Christoph Krönke, Elissa Tschachler*

Ein Opt-out für die elektronische Patientenakte (ePA)

Entfaltung und Bewertung von Gestaltungsoptionen eines Opt-out-Systems für die Nutzung der ePA zu Versorgungszwecken aus datenschutzrechtlicher Perspektive

Die 2021 eingeführte ePA sollte die Gesundheitsversorgung in Deutschland in das digitale Zeitalter überführen. Dabei blieben allerdings substanzielle datenschutzrechtliche Gestaltungsspielräume ungenutzt. Dies betrifft vor allem die vergleichsweise umständliche Ausgestaltung der ePA als strenges Opt-in-Modell. Die Einführung eines Opt-out-Systems für die ePA wird daher in Ansehung des Ziels einer effizienten und effektiven Gesundheitsversorgung sowohl in gesundheitswissenschaftlichen Fachkreisen als auch im Ende 2021 geschlossenen Koalitionsvertrag der amtierenden Bundesregierung als geboten erachtet. Der vorliegende Beitrag zeigt auf, welche denkbaren Gestaltungsoptionen dem deutschen Gesetzgeber bei der Einführung eines solchen Opt-out-Modells nach Maßgabe der Datenschutzgrundverordnung (DSGVO) sowie der grundrechtlichen Datenschutzgewährleistungen zur Verfügung stehen.

Prof. Dr. Christoph Krönke

Universitätsprofessor für Öffentliches Recht und Vorstand des Instituts für Öffentliches Recht, Nachhaltigkeits- und Technologierecht (IONTech) an der Wirtschaftsuniversität Wien (WU).

E-Mail: christoph.kroenke@wu.ac.at

Elissa Tschachler, LL.M. (WU)

Universitätsassistentin (prae doc) am Institut für Öffentliches Recht, Nachhaltigkeits- und Technologierecht (IONTech) an der Wirtschaftsuniversität Wien (WU).

E-Mail: elissa.tschachler@wu.ac.at

1 Einführung: Opt-out ist nicht gleich Opt-out

Mit dem 1. Januar 2021 wurde die ePA als Angebot für die rund 73 Millionen gesetzlich Versicherten in Deutschland eingeführt.[1] Entsprechend der gesetzlichen Definition in § 341 Abs. 1 SGB V handelt es sich bei der ePA um eine versichertengeführte elekt-

* Der Beitrag gibt wesentliche Erkenntnisse einer rechtswissenschaftlichen Studie wieder, die von Christoph Krönke im Auftrag der Bertelsmann Stiftung und der Stiftung Münch angefertigt wurde, unter Mitwirkung von Elissa Tschachler. Die vollständige Studie wird unter dem Titel „Opt-out-Modelle für die elektronische Patientenakte (ePA) aus datenschutzrechtlicher Perspektive" selbständig veröffentlicht.

1 Im Rahmen eines „3-Phasen-Modells" umfasste die sog. erste Einführungs- und Testphase ab dem 1. Januar 2021 die Zurverfügungstellung einer App zum Download auf ein Smartphone oder Tablet, mit den in § 342 Abs. 2 Nr. 1 SGB V bezeichneten Funktionalitäten. Mit 1. Januar 2022 begann die zweite Phase, wodurch Nutzer mit einem eigenen Endgerät im Rahmen eines „feingranularen Berechtigungsmanagements" die Zugriffe von Leistungserbringern in Bezug auf spezifische Dokumente und Datensätze regeln können sollen. Ab 1. Januar 2023 soll die dritte und letzte Phase eingeleitet werden, in der alle Erweiterungsschritte vollzogen und das volle Potential der ePA ausgeschöpft sein sollen, einschließlich der Möglichkeit zur Weiterleitung von Daten zu Forschungszwecken (§ 363 SGB V – sog. „Datenspende"). Näheres siehe in der rechtsvergleichenden Studie im Auftrag der Stiftung Münch von C. Krönke/V. Aichstill, in: Stiftung Münch (Hrsg.), Die elektronische Patientenakte und das europäische Datenschutzrecht, 2021, S. 9 ff.

ronische Akte, die den Versicherten von den Krankenkassen auf Antrag zur Verfügung gestellt werden muss. Dabei wurde die ePA vom deutschen Gesetzgeber unter das Banner der größtmöglichen Patientensouveränität gestellt. Diesem Leitbild hat der Gesetzgeber vor allem Rechnung getragen, indem er nahezu sämtliche Nutzungen der ePA von einer Einwilligung durch die einzelnen Versicherten abhängig gemacht hat. Insbesondere darf die ePA nur dann eingerichtet und mit Gesundheitsdaten „befüllt" werden, wenn der/die einzelne Versicherte aktiv geworden ist und seine Einwilligung dazu erteilt hat (sog. „Opt-in"). Im Gegensatz zu einem sog. „Opt-out"-Modell, wie es im Bereich der Gesundheitsdatennutzung zu Versorgungszwecken in einigen anderen EU-Mitgliedstaaten (z.B. in Österreich, Spanien, Estland)[2] vorgesehen ist, bietet das derzeitige Regelungskonzept in Deutschland keine Möglichkeit zu einer automatischen Einspeisung von Informationen in die ePA, der die Versicherten entgegentreten müssten. Die Nutzbarkeit einer ePA ist somit zwingend auf das aktive Tätigwerden des einzelnen Versicherten angewiesen. Neben der Einrichtung und Befüllung der ePA betrifft dies außerdem – in persönlicher Hinsicht – auch die Zugriffsberechtigung der einzelnen Leistungserbringer, die einer gesonderten Einwilligung bedarf, sowie – in sachlicher Hinsicht – die ebenfalls einwilligungspflichtige Auslesbarkeit von in der ePA abgespeicherten Informationen.

Diese gegenwärtige, vergleichsweise umständliche Ausgestaltung der ePA als „Einwilligungskaskade" ist im Schrifttum – zu Recht – auf Kritik gestoßen.[3] Denn das Einwilligungssystem entspricht insbesondere nicht der Idee eines fach- und sektorenübergreifenden Behandelns durch mehrere Leistungserbringer, gegebenenfalls über einen längeren Zeitraum. Bei dem derzeitigen Einwilligungsverfahren sei unter anderem zu befürchten, „dass selbst bei teilnahmewilligen[4] Patientinnen und Patienten ein vollständiger Datenbestand der ePA häufig nicht zustande kommt, weil die Überlagerung von multiplen Einwilligungen dieses Ergebnis unwahrscheinlich macht."[5]

Erst jüngsthin betonte auch der Corona-Expertenrat der Bundesregierung, dass Deutschland eine umfassende Digitalisierung des Gesundheitswesens benötige, und verlangte, die Einführung der ePA „mit höchster Priorität" umzusetzen. Das Gremium mahnte an, dass „eine weitere Verzögerung der 2003 beschlossenen und gesetzlich verankerten elektronischen Patientenakte […] nicht mehr mit einem modernen Gesundheitswesen und Pandemiemanagement vereinbar" sei.[6]

