreten Maßnahmen zur Datensicherheit vor. Der Verantwortliche muss selbst einen abgestimmten Katalog technischer und organisatorischer Maßnahmen ermitteln und umsetzen, der in seiner Gesamtschau dazu geeignet ist, die in Art. 5 lit. f DSGVO benannten Risiken zu minimieren.[197]

In der ersten Ausbaustufe der ePA ist technisch nicht ausgeschlossen, dass Leistungserbringer auf Daten zugreifen

[183] Vgl. Teager/Gabel/Taeger, DSGVO, Art. 7 Rn. 69.
[184] Vgl. GKV-Spitzenverband (2020a, S. 8).
[185] Vgl. a.a.O., S. 14.
[186] Vgl. BfDI (2020b, S. 3).
[187] Vgl. Kühling/Buchner/Herbst, DSGVI, Art. 5 Rn. 57; Sydow/Reimer, DSGVO Art. 5 Rn. 32.
[188] BeckOK DatenschutzR/Schantz, Art. 5 Rn. 25.; Böllhoff, Cornelius, et al. (2020, S. 33).
[189] Vgl. Paal/Pauly/Frenzel. DSGVO, Art. 5 Rn. 35.
[190] Vgl. BeckOK DatenschutzR/Wolff, Art.5 Rn. 24.
[191] Vgl. BeckOK DatenschutzR/Wolff, Syst. A Prinzipien des Datenschutzrechts, Rn. 57.
[192] Vgl. Böllhoff, Cornelius, et al. (2020, S. 34).
[193] Vgl. ebd.; Sydow/Ingold, DSGVO, Art. 7 Rn. 10 DSGVO: Einwilligung als Realisierung der Autonomie als primärrechtlich garantierte Grundrechtsausübung.
[194] Vgl. BeckOK DatenschutzR/Wolff, Syst. A Prinzipien des Datenschutzrechts, Rn. 57.
[195] Vgl. GKV-Spitzenverband (2020a, S. 13 ff).
[196] Vgl. Kühling/Buchner/Herbst, DSGVO, Art. 5 Rn. 76.
[197] Vgl. Kühling/Buchner/Herbst, DSGVO, Art. 32 Rn. 5; Zur Vielfalt möglicher technischer und organisatorischer Maßnahmen Paal/Pauly/Martini, DSGVO, Art. 32 Rn. 29.

können, die sie nicht zwingend benötigen, um die Gesundheitsversorgung des Versicherten sicherzustellen.

Eine *unrechtmäßige* Verarbeitung nach Art. 5 lit. f DSGVO liegt aber wegen einer wirksam erteilten Einwilligung nicht vor.[198] Dem Schutz vor einer *unbefugten* Verarbeitung dient § 352 SGB V, der Leistungserbringer den Zugriff auf Daten verbietet, die zur Behandlung nicht erforderlich sind. Der Rückgriff auf das Berufsgeheimnis[199] vermag indes nicht zu überzeugen, da eine unbefugte Verarbeitung auch durch Berufsgeheimnisträger vorgenommen werden kann. Eine technische Umsetzung wäre zwar zu befürworten, aber am Ende kann auch hier diskutiert werden, inwiefern das Risiko einer unbefugten Verarbeitung von der Einwilligung des Versicherten gedeckt wäre.[200]

Grundsatz der Zweckbindung

Es liegt kein Verstoß gegen den Zweckbindungsgrundsatz nach Art. 5 Abs. 1 lit. b DSGVO vor, weil die Versicherten ihre freiwillige und informierte Einwilligung im Hinblick auf einen bestimmten Zweck abgeben (s.o. 2.7.1.2).[201] Eine Verarbeitung der Daten zu anderen Zwecken ist nicht ersichtlich.

2.7.3. Art. 25 DSGVO

Art. 25 DSGVO enthält ausschließlich Konkretisierungen der in Art. 5 DSGVO genannten datenschutzrechtlichen Grundsätze.[202] Wie zuvor ausgeführt ist aufgrund der wirksamen Einwilligung nicht von einem Verstoß gegen die Datenschutzgrundsätze auszugehen, daher können auch die Konkretisierungen des Art. 25 DSGVO nicht zu einem anderen Ergebnis führen.[203]

2.7.4. „Datensouveränität“

Der BfDI kritisiert mehrfach, dass Versicherte durch das defizitäre Berechtigungsmanagements in ihrer „Datensouveränität“ beschnitten würden.[204] Richtig ist, dass eine Datensouveränität in der DSGVO weder datenschutzrechtlicher Grundsatz noch Wirksamkeitsvoraussetzung einer Einwilligung ist.[205] Allerdings muss festgehalten werden, dass der BfDI diesen Begriff nie ausdrücklich im Zusammenhang mit den Anforderungen der DSGVO, sondern vielmehr mit einem möglichen Wertungswiderspruch innerhalb der Sozialgesetzgebung nennt. Dies ist aber nicht Prüfgegenstand dieser Arbeit.