Die an der gegenwärtigen Ausgestaltung der ePA geäußerte Kritik hat offenbar Gehör seitens der Bundesregierung gefunden. Denn der Koalitionsvertrag 2021-2025 „Mehr Fortschritt wagen – Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit" zwischen SPD, Bündnis 90/Die Grünen und FDP enthält auf Seite 83 folgenden Vorsatz zur künftigen Umgestaltung der ePA und zur Nutzung von Gesundheitsdaten:

> *„Wir beschleunigen die Einführung der […] ePA und des E-Rezeptes sowie deren nutzenbringende Anwendung […] Alle Versicherten bekommen DSGVO-konform eine ePA zur Verfügung gestellt; ihre Nutzung ist freiwillig (opt-out).*"

Mit diesen Festlegungen ist freilich noch keineswegs entschieden, wie der Opt-out für die ePA im Einzelnen ausgestaltet werden soll. Gerade der Blick in andere Mitgliedstaaten der Europäischen Union zeigt, dass „Opt-out nicht gleich Opt-out" ist, sondern durchaus unterschiedliche Opt-out-Varianten denkbar sind und existieren. Bei der Einführung eines Opt-out-Systems für eine ePA bestehen mithin diverse Ausgestaltungsspielräume, von denen ein Gesetzgeber Gebrauch machen kann – aber nicht muss.

Vor diesem Hintergrund möchten wir im Folgenden die Möglichkeiten zur Ausgestaltung von Opt-out-Modellen für die ePA-Nutzung zu Versorgungszwecken aufzeigen, die sich im Rahmen der *Vorgaben des europäischen Datenschutzrechts* sowie *grundrechtlicher Datenschutzgehalte* – dazu sogleich im Überblick unter Punkt 2 – bewegen. Konkret betreffen diese vor allem die *Anlage und Befüllung der ePA* (3) sowie den Zugriff darauf, respektive die *Berechtigung zum Zugriff auf die ePA* (4) einerseits sowie *einzelne abrufbare Inhalte der ePA* (5) andererseits.

2 Unions- und verfassungsrechtlicher Rahmen der ePA

Die in Deutschland geltenden rechtlichen Maßstäbe für die Verarbeitung von personenbezogenen Daten werden in erster Linie durch die *DSGVO*[7] gesetzt, die seit ihrem Inkrafttreten am 25. Mai 2018 unmittelbar geltendes Recht in den Mitgliedstaaten ist, so auch in Deutschland. Sie ist der wesentliche rechtliche Maßstab für die nachstehenden Darlegungen (dazu sogleich 2.1).

Sowohl die DSGVO als auch die speziellen datenschutzrechtlichen Sekundärrechtsakte sind dabei „primärrechtskonform" unter Beachtung der Vorgaben aus Art. 7 und Art 8 der *GRC* sowie aus Art 16 Abs. 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) auszulegen und anzuwenden. Da sich die wichtigsten spezifischen datenschutzrechtlichen Maßstäbe freilich nicht aus dem primär-, sondern aus dem sekundärrechtlichen Unionsrecht ergeben, sind unionsgrundrechtliche Erwägungen bei der Auslotung von Gestaltungsoptionen für die ePA lediglich ergänzend heranzuziehen. Gleiches gilt für die zur Anwendung kommenden grundrechtlichen Gehalte des Grundgesetzes, insbesondere des *Rechts auf informationelle Selbstbestimmung* (dazu 2.2).

2 Vgl. zu den Systemen dieser Mitgliedstaaten C. Krönke/V. Aichstill, in: Stiftung Münch (Hrsg.), Die elektronische Patientenakte und das europäische Datenschutzrecht, 2021, S. 29 ff.

3 Vgl. beispielhaft den Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen, Digitalisierung für Gesundheit. Ziele und Rahmenbedingungen eines dynamisch lernenden Gesundheitssystems, 2021, S. 86, verfügbar unter https://www.svr-gesundheit.de/fileadmin/Gutachten/Gutachten_2021/SVR_Gutachten_2021.pdf.

4 Erwähnenswert in diesem Zusammenhang ist allerdings, dass mit Stand November 2021 lediglich ein Fünftel der Versicherten die ePA ihrer Krankenkasse überhaupt kennen. Vgl. gematik GmbH (Hrsg.), Atlas zur Telematikinfrastruktur. Zahlen. Daten. Fakten, 2021, S. 5, verfügbar unter https://www.gematik.de/fileadmin/user_upload/gematik/images/TI-Atlas/gematik_TI-Atlas_web_202111_.pdf.

5 Siehe neben dem Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen, Digitalisierung für Gesundheit. Ziele und Rahmenbedingungen eines dynamisch lernenden Gesundheitssystems, 2021, S. 85 ff., ebenso C. Krönke/ V. Aichstill, in: Stiftung Münch (Hrsg.), Die elektronische Patientenakte und das europäische Datenschutzrecht, 2021, S. 96.

6 Hierbei wurde eine einhellige Zustimmung (19/19) im ExpertInnenrat erlangt. Vgl. ExpertInnenrat der Bundesregierung zu COVID-19, 4. Stellungnahme zu dringenden Maßnahmen für eine verbesserte Datenerhebung und Digitalisierung, 2022, S. 2, verfügbar unter https://www.bundesregierung.de/resource/blob/974430/2000794/f189a6b7b0f581965f746e957db90af7/2022-01-22-nr-4ex-pertenrat-data.pdf?download=1.

7 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119/1 vom 4. Mai 2016, S. 1-88.

2.1 Datenschutzgrundverordnung

Im Rahmen von medizinischen Behandlungen weisen nahezu alle Informationen einen Personen- und Gesundheitsbezug auf und machen die dahinterstehende Person zumindest „identifizierbar" im Sinne des Art. 4 Nr. 1 DSGVO; es handelt sich mithin um personenbezogene Daten. Die wesentlichen Arbeitsschritte im Umgang mit der ePA (Erheben, Erfassen, Speichern, Verändern, Abfragen, Verwenden, Übermitteln, Löschen usw.) stellen dabei Verarbeitungen im Sinne von Art. 4 Nr. 2 DSGVO dar.

Zudem handelt es sich bei den in den ePA dargestellten Informationen überwiegend um *Gesundheitsdaten* im Sinne des Art. 4 Nr. 15 DSGVO[8]. Als Informationen „höchstpersönlicher" Natur mit (kontextbedingt) besonders hohem Schadens- sowie Diskriminierungspotenzial[9] und zudem sehr ausgeprägter Identifikationskraft[10] unterliegen die ePA-Daten daher besonders strikten Vorgaben – sei es beim (1) „Ob" der Verarbeitung oder beim (2) „Wie" der Verarbeitungsmodalitäten. Insbesondere werden die *engeren Verarbeitungstatbestände in Art. 9 DSGVO* aktiviert, die bereits beim „Ob" der Gesundheitsdatenverarbeitung striktere Grenzen ziehen als die in Art. 6 DSGVO verankerten Regelungen zur „Rechtmäßigkeit der Datenverarbeitung".

Ob die DSGVO auf die Verarbeitung von Daten im Zusammenhang mit digitalen Anwendungen im Gesundheitswesen wie der ePA, der eGK oder der TI unmittelbar zur Anwendung gelangt, wird mit Rücksicht auf die gemäß Art. 16 Abs. 2 Satz 1 AEUV auf den *Anwendungsbereich des Unionsrechts* begrenzte datenschutzrechtliche Regelungskompetenz des Unionsgesetzgebers teilweise bestritten.[11] Dies kann vorliegend letztlich offenbleiben, da die DSGVO jedenfalls mittelbar über die Verweisung in § 35 Abs. 2 Satz 2 SGB I Anwendung findet.[12] Die Regelungen der DSGVO bilden somit in jedem Falle die wesentlichen rechtlichen Maßstäbe für die Ausgestaltung der ePA. Sie statuieren, wie in den Abschnitten 3 bis 5 im Einzelnen zu zeigen ist, konkrete *Anforderungen* an das *„Ob"* und das *„Wie"* der Verarbeitung von Gesundheitsdaten im Zusammenhang mit der ePA.

2.2 Grundrechtliche Gewährleistungen

Ebenfalls von Relevanz sind über die Einzelbestimmungen der DSGVO hinaus auch grundrechtliche Datenschutzgewährleistungen. Soweit die Bestimmungen der DSGVO dem nationalen Gesetzgeber nämlich Gestaltungsspielräume belassen – etwa wenn Art. 9 Abs. 2 lit. g) DSGVO gesetzliche Grundlagen zur Verarbeitung von Daten aus Gründen eines erheblichen öffentlichen Interesses gestattet und diese Grundlage unter den Vorbehalt eines angemessenen Verhältnisses zu dem verfolgten Ziel stellt –, sind bei der Ausfüllung dieser Spielräume vor allem auch grundrechtliche Wertungen des Grundgesetzes sowie der Charta der Grundrechte der Europäischen Union (GRC) zu beachten[13] – allen voran das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG[14]) und das Recht auf Leben und körperliche Unversehrtheit (Art. 2 Abs. 2 Satz 1 GG) sowie Art. 7 und 8 GRC. Hierbei ist freilich darauf hinzuweisen, dass mit Blick auf die Verarbeitung von Gesundheitsdaten in der ePA sich aus Art. 7 und 8 GRC, soweit ersichtlich, keine weitergehenden Gewährleistungen als aus dem grundgesetzlichen Recht auf informationelle Selbstbestimmung ergeben.[15]

Des Weiteren gilt es in diesem Zusammenhang zu beachten, dass das Recht auf informationelle Selbstbestimmung nicht nur als ein (negatives) *Abwehrrecht* gegen die Verarbeitung der eigenen Gesundheitsdaten in der ePA in Stellung gebracht werden muss, sondern auch als ein (positives) *Recht auf Gesundheitsdatenverarbeitung* interpretiert werden kann, das es dem Berechtigten überhaupt erst ermöglicht, seine Gesundheitsdaten selbstbestimmt zu nutzen bzw. für eine Behandlung zur Verfügung zu stellen.

Dieses auch positiv konnotierte Recht korrespondiert mit der vielzitierten *Patientensouveränität*: Um das letztlich im Recht auf Leben und körperliche Unversehrtheit aus Art. 2 Abs. 2 Satz 1 GG wurzelnde Selbstbestimmungsrecht bezüglich der eigenen Gesundheit[16] im Krankheitsfall überhaupt effektiv nutzen zu können, bedarf es vielfach einer hinreichenden informationellen Grundlage, die bereits im Vorfeld in sorgfältiger und möglichst vollständiger Weise zusammengetragen worden ist – gegebenenfalls und unter Effizienz- bzw. Effektivitätsgesichtspunkten auch ohne aktives Zutun des Patienten, im Rahmen eines ePA-Systems mit Opt-out-Elementen. Eine möglichst effiziente und effektive, gleichzeitig aber auch informationssichere Gesundheitsversorgung kann ein autonomiesichernd ausgestaltetes Opt-out-Modell somit nicht nur unter dem Gesichtspunkt der Wirksamkeit des Patientenaktensystems legitimieren, sondern auch unter

8 Für die vorliegende Darlegung erweisen sich insbesondere die sog. „unmittelbaren Gesundheitsdaten als Gesundheitsdaten im engeren Sinne" von Relevanz, weshalb diese vordergründig angesprochen sind. Diese umfassen unter anderem Befunde, Diagnosen etc. Unter den „mittelbaren Gesundheitsdaten als Gesundheitsdaten im weiteren Sinne" sind beispielsweise die Schulreife, die Haftfähigkeit oder Schuldfähigkeit gemeint. Letztere werden folglich aufgrund mangelnder Relevanz für die ePA nicht angesprochen, wenn die Rede von „Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DSGVO" ist. Vgl. bezüglich der Unterscheidung J. Geiger, in: S. Weth/M. Herberger/M. Wächter/C. Sorge (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Auflage 2019, Rn. 1 ff.; siehe ebenso in J. Eichenhofer, NVwZ 2021, 1090 (1092); vgl. zudem Erwägungsgrund 35 DSGVO.

9 Vgl. statt vieler etwa M. Frenzel, in: B. Paal/D. A. Pauly (Hrsg.), DSGVO BDSG, 3. Aufl. 2021, Art. 9 Rn. 6 ff.

10 Vom eigenen körperlichen Zustand kann sich der Einzelne typischerweise kaum befreien, diesbezügliche Informationen ermöglichen regelmäßig eine genaue Bestimmung der dazugehörigen Person.

11 Vgl. etwa M. Schröder, in: R. Streinz (Hrsg.), EUV/AEUV, 3. Aufl. 2018, Art. 16 AEUV Rn. 9 mwN; für das Gesundheitswesen C. Dochow, GesR 2016, 401 (403).

12 Vgl. ebenso offenlassend im Kontext der datenschutzrechtlichen Beurteilung der Regelungen über die eGK etwa BSG, Urteil vom 20.1.2021, B 1 KR 7/20 R, Rn. 25 ff.

13 Vgl. dazu und zum Folgenden BVerfG, 6.11.2019 – 1 BvR 16/13 (1. Leitsatz). Das Bundesverfassungsgericht hat in seinem Beschluss „Recht auf Vergessen I" (2019) gerade in Bezug auf eine datenschutzrechtliche Konstellation entschieden, dass mitgliedstaatliches Recht auch dann, wenn es der Durchführung von Unionsrecht dient, primär am Maßstab des Grundgesetzes zu messen ist, soweit es unionsrechtlich nicht vollständig determiniert ist.