[198] Vgl. Böllhoff, Cornelius, et al. (2020, S. 35).
[199] Vgl. ebd.
[200] Vgl. so dann wieder Böllhoff, Cornelius, et al. (2020, S. 37).
[201] Vgl. so auch Böllhoff, Cornelius, et al. (2020, S. 36).
[202] Vgl. Ehmann/Selmayr/Heberlein, DSGVO, Art. 5 Rn. 23; Kühling/Buchner/Herbst, DSGVO, Art. 5 Rn. 59; Teager/Gabel/Voigt, DSGVO, Art. 5 Rn. 29.; Gola/Pötters, DSGVO, Art. 5 Rn. 23.
[203] Vgl. so auch Böllhoff, Cornelius, et al. (2020, S. 37).
[204] Vgl. BfDI (2020a, S. 13.); BfDI (2020b, S. 3.); BfDI (2020a, S. 2).
[205] Vgl. so auch Böllhoff, Cornelius, et al. (2020, S. 24 f).

2.7.5. Zwischenergebnis

Das Berechtigungsmanagement der ePA in der ersten Ausbaustufe bis zum 1. Januar 2022 genügt den Anforderungen der DSGVO. Die freiwillige und informierte Einwilligung dient als Rechtsgrundlage für die Verarbeitung der Daten und damit verbundener potentieller Einschränkungen der Datenverarbeitungsgrundsätze.

2.8. Berechtigungsmanagement ab 1. Januar 2022, § 342 Abs. 2 Nr. 2 SGB V

Anhand des oben festgestellten Ergebnisses kann für die zweite Stufe des Berechtigungsmanagement, die noch eine feinere Differenzierung ermöglicht, mit einem Erst-Recht-Schluss festgestellt werden, dass hier ebenso kein Verstoß gegen europäisches Datenschutzrecht vorliegen wird.

2.9. Authentifizierungsanforderungen, § 336 Abs. 2 Nr. 2 SGB V

§ 336 Abs. 2 Nr. 2 SGB V regelt den Zugriff des Versicherten auf die ePA ohne Verwendung der elektronischen Gesundheitskarte (eGK) durch ein geeignetes technisches Verfahren, das einen hohen Sicherheitsstandard gewährleistet. Der BfDI kritisiert das aktuelle von der gematik zugelassene Zugriffsverfahren „Alternative Versicherten-Identität“ (al.vi).[206] Er fordert eine Sicherheitseinstufung „hoch“ entsprechend der eIDAS-VO.[207]

Im Rahmen der DSGVO kommt ein Verstoß gegen Art. 32 Abs. 1 und 2 DSGVO in Betracht. Wie oben in Kapitel 2.7.2.2 ausgeführt, schreibt die DSGVO dem Verantwortlichen jedoch keine konkreten Maßnahmen hinsichtlich der Ausgestaltung der Datensicherheit, sondern vielmehr Prüfungen vor, anhand derer er die notwendigen Maßnahmen selbst ermittelt.[208] Im Laufe der Verarbeitung besteht gleichwohl die Pflicht zu einer regelmäßigen Überprüfung und gegebenenfalls erforderlichen Anpassung der technischen und organisatorischen Maßnahmen.[209]

Diesen Anforderungen steht § 336 Abs. 2 Nr. 2 SGB V nicht entgegen. Denn dieser gibt lediglich vor, dass ein gewisser Sicherheitsstandard („hoch“) nicht unterschritten werden darf.

2.10. Ergebnis

Im Ergebnis kann festgestellt werden, dass die ePA weder hinsichtlich des Berechtigungsmanagements der unterschiedlichen Ausbaustufen noch hinsichtlich der Sicherheit des Authentifizierungsverfahrens der Datenschutz-Grundverordnung nach zu beanstanden ist. *Insofern ist die elektronischen Patientenakte in ihrer derzeitigen Ausgestaltung mit der DSGVO vereinbar.*

[206] Vgl. BfDI (2020a, S. 7 f); BfDI (2020a, o. S).
[207] Verordnung (EU) 910/2914.
[208] Vgl. so auch Böllhoff, Cornelius, et al. (2020, S. 50).
[209] Vgl. ebd.; Paal/Pauly/Martini, DSGVO, Art. 32 Rn. 56; Taeger/Gabel/Schultze-Melling, DSGVO, Art. 32 Rn. 13.