14 Vgl. auch J. Eichenhofer, NVwZ 2021, 1090 (1093 f.). Der Einzelne soll demnach „selbst über die Preisgabe und Verwendung seiner persönlichen Daten […] bestimmen" können, mit der Folge, dass die Grundrechtsträger grundsätzlich stets wissen können müssen, „wer was wann und bei welcher Gelegenheit über sie weiß", BVerfGE 65, 1 (Rn. 146 f.). Vor diesem Hintergrund erweisen sich alle Regelungen, die die Nutzung von Gesundheitsdaten erlauben, als Grundrechtseingriffe, die einer Rechtfertigung bedürfen. Das informationelle Selbstbestimmungsrecht wird dabei freilich nicht grenzenlos gewährleistet, sondern lässt sich unter gewissen Voraussetzungen und in bestimmten Grenzen seinerseits einschränken.

15 Vgl. ebenso, wiederum zu den Regelungen zur eGK, in bemerkenswerter Knappheit BSG, Urteil vom 20.1.2021, B 1 KR 7/20 R, Rn. 107 ff., insb. Rn. 110: „Auch diesen Anforderungen, die sich mit denen des GG im Wesentlichen decken, werden die entscheidungserheblichen Regelungen zur eGK gerecht".

16 Vgl. zu dem aus Art. 2 Abs. 2 Satz 1 GG folgenden Selbstbestimmungsrecht nur BVerfGE 128, 282 (Rn. 39 ff.), im Kontext von Zwangsbehandlungen.

dem Aspekt der Patientensouveränität. Diese beiden Prinzipien sollten insoweit keineswegs nur als gegenläufige Regelungszwecke begriffen werden.

3 Anlage und Befüllung der ePA

Vor dem Hintergrund dieser rechtlichen Rahmenbedingungen lässt sich im Folgenden aufzeigen, wie sich ein Opt-out-Konzept bei der Ausgestaltung der einzelnen Phasen der ePA-Nutzung zu Versorgungszwecken umsetzen lässt und jeweils datenschutzrechtlich zu bewerten ist. Der logisch erste Schritt der Nutzung einer ePA ist die Anlage der Patientenakte als solche, im Sinne eines leeren virtuellen „Aktenordners". Damit verbunden sind zwar in aller Regel keine Verarbeitungen von Gesundheitsdaten, wohl aber von sonstigen personenbezogenen Daten (wie z.B. Stammdaten). Da es aus der Perspektive einer effektiven ePA wenig sinnvoll erscheint, einen Opt-out lediglich für die Anlage, nicht aber für die Befüllung der ePA vorzusehen, sollen gemeinsam mit den Varianten für die Einrichtung zugleich auch die Gestaltungsoptionen für einen Opt-out bei der Befüllung der ePA berücksichtigt werden.

3.1 Wesentliche denkbare Gestaltungsoptionen

Bei der Ausgestaltung der Anlage und *Befüllung* der ePA im Rahmen eines Opt-out-Modells – also unabhängig von einer Einwilligung des Patienten – könnte der deutsche Gesetzgeber im Wesentlichen folgende *drei Gestaltungsentscheidungen* treffen: Er könnte (1) die automatische, einwilligungsunabhängige Anlage und Befüllung an ein gesondertes *Registrierungserfordernis* für den Patienten knüpfen oder auf eine Registrierungspflicht verzichten. Er könnte (2) ferner, im Zuge einer *„All-in"-Lösung*, unterschiedslos alle Gesundheitsdaten in der ePA speichern lassen oder eine *differenzierte Befüllung* vorsehen, wobei bestimmte, besonders sensible Informationen (z.B. bzgl. einer HIV-Infektion oder einer psychischen Erkrankung) nur unter qualifizierten Voraussetzungen gespeichert werden könnten. Und schließlich müsste der Gesetzgeber (3) entscheiden, ob die ePA nur *„ex nunc"* mit solchen Daten befüllt werden soll, die nach ihrer Anlage generiert werden, oder ob eine Befüllung *„ex tunc"* erfolgen soll, also auch mit bereits vorliegenden Daten.

3.2 Datenschutzrechtliche Bewertung

Die *Zulässigkeit* des *„Ob"* der Anlage und Befüllung der ePA mit (Gesundheits-)Daten im Sinne des Art. 4 Nr. 15 DSGVO richtet sich für alle Gestaltungsoptionen in erster Linie nach Art. 9 DSGVO.[17] Für ein Opt-out-Modell, das die Anlage und Befüllung der ePA ohne vorherige Einwilligung der Patienten vorsieht, stehen dem Gesetzgeber grundsätzlich die Verarbeitungstatbestände des *Art. 9 Abs. 2 lit. h) i.V.m. Abs. 3 DSGVO* („individuelle Gesundheitsversorgung") sowie des *Art. 9 Abs. 2 lit. i) DSGVO* („öffentliche Gesundheitsvorsorge") zur Verfügung. Deren tatbestandliche Voraussetzungen dürften in Anbetracht des Zwecks der ePA, eine qualitativ bessere, fach-, sektoren- und zeitübergreifende Gesundheitsversorgung auf breiter, möglichst vollständiger Informationsgrundlage zu ermöglichen,[18] prinzipiell erfüllt sein. Ein über diese Tatbestandsvoraussetzungen hinausgehender „Vorrang von Einwilligungslösungen" oder ein pauschaler „Vorrang des Opt-in" lässt sich dem geltenden Datenschutzrecht nach herrschender Meinung nicht entnehmen.[19]

Unter dem Eindruck der datenschutzrechtlichen Anforderungen an die *Modalitäten* – also das *„Wie"* – der Anlage und Befüllung der ePA zeigen sich gewisse Unterschiede bei der Beurteilung der Gestaltungsoptionen. Der datenschutzrechtliche Grundsatz der *Transparenz (Art. 5 Abs. 1 lit. a) DSGVO)* ist vor allem für solche Opt-out-Gestaltungen relevant, mit der der durchschnittliche Patient nicht ohne Weiteres rechnet – etwa der automatischen, einwilligungsunabhängigen Anlage und Befüllung ohne Registrierungserfordernis. Selbst der Verzicht auf ein gesondertes *Registrierungserfordernis* wäre unseres Erachtens allerdings mit dem Datenschutzgrundsatz der Transparenz vereinbar, solange die betroffenen Personen die Möglichkeit haben, eine Registrierung vorzunehmen und mithin eine niedrigschwellige Einsichtsmöglichkeit in die Verarbeitung ihrer personenbezogenen Gesundheitsdaten gewährleistet wird. Auch eine nachträgliche Befüllung der ePA *„ex tunc"* wäre mit dem Grundsatz der Transparenz vereinbar, da die Patienten in zumutbarer Weise Kenntnis von der Befüllung ihrer ePA nehmen können.

Mit Blick auf den Grundsatz der *Zweckfestlegung und -bindung (Art. 5 Abs. 1 lit. b) DSGVO)* ginge mit einer Befüllung *„ex tunc"* zwar eine gesondert rechtfertigungsbedürftige Zweckänderung einher; allerdings bestünde aufgrund der jeweils versorgungsbezogenen Zwecksetzung insoweit eine Zweckvereinbarkeit, weshalb die Zweckänderung in keinem Widerspruch zu jenem Datenschutzgrundsatz stehen dürfte.[20] Des Weiteren ist festzuhalten, dass in den Opt-out-Gestaltungen für die ePA *keine unzulässige „Vorratsgesundheitsdatenspeicherung"*[21] gesehen werden könnte. Die Einspeisung und Speicherung von Gesundheitsdaten im Kontext der Anlage und Befüllung dienen in erster Linie dazu, zukünftige ordnungsgemäße und qualitativ hochwertige Behandlungen und andere Maßnahmen, die zum Zeitpunkt der Er-

17 Vgl. M. Albers/R. Veit, in: H. A. Wolff/S. Brink (Hrsg.), BeckOK Datenschutzrecht, Stand 1.11.2021, Art. 9 DSGVO Rn. 1 ff. In diesem Kontext wird teilweise erörtert, ob neben den Ausnahmetatbeständen des Art. 9 Abs. 2 bzw. Abs. 3 DSGVO, zusätzlich die allgemeinen Rechtmäßigkeitsbedingungen des Art. 6 DSGVO zu beachten sind. Letztere könnten vom Gesetzgeber ebenso zu berücksichtigen sein, da die Anforderungen des Art. 6 DSGVO durch Art. 9 DSGVO lediglich normativ überlagert, allerdings gerade nicht verdrängt werden. Art. 9 DSGVO entfaltet als lex specialis gegenüber Art. 6 Abs. 1 DSGVO nur insoweit eine Sperrwirkung, als die Ausnahmeregelungen in Art. 9 Abs. 2 und Abs. 3 DSGVO nicht einschlägig sind. Dies dürfte bei der hier zu betrachtenden Einführung eines Opt-out-Modells im Kontext der ePA allerdings zu verneinen sein und kann im Folgenden daher ausgeblendet werden.

18 Siehe dazu etwa A. Jorzig/F. Sarangi, Digitalisierung im Gesundheitswesen, 2020, S. 198.

19 Vgl. dazu bereits Artikel-29-Datenschutzgruppe, Stellungnahme 15/2011 zur Definition von Einwilligung, 01197/11/DE WP 187, 2011, S. 8; S. Schulz, in: P. Gola (Hrsg.), DSGVO, 2. Aufl. 2018, Art. 6 Rn. 10; P. Reimer, in: G. Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 6 Rn. 8; B. Buchner/J. Kühling, in: dies. (Hrsg.), DS-GVO BDSG, 3. Aufl. 2020, Art. 7 DSGVO Rn. 16; vorsichtiger P Schantz, in: S. Simitis/G. Hornung/I. Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 6 DSGVO Rn. 11, der die Einwilligung zwar grundsätzlich als milderen Eingriff wertet, allerdings von einer niedrigen Begründungsschwelle für den Rückgriff auf gesetzliche Verarbeitungsgrundlagen ausgeht; deutlicher für einen „Vorrang der Selbstbestimmung" noch A. Roßnagel/A. Pfitzmann/H. Garstka, Modernisierung des Datenschutzrechts, 2001, S. 72.

20 Vgl. im Allgemeinen M. Albers/R. Veit, in: H. A. Wolff/S. Brink (Hrsg.), BeckOK Datenschutzrecht, Stand 1.11.2021, Art. 6 DSGVO Rn. 98.

21 Vgl. zu deren Unzulässigkeit nach deutschem Verfassungsrecht: BVerfGE 125, 260 (Rn. 17); unionsrechtlich: EuGH, Urteil vom 8.4.2014 – C-293/12 und C-594/12, EU:C:2014:238 sowie nach A. A. und großzügiger offenbar H. A. Wolff, in: P. Schantz/H. A. Wolff (Hrsg.), Das neue Datenschutzrecht, 2017, Rn. 404.

hebung sicherlich noch nicht im Detail feststehen, überhaupt erst zu ermöglichen oder zumindest informationell zu unterstützen.

Im Zusammenhang mit den Datenschutzgrundsätzen der *Datenminimierung (Art. 5 Abs. 1 lit. c) DSGVO)* einerseits und der *Speicherbegrenzung (Art. 5 Abs. 1 lit. e) DSGVO*) anderseits müssen alle Gestaltungsoptionen die Kriterien der Erheblichkeit, Erforderlichkeit und Angemessenheit wahren.[22] Vor allem in Ansehung der Angemessenheit der Verarbeitungen dürfte dabei eine nach der Sensibilität der Gesundheitsdaten *differenzierende Befüllung* gegenüber einer unterschiedslosen „All-in"-Lösung den Vorzug verdienen. Sie erweist sich als deutlich schonendere Gestaltungoption, da sie in angemessener Weise auf die unterschiedliche Sensibilität der Daten Bezug nehmen kann. Da die Verarbeitung „auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein" muss, empfiehlt sich nebstdem, in *prozeduraler* Hinsicht den Einsatz von *Fachpersonal* vorzugeben, das die Einschätzung vornimmt, welche Gesundheitsdaten potenziell für die Gesundheitsversorgung des Patienten vonnöten sein werden. An die *Datensparsamkeit* in zeitlicher Hinsicht dürfen schließlich in Bezug auf sämtliche Gestaltungsoptionen keine allzu strengen Maßgaben gestellt werden, da vor allem im Gesundheitsbereich nicht vorhersehbar ist, wann welche Informationen aus der ePA benötigt werden.

Zur Gewährleistung des Datenschutzgrundsatzes der *Richtigkeit (Art. 5 Abs. 1 lit. d) DSGVO)* erscheint der Einsatz von *Fachpersonal* bei der Anlage und Befüllung in allen Gestaltungsvarianten unabdinglich. Bei einer *„ex tunc"-Befüllung* ist durch das Fachpersonal in besonderer Weise darauf zu achten, dass die Überführung der Bestandsdaten in die ePA gerade mit Blick auf die Semantik und die Formatierung der Daten ordnungsgemäß durchgeführt wird und es zu keinen Qualitätsverlusten kommt. Da auf die Richtigkeit der Informationen vor allem bei besonders sensiblen Daten Wert zu legen ist, weist eine differenzierte Befüllung der ePA wiederum Vorteile gegenüber einer „All-in"-Lösung auf, da sie eine besondere Berücksichtigung der gesteigerten Sensibilität erlaubt.

Aus dem Grundsatz der *Vertraulichkeit und Integrität (Art. 5 Abs. 1 lit. f) DSGVO)* ergibt sich vor allem bei einem Verzicht auf ein *Registrierungserfordernis* die Forderung nach einer Etablierung von effektiven Instrumenten zur Identifikation und Authentifizierung[23] der eingebundenen Akteure[24] sowie von Protokollierungen[25]. Das Registrierungserfordernis als solches ist in Anbetracht dieser alternativen Sicherungsmittel unseres Erachtens aus datenschutzrechtlicher Perspektive gleichwohl nicht zwingend erforderlich.