Versicherung	App	Berwertung (Distribution) (Anzahl Bewertungen)
AOKen	Mein Leben	2.5 (Apple) (206) 2.0 (Google) (323)
BARMER	eCare	3.6 (Apple) (48) 2.6 (Google) (92)
DAK	ePA	2.1 (Apple) (39) 2.0 (Google) (45)
IKK Classic	ePA	2.0 (Apple) (28) 1.6 (Google) (37)
KKH	ePA	2.1 (Apple) (25) N/A** (Google)
Knappschaft	Meine Gesundheit	3.6 (Apple) (54) 1.4 (Google) (155)
Mobil Krankenkasse	ePA	2.3 (Apple) (19) 1.7 (Google) (15)
SBK	Patientenakte	2.6 (Apple) (27) 2.6 (Google) (5)
Techniker Krankenkasse	TK-Safe*	4.8 (Apple) (197.492) 4.7 (Google) (52.961)

Stand 23.05.2021

Apple = App Store **Google = Google Play**
***App ging aus bestehender Gesundheitsakte hervor**
****App zum Zeitpunkt der Erhebung nicht im Store verfügbar**

Abbildung 11: Bewertungen ePA FdV (Krankenkassen >1.000.000 Versicherte)

Quelle: Eigene Darstellung

3. Fazit und Ausblick

Die vorliegende Arbeit zeigt, dass es verschiedene Anknüpfungspunkte für eine Prüfung der ePA mit europäischem Datenschutzrecht gibt. So wurde beispielsweise festgestellt, dass die Rolle des Verantwortlichen gemäß Art. 4 Nr. 7 DSGVO durch § 307 SGB V zwar ausführlich konkretisiert wird, es aber möglich erscheint, dass es doch zu Diskussionen kommen wird, beispielsweise in Bereichen der Schnittstelle zwischen TI und ePA-Aktensystemen.

Datensicherheit ist ein unerlässlich wichtiges Thema im Bereich der Verarbeitung von Gesundheitsdaten, daher ist der Gesetzgeber angehalten, die Standards entsprechend hoch zu halten. Hinsichtlich der ePA kann mit vorsichtigem Optimismus von einer sicheren Anwendung innerhalb der TI ausgegangen werden. Schwachstellen sind den Beteiligten bewusst und werden beseitigt.

Die Datenschutz-Folgenabschätzung hat im Angesicht ihrer wenig konkreten Ausgestaltung durch Art. 35 DSGVO das Potential für weitere Diskussionen zu sorgen. Jedoch betreffen die Pflichten aus Art. 35 DSGVO nicht die Rechtmäßigkeit eines Verarbeitungsvorgangs.

Hauptkritikpunkt des Bundesbeauftragten für Datenschutz und Informationsfreiheit ist das aus seiner Sicht defizitäre Berechtigungsmanagement. Der Schwerpunkt der Arbeit richtet sich an dieser Kritik aus. Es wird festgestellt, dass die Rechtsgrundlage der Datenverarbeitungen in der ePA im Regelfall die Einwilligung nach Art. 6 Abs. 1 Satz 1 lit. a bzw. Art. 9 Abs. 2 lit a DSGVO ist. Im Detail werden die Anforderungen des Art.4 Nr. 11 DSGVO geprüft. Der Freiwilligkeit entgegen steht weder eine Ungleichbehandlung von Personen, die die ePA nutzen und solchen, die es nicht tun, noch ein Ungleichgewicht im Arzt-Patienten-Verhältnis. Auch eine unzulässige Kopplung der Datenverarbeitung an andere Zwecke liegt nicht vor. Das fehlende feingranulare Berechtigungsmanagement in der ersten Ausbaustufe spricht nicht gegen die Anforderungen an die Bestimmtheit der Einwilligung. Dem Berechtigungsmanagement liegt insbesondere kein „Alles-oder-nichts-Prinzip“ zugrunde. Eine konkrete Anforderung an die Differenziertheit der Einwilligung lässt sich aus der DSGVO nicht ableiten. Ein Minus in der Granularität der Einwilligung sollte nach Ansicht des Verfassers durch ein Plus an Information und Transparenz ausgeglichen werden. Den Informationspflichten der DSGVO wird in der Sozialgesetzgebung und in der konkreten Ausgestaltung der Anwendungen hinreichend Rechnung getragen. Jedoch könnte eine anschaulichere Informationsvermittlung zu einer besseren Informiertheit und zu einem stärkeren Vertrauen des Versicherten in die Anwendung beitragen. Datenschutzgrundsätze nach Art. 5 DSGVO sind hinsichtlich des Erforderlichkeitsprinzips durch das undifferenzierte Rechtemanagement in der ersten Ausbaustufe zwar eingeschränkt; diese Einschränkung ist aber von der freiwilligen und informierten Einwilligung abgedeckt.