Ergänzend zu den aus den Datenschutzgrundsätzen folgenden einschränkenden Vorgaben lassen sich den *Grundrechten* des GG und der GRC vor allem Impulse zur Wahl *ermöglichender Gestaltungsoptionen* entnehmen. Um künftige gesundheitsbezogene Entscheidungen selbstbestimmt vornehmen zu können, benötigt der Einzelne eine hinreichende informationelle Entscheidungsgrundlage. Diese dürfte sich durch einen *Verzicht* auf ein *gesondertes Registrierungserfordernis* einerseits sowie eine *umfassende, obligatorische Befüllung der ePA „ex tunc"* andererseits deutlich effektiver schaffen lassen – selbstverständlich unter angemessener Berücksichtigung der Rechte der Leistungserbringer, zumal der Ärzte.

Die sonstigen datenschutzrechtlichen Vorgaben – etwa die Informationspflichten nach Art. 12 ff. DSGVO sowie die Betroffenenrechte aus Art. 15 ff. DSGVO und die Pflichten der Verantwortlichen nach Art. 24 ff. DSGVO – bestätigen schließlich im Wesentlichen die bereits den Datenschutzgrundsätzen entnommenen Anforderungen und Wertungen. So lässt sich beispielsweise auch dem Gebot der *datenschutzfreundlichen Voreinstellungen* im Sinne des Art. 25 Abs. 2 DSGVO entnehmen, dass die Anlage und Befüllung eher dem Konzept einer *differenzierten Befüllung* als einer „All-in"-Lösung folgen sollte – jedenfalls in Gestalt von dispositiven Voreinstellungen.

4 Berechtigung zum Zugriff auf die ePA

Neben der Anlage und Befüllung der ePA bestehen auch bezüglich der Berechtigungen zum Zugriff auf die ePA unterschiedliche Gestaltungsoptionen des Gesetzgebers. Da die Befüllung der ePA einen vom Zugriff darauf unabhängigen Datenverarbeitungsvorgang darstellt, muss bei letzterem erneut die datenschutzrechtliche Zulässigkeit des „Ob" und des „Wie" im Blick behalten werden. Dabei sei vorausgeschickt, dass sich im Kontext der Zugriffe auf die ePA-Daten prinzipiell zwei Aspekte unterscheiden lassen: die Frage, wer in persönlicher Hinsicht zum Zugriff berechtigt ist, und die Frage, wie in sachlicher Hinsicht die abrufbaren Inhalte der ePA gesteuert werden. Nachstehend geht es zunächst allein um die Eingrenzungen in persönlicher Hinsicht. Die Steuerungsmöglichkeiten in sachlicher Hinsicht werden unter Punkt „5 Einzelne abrufbare Inhalte der ePA" aufgezeigt.

4.1 Wesentliche denkbare Gestaltungsoptionen

In Bezug auf die Frage, wer neben dem Patienten im Allgemeinen und im Konkreten Zugriff auf die ePA haben soll, steht der Gesetzeber im Wesentlichen vor *vier Gestaltungsentscheidungen*. Zum einen hat er (1) über die *Modalitäten* der Erteilung der Zugriffsberechtigungen zu bestimmen – hier kann er einerseits automatische Zugriffsberechtigungen erteilen, d.h. ohne gesondertes Zutun der betroffenen Personen, und andererseits Zugriffsberechtigungen nach gesonderter Freischaltung durch den Patienten bezüglich der Leseberechtigung; auch eine Mischung aus diesen beiden Gestaltungsoptionen wäre denkbar, namentlich ein differenziertes Berechtigungssystem. Zum anderen steht der Gesetzgeber (2) vor der Frage, welchen *sachlichen Umfang* die Zugriffsberechtigungen haben sollten. So könnte er insbesondere umfassende Zugriffsberechtigungen oder typisiert beschränk-

22 Siehe genauer P. Schantz, in: H. A. Wolff/S. Brink (Hrsg.), BeckOK Datenschutzrecht, Stand 1.11.2021, Art. 5 DSGVO Rn. 24 ff.

23 Für eine sichere Identifizierung der Betroffenen können Identifikationsmerkmale wie etwa der Name, das Geburtsdatum oder die Wohnanschrift herangezogen werden. Es muss eine zweifelsfrei richtige Beschreibung der Personen stattfinden. Um die Richtigkeit der Beschreibung garantieren zu können, bedarf es z.B. amtlicher Bescheinigungen wie die Sozialversicherungsnummer oder die Geburtsurkunde. Davon sind sog. Authentifizierungen strikt zu trennen. Diese fordern den Nachweis einer betroffenen Person, dass sie wirklich diejenige ist, für die sie sich ausgibt. Eine amtliche Bescheinigung wie etwa durch die Geburtsurkunde ist im Rahmen der Authentifizierung daher nicht ausreichend. Denkbar wären amtliche Ausweispapiere wie etwa der Pass oder die Heranziehung der elektronischen Signatur. Vgl. zur Differenzierung Artikel 29-Datenschutzgruppe, Arbeitspapier zur Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA), 00323/07/DE WP 131, 2007, S. 14 ff.

24 Artikel 29-Datenschutzgruppe, Arbeitspapier zur Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA), 00323/07/DE WP 131, 2007, S. 15 ff.

25 Gegenwärtig ist eine Löschung der Protokolle nach drei Jahren vorgesehen. (vgl. § 309 Abs. 1 i.V.m. § 334 Abs. 1 Nr. 1 i.V.m. § 341 SGB V).

te, gruppenspezifische Berechtigungen vorgeben – sei es als starre, zwingende gesetzliche Festlegung, sei es als dispositive, flexible Voreinstellung, die vom Patienten nachträglich abgeändert werden kann. Zudem muss der Gesetzgeber (3) über eine etwaige (wiederum starr oder flexibel festsetzbare) Beschränkung der *Dauer* der Zugriffsberechtigungen entscheiden und überdies (4) die Modalitäten des *Entzugs* der Zugriffsberechtigungen regeln.

4.2 Datenschutzrechtliche Bewertung

Wie schon im Kontext der Anlage und Befüllung der ePA dargelegt, unterliegen die Ausgestaltungen der Zugriffe auf die ePA datenschutzrechtlichen Vorgaben in Bezug auf die Zulässigkeit des „Ob" des Zugriffs sowie bezüglich der Rechtmäßigkeit, d.h. des „Wie" des Zugriffs. Für die Zulässigkeit des „*Ob*" eines Informationsabrufs zu den hier allein relevanten Versorgungszwecken ist vor allem *Art. 9 Abs. 2 lit. h) i.V.m. Abs. 3 DSGVO*[26] einschlägig, es sei denn für die Leseberechtigung würde ein gesondertes, einer Einwilligung gleichkommendes Freischaltungserfordernis (Art. 9 Abs. 2 lit. a) DSGVO) eingeführt werden. Bei sämtlichen der beschriebenen Gestaltungsoptionen muss der Gesetzgeber somit spezifische Bedingungen und Garantien vorsehen, die dem jeweiligen Charakter der gewählten Option bezüglich der Zugriffsberechtigung hinreichend Rechnung tragen.[27] Vorgaben für die nähere Ausgestaltung dieser Bedingungen und Garantien ergeben sich vor allem aus den Datenschutzgrundsätzen sowie den grundrechtlichen Vorgaben.

Maximale *Transparenz* bestünde sicherlich im Falle eines gesonderten Freischaltungserfordernisses hinsichtlich der Leseberechtigung von Leistungserbringern, da die betroffenen Personen prinzipiell jeden Zugriffsberechtigten selbst freischalten müssten. Es liegt indes auf der Hand, dass dies nicht zur erhöhten Effizienz und Nutzbarkeit der ePA beitragen würde. Diesem Anliegen dürften vielmehr *automatische Zugriffsberechtigungen* entsprechen. Sofern die betroffenen Personen im Rahmen eines Modells mit automatisch erteilten Berechtigungen in hinreichender Weise über diesen Umstand sowie die damit verbundenen Verarbeitungen informiert werden und entsprechende Einsichtsmöglichkeiten in die ePA haben, ferner ein Protokollierungssystem für die Nachvollziehbarkeit der Zugriffe eingerichtet ist und effektive Möglichkeiten zum Entzug von Zugriffsberechtigungen bestehen, sind automatische Zugriffsberechtigungen mit dem Datenschutzgrundsatz der Transparenz vereinbar.

Im Kontext der Grundsätze der *Zweckbindung und -festlegung* sowie der *Datenminimierung* ist zunächst herauszustellen, dass diese Grundsätze deutlich für die Einführung von *Gruppenzugriffsberechtigungen* sprechen. Durch diese kann entsprechend dem Verarbeitungszweck in typisierender Weise eine Eingrenzung der Zugriffsberechtigungen vorgenommen werden und prinzipiell nur jenen Personen eine technische Berechtigung zum Zugriff gewährt werden, die diesen regelmäßig auch materiellrechtlich zusteht, weil sie die betreffenden Informationen typischerweise z.B. für konkrete Behandlungs- bzw. Versorgungszwecke benötigen. Bei umfassend ausgestalteten Zugriffsberechtigungen würden demgegenüber keine standardmäßig beschränkten Zugriffsberechtigungen für bestimmte Akteure vorgesehen, die typischerweise keinen umfassenden Zugriff benötigen. Das Recht auf informationelle Selbstbestimmung im positiven Sinne dürfte dabei für eine flexible und also *dispositive* gesetzliche Voreinstellung der Gruppenzugriffsberechtigungen sprechen, die von den betroffenen Personen selbstbestimmt abgeändert, d.h. erweitert oder auch einschränkt werden könnten. Gleiches dürfte für die gesetzliche Vorgabe von *zeitlichen Beschränkungen* der Zugriffsmöglichkeiten gelten – auch sie schränken übermäßige Verarbeitungen in zeitlicher Hinsicht ein, sollten aber *flexibel* ausgestaltet sein, damit der Patient nötigenfalls auch verlängerte, verkürzte oder unbegrenzte Zugriffe auf seine ePA gestatten kann. Ungeachtet der gewählten Gestaltungsoption sollten mit Blick auf die Grundsätze der Zweckbindung und Datenminimierung auch *prozedurale* Vorkehrungen getroffen werden, um die Zweckmäßigkeit und Erforderlichkeit der Zugriffe zu gewährleisten. Welche konkreten Gesundheitsdaten im Rahmen des aktuellen Behandlungs- bzw. Versorgungskonnexes z.B. für den Abruf erforderlich sind, dürften vor allem wiederum Angehörige des *Fachpersonals* treffen können.

Der Datenschutzgrundsatz der *Richtigkeit* ist ebenfalls für sämtliche Gestaltungsoptionen relevant. Er verlangt zwar keine eigenhändige Kontrolle und/oder Korrektur von ePA-Informationen, gibt den verantwortlichen Krankenkassen[28] aber vor, dass insoweit „alle angemessenen Maßnahmen zu treffen" sind. Die Krankenkassen müssen daher die nötigen technischen Systeme vorhalten, um die sachliche Richtigkeit der ePA-Daten hinsichtlich der äußeren Form zu gewährleisten. Dazu gehören nicht nur eine saubere Konzeption der ePA und eine sorgfältige Auswahl der Dienstleister im Allgemeinen, sondern auch konkrete Maßnahmen, die auf die Gewährleistung der inhaltlichen Richtigkeit und Aktualität der ePA-Daten abzielen – beispielsweise Gestaltungen, die sicherstellen, dass sich der jeweils aktuellste Befund in der ePA befindet und einsehbar ist. Mit Blick auf die sachlich-inhaltliche Richtigkeit[29] dürfen die datenschutzrechtlich Verantwortlichen freilich auch auf die Kompetenz des Fachpersonals vertrauen, die zum Zugriff auf die Informationen berechtigt sind.

Der Grundsatz der *Vertraulichkeit und Integrität* entfaltet zwar Vorgaben zum einen für die Einrichtung *automatischer Zugriffsberechtigungen*, steht diesen aber zum anderen nicht prinzipiell entgegen. Solange lediglich registrierte bzw. authentifizierte zugriffsberechtigte Akteure einen Zugriff auf die ePA erhalten und überdies ein hinreichender Kontakt zu dem betreffenden Patienten besteht[30] – insbesondere in Form einer physischen Anwesenheit oder zumindest eines nachweisbaren virtuellen Kontakts –, dürfte der Vertraulichkeit und Integrität der Verarbeitungen hinreichend Rechnung getragen sein. Zuträglich erweisen sich überdies starre bzw. flexible *Gruppenzugriffsberechtigungen*, da sie aufgrund der auf Basis von Typisierungen vorgegebenen techni-

26 Vgl. T. Petri, in: S. Simitis/G. Hornung/I. Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 9 DSGVO Rn. 78. Ebenso die ErwGr 53 und 54 scheinen darauf hinzudeuten, dass Art. 9 Abs. 2 lit. i) DSGVO primär die „gefahren-, sicherheits- und produktrechtliche Komponente" und Art. 9 Abs. 2 lit. h) DSGVO hingegen vor allem die „infrastrukturelle bzw. systemische Seite des Gesundheitswesens" im Blick hat. Siehe A. Schiff, in: E. Ehmann/M. Selmayr (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 9 Rn. 59 und 62.

27 Vgl. etwa M. Albers/R. Veit, in: H. A. Wolff/S. Brink (Hrsg.), BeckOK Datenschutzrecht, Stand 1.11.2021, Art. 9 DSGVO Rn. 55.

28 Siehe § 341 Abs. 4 SGB V sowie ebenso z.B. J. Eichenhofer, NVwZ 2021, 1090 (1092 f.).

29 Vgl. etwa C. Dochow/B.-S. Dörfer/B. Halbe/M. Hübner/J. Ippach/J. Schröder/J. Schütz/J. Strüve, Datenschutz in der ärztlichen Praxis, 2019, S. 28; T. Herbst, in: J. Kühling/B. Buchner (Hrsg.), DS-GVO BDSG, 3. Aufl. 2020, Art. 5 Rn. 60 sowie Art. 16 Rn. 8 f.