Die DSGVO schreibt keine konkreten Maßnahmen hinsichtlich der Datensicherheit vor. Die Ausgestaltung der Datensicherheit obliegt dem nationalen Gesetzgeber bzw. direkt dem Verantwortlichen durch Festlegung der technischen und organisatorischen Maßnahmen zur Risikovermeidung. Daher trifft die Kritik des BfDI hinsichtlich der alternativen Authen-

tifizierungsverfahren nicht zu. Eine differenzierte Auseinandersetzung mit den Sicherheitsstandards der ePA wäre ein interessantes Thema für eine weitere Ausarbeitung.

Wegen der eiligen Terminierung des Gesetzgebers trägt die ePA zu Beginn viele Softwarefehler in sich. Ein Blick in die Bewertungs- und Kommentarsektionen der Vertriebsplattformen von Apple und Google lässt vermuten, dass die Versicherten hier zu Beta-Testern gemacht werden (Abbildung 11). Vor allem scheinen Funktionalitäten und Dienste nicht zuverlässig verfügbar zu sein. Der Anzahl der Bewertungen im Verhältnis zu den Versicherten nach zu urteilen, stößt die ePA bei den Versicherten noch nicht auf große Resonanz.[210] Das mag auch daran liegen, dass die Krankenkassen die ePA derzeit nicht aktiv bewerben.

Auf der Leistungserbringerseite ist es für eine Bewertung der Testphase noch zu früh. Die Produkte der Konnektoren-Hersteller befinden sich derzeit noch in der Zulassungsprüfung.[211]

Fraglich ist indes das Vorgehen des BfDI. Er hat seine Kritik zwar schon frühzeitig geäußert, jedoch nie substantiiert dargelegt. Bezeichnend insofern ist auch der Verweis auf allgemeine Grundsätze (Art. 5, Art. 25, Art. 32 DSGVO) und politische Schlagworte („Datensouveränität“). Selbst die Warnung an die Krankenkassen enthält keine differenzierten Ausführungen zu den Kritikpunkten. Auf Nachfrage des Verfassers verwies die Behörde auf die öffentlich zugängliche Stellungnahme zum Entwurf des PDSG. Die Vorgehensweise des BfDI stieß angeblich auch in der eigenen Partei und in anderen Aufsichtsbehörden auf Kritik.[212] Ob der BfDI wie angekündigt[213] weitere Maßnahmen ergreifen wird, bleibt mit Spannung abzuwarten. Eine gerichtliche Klärung scheint dann nicht unwahrscheinlich.[214]

[210] Vgl. dazu auch golem.de (2021, o. S.); Klöckner, Jürgen, Olk, Julian (2021, o. S.)
[211] Vgl. Gesellschaft für Telematik (gematik) (2021d, o. S.)
[212] Vgl. Olk (2020a, o. S.)
[213] BfDI (2020a, S. 2); BfDI (2020c).
[214] Vgl. zur Befugnis des BAS als Rechtsaufsichtsbehörde der Krankenkassen: BAS, Stellungnahme zur elektronischen Patientenakte, S. 4.

Literatur

aerzteblatt.de Elektronische Patientenakte. (2020, Dezember). *Elektronische Patientenakte: Kassen warten mit Werbung ab.* Zugriff auf https://www.aerzteblatt.de/archiv/217189/Elektronische-Patientenakte-Kassen-warten-mit-Werbung-ab ([Zugriff 2021-05-15])

aerztezeitung. (2018). *TK-Versicherte erhalten E-Akte.* Zugriff am 2021-05-15 auf https://www.aerztezeitung.de/Politik/TK-Versicherte-erhalten-E-Akte-229937.html

aerztezeitung. (2020). *PKV bereitet sich auf ePA-Einstieg vor.* Zugriff am 2021-05-15 auf https://www.aerztezeitung.de/Wirtschaft/PKV-bereitet-sich-auf-ePA-Einstieg-vor-414315.html

aerztezeitung.de. (2018). *Neue Gesundheitsakte bringt GKV und PKV zusammen.* Zugriff auf https://www.aerztezeitung.de/Wirtschaft/Neue-Gesundheitsakte-bringt-GKV-und-PKV-zusammen-231694.html ([Zugriff 2021-05-15])

Artikel-29-Datenschutzgruppe . (2007). *Arbeitspapier zu elektronischen Patientenakten, 2007): Working Document on the processing of personal data relating to health in electronic health records (EHR), WP 131, Februar 2007.* Zugriff auf https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf

BfDI. (2019). *Liste der Verarbeitungsvorgänge gem. Art. 35 Abs. 4 DSGVO, 2019): Liste von Verarbeitungsvorgängen gemäß Artikel 35 Absatz 4 DSGVO für Verarbeitungstätigkeiten öffentlicher Stellen des Bundes, Oktober 2019.* Zugriff auf https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Liste_VerarbeitungsvorgaengeArt35.pdf?

BfDI. (2020a). *BfDI zu Folgen der Gesetzgebung des PDSG, Pressemitteilung vom 19. August 2020.* Zugriff am 2021-05-21 auf https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2020/20_BfDI-zu-PDSG.html

BfDI. (2020b). *Bundespressekonferenz vom 19.08.2020.* Zugriff am 2021-05-23 auf https://www.youtube.com/watch?v=vsLM8EPH9NY

BfDI. (2020c). *Bundespressekonferenz vom 19.08.2020.* Zugriff auf https://www.youtube.com/watch?v=vsLM8EPH9NY

BfDI. (2020a). *Schreiben an die LfDI, 2020): Weiteres Vorgehen nach dem Beschluss des Deutschen Bundestages zum PDSG am 3. Juli 2020, August 2020.* Zugriff auf https://www.bfdi.bund.de/DE/Infothek/Transparenz/AccessforoneAccessforall/2021/2020_Anschreiben-LfDs-PDSG.pdf?

BfDI. (2020b). *Stellungnahme zum PDSG, 2020): Stellungnahme [...] zum Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur, April 2020.* Zugriff auf https://www.bfdi.bund.de/DE/Infothek/Transparenz/Stellungnahmen/2020/StgN_Patientendaten-Schutz-Gesetz.pdf?

BfDI. (2020). *Stellungnahme [...] zur öffentlichen Anhörung [...] zum Entwurf eines Geset-zes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patienten-Datenschutz-Gesetz), Mai 2020.* Zugriff am 2021-05-15 auf https://www.bfdi.bund.de/DE/Infothek/Transparenz/Stellungnahmen/2020/StgN_Patienten-Datenschutz-Gesetz.pdf?

BfDI. (2020a). *Stellungnahme zur öffentlichen Anhörung zum PDSG, 2020): Stellungnahme [...] zur öffentlichen Anhörung [...] zum Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patienten-Datenschutz-Gesetz), Mai 2020.* Zugriff auf https://www.bfdi.bund.de/DE/Infothek/Transparenz/Stellungnahmen/2020/StgN_Patienten-Datenschutz-Gesetz.pdf?

BfDI. (2020b). *Warnung an die gesetzlichen Krankenkassen, 2020): Warnung nach Artikel 58 Abs. 2 Buchst. a) DSGVO, November 2020.* Zugriff auf https://www.bfdi.bund.de/DE/Infothek/Transparenz/Rundschreiben/Allgemein/2020/Warnung-Krankenkassen-ePA.pdf?

BfDI. (2020). *Warnung nach Artikel 58 Abs. 2 Buchst. a) DSGVO, November 2020.* Zugriff am 2021-05-15 auf https://www.bfdi.bund.de/DE/Infothek/Transparenz/Rundschreiben/Allgemein/2020/Warnung-Krankenkassen-ePA.pdf?

BfDI. (2021). *Zuständigkeit für gesetzliche Krankenkassen, 2021.* Zugriff auf https://www.bfdi.bund.de/DE/Datenschutz/Themen/Gesundheit_Soziales/KrankenkassenArtikel/Krankenkassen-Zust%C3%A4ndigkeit-BfDI.html?nn=5217154

Böllhoff, Cornelius, et al. (2020). *Vereinbarkeit der ePA mit europäischem Datenschutzrecht, 2020): Vereinbarkeit der Regelungen zur elektronischen Patientenakte (ePA) nach dem Patienten-Datenschutz-Gesetz (PDSG) mit europäischem Datenschutzrecht – Rechtsgutachten im Auftrag des health innovation hub, November 2020.* Zugriff auf https://hih-2025.de/wp-content/uploads/2021/02/Redeker_Rechtsgutachten_ePA.pdf

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2018). *Technische Richtlinie TR-03147, 2018): Technische Richtlinie TR-03147 Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen, Dezember 2018.* Zugriff auf https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03147/TR03147.pdf

Bundesärztekammer. (2020a). *Stellungnahme der Bundesärztekammer zum Referentenentwurf eines Gesetzes zum Schutz elektronischer Patientenakten in der Telematikinfrastruktur.* Zugriff am 2021-05-15 auf https://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/Stellungnahmen/SN_BAEK__PDSG_25022020.pdf

Bundesärztekammer. (2020b). *Stellungnahme zum PDSG, 2020): Stellungnahme der Bundesärztekammer zum Referentenentwurf eines Gesetzes zum Schutz elektronischer Patientenakten in der Telematikinfrastruktur, Februar 2020.* Zugriff auf https://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/Stellungnahmen/SN_BAEK__PDSG_25022020.pdf

Bundesministerium für Gesundheit (BMG). (2019). *TSVG, 2019): Terminservice- und Versorgungsgesetz (TSVG).* Zugriff auf https://www.bundesgesundheitsministerium.de/terminservice-und-versorgungsgesetz.html

Bundesministerium für Gesundheit (BMG). (2021, März). *Online-Ratgeber Krankenversicherung, 2021): Versicherte in der gesetzlichen Krankenversicherung.* Zugriff auf https://www.bundesgesundheitsministerium.de/gesetzlich-versicherte.html

DAK. (2021). *Datenschutzhinweise für die elektronische Patientenakte (ePA), 2021.* Zugriff auf https://www.dak.de/dak/unternehmen/datenschutzhinweise-fuer-die-elektronische-patientenakte-epa-2377742.html#/

Gematik. (2021a). *ePA-Aktensyteme.* Zugriff am 2021-05-15 auf https://fachportal.gematik.de/hersteller-anbieter/komponenten-dienste/epa-frontend-des-versicherten

Gematik. (2021b). *E-Patientenakte.* Zugriff am 2021-05-15 auf https://www.gematik.de/anwendungen/e-patientenakte/

Gematik. (2021c). *Zulassungsübersicht.* Zugriff am 2021-05-15 auf https://fachportal.gematik.de/zulassungs-bestaetigungsuebersichten

Gesellschaft für Telematik (gematik). (2019). *Systemspezifisches Konzept ePA, Oktober 2019.* Zugriff auf https://www.vesta-gematik.de/standard/formhandler/324/gemSysL_ePA_V1_3_0.pdf

Gesellschaft für Telematik (gematik). (2020a). *Gesellschafteranteile, 2020.* Zugriff auf https://www.gematik.de/news/news/welcome-pkv-wird-gesellschafter-der-gematik/

Gesellschaft für Telematik (gematik). (2020b). *Informationsblatt Sicherheits- und Produktgutachten, Mai 2020.* Zugriff auf https://fachportal.gematik.de/fileadmin/Fachportal/Downloadcenter/Informationen_fuer_Gutachter/gemInfo_Gutachter_ePA-FdV.pdf

Gesellschaft für Telematik (gematik). (2020c). *Richtlinie zur Prüfung der Sicherheitseignung, April 2020.* Zugriff auf https://fachportal.gematik.de/fileadmin/user_upload/fachportal/files/Service/Sicherheitsgutachten/gemRL_PruefSichEig_DS_V2.1.0.pdf

Gesellschaft für Telematik (gematik). (2020d). *Vorwort zum Gutachten der TU Graz, 2020): Vorwort zum Gutachten der TU Graz zur Sicherheitsanalyse der Kernkomponenten der elektronischen Patientenakte (ePA).* Zugriff auf https://www.gematik.de/fileadmin/user_upload/MediaUploads/Sicherheitsanalyse_TU_Graz

_zur_ePA_mit_Vorwort_der_gematik.pdf

Gesellschaft für Telematik (gematik). (2021a). *ePA-Aktensyteme, 2021*. Zugriff auf https://fachportal.gematik.de/hersteller-anbieter/komponenten-dienste/epa-aktensystem

Gesellschaft für Telematik (gematik). (2021b). *ePA-Frontend des Versicherten, 2021*. Zugriff auf https://fachportal.gematik.de/hersteller-anbieter/komponenten-dienste/epa-frontend-des-versicherten

Gesellschaft für Telematik (gematik). (2021c). *E-Patientenakte, 2021*. Zugriff auf https://www.gematik.de/anwendungen/e-patientenakte/

Gesellschaft für Telematik (gematik). (2021d). *Erste Bilanz der Testphase, 2021*. Zugriff auf https://www.gematik.de/news/news/elektronische-patientenakte-in-der-testphase-konnektorhersteller-ziehen-erste-bilanz/

Gesellschaft für Telematik (gematik). (2021e). *Gesetzliche Grundlagen, 2021*. Zugriff auf https://www.gematik.de/ueber-uns/gesetzliche-grundlagen/

Gesellschaft für Telematik (gematik). (2021f). *KTR-Consumer, 2021*. Zugriff auf https://fachportal.gematik.de/hersteller-anbieter/komponenten-dienste/ktr-consumer

Gesellschaft für Telematik (gematik). (2021g). *Spezifikation ePA-Aktensystem, Februar 2021*. Zugriff auf https://fachportal.gematik.de/fachportal-import/files/gemSpec_Aktensystem_V1.7.0_Aend.pdf

Gesellschaft für Telematik (gematik). (2021h). *Spezifikation ePA-Frontend des Versicherten, Februar 2021*. Zugriff auf https://fachportal.gematik.de/fachportal-import/files/gemSpec_ePA_FdV_V1.8.0_Aend.pdf

Gesellschaft für Telematik (gematik). (2021i). *Telematikinfrastruktur (Glossar), 2021*. Zugriff auf https://www.gematik.de/glossar/begriffe/telematikinfrastruktur/397/

GKV-Spitzenverband. (2020a). *Informationen zur elektronischen Patientenakte): Informationen zur elektronischen Patientenakte (ePA) nach § 343 SGB V, November 2020*. Zugriff auf https://www.aok.de/pk/fileadmin/user_upload/Universell/05-Content-PDF/RS_2020-852_Anlage_01_-_mit_AOK_Anpassung_ITSG_GKV-SV.pdf

GKV-Spitzenverband. (2020b). *Stellungnahme zum PDSG, 2020): Stellungnahme des GKV-Spitzenverbandes vom 19.05.2020 zum Gesetzesentwurf [. . .] – PDSG vom 31.03.2020, Mai 2020*. Zugriff auf https://www.gkv-spitzenverband.de/media/dokumente/presse/p_stellungnahmen/200519_Stellungnahme_GKV-SV_PDSG_Gesetzentwurf.pdf

golem.de. (2021). *Die Patientenakte auf dem Smartphone bleibt ungeöffnet*. Zugriff auf https://www.golem.de/news/telemedizin-die-patientenakte-auf-dem-smartphone-bleibt-ungeoeffnet-2103-154751.html

Golland, A. (2018). Das Kopplungsverbot in der Datenschutz-Grundverordnung – Anwendungsbe-reich, ökonomische Auswirkungen auf Web 2.0-Dienste und Lösungsvorschlag. *Multimedia und Recht*, 130–135.

Hof, H.-J. (2020). Datenschutz mittels IT-Sicherheit. In M.-T. Tinnefeld, B. Buchner & et al. (Hrsg.), *Einführung in das Datenschutzrecht – Datenschutz und Informationssicherheit in europäischer Sicht, 7. Auflage*. de Gruyter.

Jäschke, T. & Hacks, S. (2016). Einführung Datenschutz im Gesundheitswesen. In T. Jäschke (Hrsg.), *Datenschutz im Gesundheitswesen: Grundlagen, Konzepte und Umsetzung* (S. 2–17). Medizinisch Wissenschaftliche Verlagsgesellschaft (MWV).

Jorzig, A. & Sarangi, F. (2020). Digitalisierung im Gesundheitswesen – Ein kompakter Streifzug durch Recht. *Technik und Ethik*.

Kassenärztliche Bundesvereinigung (KBV). (2020). *Statistische Informationen aus dem Bundesarztregister*. Zugriff am 2021-05-15 auf https://www.kbv.de/media/sp/2020-12-31_BAR_Statistik.pdf

KBV. (2020). *Richtlinie zur Zertifizierung nach § 75b Absatz 5 SGB V, Mai 2020*. Zugriff auf https://www.kbv.de/media/sp/RiLi___75b_Abs._5_SGB_V_Zertifizierung.pdf

Klöckner, J. & Olk, J. (2021). Geteiltes Bild zur elektronischen Patientenakte bei den Versicherten. *Handelsblatt*.

Klöckner, Jürgen, Olk, Julian. (2021). *Geteiltes Bild zur ePA, 2021): Geteiltes Bild zur elektronischen Patientenakte bei den Versicherten, Januar 2021*. Zugriff auf https://www.handelsblatt.com/inside/digital_health/umfrage-geteiltes-bild-zur-elektronischen-patientenakte-bei-den-versicherten/26774244.html

Koch, M. & Henke, M. (2016). Datenschutz in der Telematikinfrastruktur. In T. Jäschke (Hrsg.), *Datenschutz im Gesundheitswesen: Grundlagen, Konzepte und Umsetzung* (S. 309–322). Medizinisch Wissenschaftliche Verlagsgesellschaft (MWV).

netzpolitik.org. (2020). *Jens Spahn hat es eilig, Oktober 2020*. Zugriff auf https://netzpolitik.org/2020/jens-spahn-hat-es-eilig/

Olk, J. (2020a). *Breite Front stellt sich hinter Jens Spahn*. Zugriff auf https://www.handelsblatt.com/inside/digital_health/streit-um-digitale-patientenakte-breite-front-stellt-sich-hinter-jens-spahn/26732890.html?ticket=ST-3044829-txdeZGvwodaQPYTHWmle-ap5

Olk, J. (2020b). *Private Krankenversicherung will wieder an gesetzlicher Digitalisierung teilhaben*. Zugriff auf https://www.handelsblatt.com/politik/deutschland/rueckkehr-zur-gematik-private-krankenversicherung-will-wieder-an-gesetzlicher-digitalisierung-teilhaben/25592704.html?ticket=ST-6959017-lRb22uKapYhKAnwchnMk-ap4

Otto, D. & Rüdlin, M. (2017). Standardisierung von Patienteneinwilligungen im Krankenhaus. *Zeitschrift für Datenschutz*, 519–524.

PKV Verband der Privaten Krankenversicherung. (2020). *PKV und eHealth*. Zugriff auf https://www.pkv.de/verband/presse/pressemitteilungen/gemeinsame-pressemitteilung-einheitliche-digitale-infrastruktur-fuer-das-gesundheitswesen/

Slany, W. (2020). *ePA Sicherheitsanalyse der TU Graz, 2020): Sicherheitsanalyse zur Sicherheit der kritischen Komponenten der elektronischen Patientenakte nach §291a SGB V – Fokus auf VAU und kryptographische Sicherheitsleistung SGD, 03.03.2020*. Zugriff auf https://www.gematik.de/fileadmin/user_upload/MediaUploads/Sicherheitsanalyse_TU_Graz_zur_ePA_mit_Vorwort_der_gematik.pdf

Stöferle, B. (2016). Kooperations- und Kommunikationspartner aus Anwendersicht. In T. Jäschke (Hrsg.), *Datenschutz im Gesundheitswesen: Grundlagen, Konzepte und Umsetzung* (S. 135–161). Medizinisch Wissenschaftliche Verlagsgesellschaft (MWV).

sueddeutsche.de. (2020). *Interview mit Christoph Saatjohann zur ePA, 2020): „Ich bin vorsichtig optimistisch“*. Zugriff auf https://www.sueddeutsche.de/digital/elektronische-patientenakte-epa-gesundheit-it-sicherheit-1.5159783

tagesschau.de. (2020). *IT-Sicherheitslücken in Praxen*. Zugriff auf https://www.tagesschau.de/investigativ/br-recherche/sicherheit-telematik-101.html

v. Brocke, Jan, Simons, Alexander, et. al. (2009). *Reconstructing the Giant, 2009): Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process, 2009*. Zugriff auf https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1145&context=ecis2009

Verbraucherzentrale, v. (2020). *Digitalisierung im Gesundheitswesen muss allen offenstehen*. Zugriff auf https://www.vzbv.de/meldungen/digitalisierung-im-gesundheitswesen-muss-allen-offenstehen