30 Artikel 29-Datenschutzgruppe, Arbeitspapier zur Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA), 00323/07/DE WP 131, 2007, S. 15 ff.

schen Einschränkungen der Zugriffsberechtigungen zumindest die Wahrscheinlichkeit erhöhen dürften, dass keine unrechtmäßigen Verarbeitungen stattfinden. Gleiches gilt für eine vorgezeichnete Beschränkung der *Dauer* der Zugriffsberechtigungen, da diese den formal Zugriffsberechtigten von vornherein nur ein begrenztes Zeitfenster für den Zugriff bietet.

Für beide dieser Gestaltungsoptionen – also die *Gruppenzugriffsberechtigungen* sowie die *zeitliche Beschränkung* der Zugriffsmöglichkeiten – sollte mit Rücksicht auf das *Selbstbestimmungsrecht* der Patienten eine *dispositive*, also flexible gesetzliche Voreinstellung vorgesehen werden. Eine zwingende, starre Vorgabe würde insofern über das Ziel hinausschießen und wäre eine unverhältnismäßige Beschränkung der Patientenrechte.

Von den übrigen datenschutzrechtlichen Regelungen erscheint vor allem das Erfordernis einer *Widerspruchsmöglichkeit (Art. 21 DSGVO)* höchst relevant. Dies betrifft insbesondere die Gestaltungen bezüglich der Modalitäten des *Entzugs* von Zugriffsberechtigungen. Entscheidend erscheint unseres Erachtens, dass der Gesetzgeber für den Entzug eine *multimodale* Gestaltungsoption wählt, d.h. nicht einseitig auf eine bestimmte Modalität setzt. In jedem Falle vorgesehen sein sollte eine elektronische Entzugsmöglichkeit über ein eigenes Endgerät. Darüber hinaus sollte mindestens eine Entzugsmöglichkeit vorgesehen sein, die auch Menschen ohne eigenes Endgerät einfach zur Verfügung steht, etwa über ein Serviceterminal oder direkt vor Ort beim Leistungserbringer.

5 Einzelne abrufbare Inhalte der ePA

Die nachstehenden Ausführungen sind vor allem der Frage gewidmet, wie in sachlicher Hinsicht die (einzelnen) abrufbaren Inhalte der ePA gesteuert werden könnten. Neben der Möglichkeit für die betroffenen Personen, selbstbestimmt steuern zu können, wer – im positiven Sinne – einen Zugriff auf ihre ePA-Daten erhält, sollen die Betroffenen ebenso die Möglichkeit besitzen, dass einzelne Daten(-sätze) – im negativen Sinne – gelöscht werden bzw. gar nicht oder nur teilweise für die anderen Zugriffsberechtigten einsehbar sind.

5.1 Wesentliche denkbare Gestaltungsoptionen

Bei der Regelung der Steuerungsmöglichkeiten der Patienten bezüglich der abrufbaren Inhalte in ihrer ePA hat der Gesetzgeber im Wesentlichen *fünf Gestaltungsentscheidungen* zu treffen. Er hat zunächst (1) den *technischen Zugang* der Patienten zur Steuerung der Inhalte auszugestalten. Außerdem muss er (2) den *Umfang* der Steuerungsmöglichkeiten festlegen (mit feingranularen oder mittel- bis grobgranularen Steuerungsmöglichkeiten). Ferner hat er (3) die *Modalitäten der Entfernung* von Inhalten vorzugeben (mit der Möglichkeit zur Löschung und/oder lediglich der vollständigen oder beschränkten Ausblendung der entfernten Daten, mit oder ohne „Notfall-Modus" z.B. bei Bewusstlosigkeit des Patienten). Er könnte sich (4) überdies dazu entschließen, nicht nur den Patienten selbst, sondern auch anderen Zugriffsberechtigten eine *Steuerungsberechtigung* zuzuordnen. Und schließlich hat der Gesetzgeber (5) über Gestaltungselemente zur *informationellen Unterstützung* der Patienten bei der Steuerung der ePA-Inhalte nachzudenken, insbesondere über Hinweise (z.B. vor einer endgültigen Löschung) und Kontrollfunktionen (z.B. eine „Preview-Funktion" zur Darstellung der Einsehbarkeit der ePA aus der Sicht eines bestimmten Leistungserbringers) für die betroffenen Personen.

5.2 Datenschutzrechtliche Bewertung

Der deutsche Gesetzgeber muss bei der Einführung der ePA als Opt-out-Modell zu Versorgungszwecken *effektive* Möglichkeiten zur *Einsichtnahme* und zur *Steuerung* der Inhalte durch die Patienten vorsehen. Diese Maxime resultiert im Wesentlichen aus den für die Befüllung der ePA bemühten Verarbeitungsgrundlagen in Art. 9 Abs. 2 lit. h) i.V.m. Abs. 3 und Art. 9 Abs. 2 lit. i) DSGVO, die nach „Bedingungen und Garantien" sowie „angemessenen und spezifischen Maßnahmen zur Wahrung der Rechte und Interessen der betroffenen Person" verlangen. Dabei sind auch die Datenschutzgrundsätze, allen voran das Transparenzgebot, sowie das Recht auf informationelle Selbstbestimmung maßstäblich.

Um den durchschnittlichen betroffenen Personen einen niedrigschwelligen *Zugangsweg* zu ermöglichen, scheint als „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person" jedenfalls der Zugangsweg über das *Endgerät* bzw. eine *Website* zwingend einzufordern zu sein. Daneben sollte der Gesetzgeber *zusätzlich* auch einen *„analogen" Zugangsweg* eröffnen, d.h. einen Zugang auch direkt vor Ort beim Leistungserbringer und/oder über Serviceterminals.

Mit Blick auf den möglichen *Umfang* der Steuerung von ePA-Daten hat der Gesetzgeber für die betroffenen Personen zwingend eine *feingranulare* Steuerungsmöglichkeit einzuführen. Dabei sollte der Gesetzgeber im Rahmen einer insgesamt als Opt-out-Modell ausgestalteten ePA die feingranularen Steuerungsmöglichkeiten auf *sämtlichen Zugriffswegen* implementieren.[31]

Bei seiner Entscheidung über die *Modalitäten der Entfernung* von ePA-Daten hat der Gesetzgeber prinzipiell die freie Wahl zwischen einer Löschung und – zusätzlich oder alternativ – der bloßen Ausblendung von ePA-Daten. In jedem Falle ist er unseres Erachtens verpflichtet, zumindest einen gewissen Übereilungsschutz zu gewährleisten. Ob dieser Schutz im Ausschluss einer punktuellen *Löschung* von ePA-Daten besteht oder über entsprechende Warnhinweise vor der endgültigen Löschung erfolgt, liegt unseres Erachtens im freien Ermessen des Gesetzgebers. In Bezug auf eine mögliche *Ausblendungsfunktion* hat der Gesetzgeber einerseits die Option, eine vollständige Ausblendung vorzusehen. Andererseits und zum Schutze der Interessen der Patienten hat er aber auch die Möglichkeit, eine Verschattung ausgeblendeter Informationen sowie einen „Notfall-Modus" für bestimmte Zugriffsberechtigte einzuführen.

31 Vgl. zur Frage der Datenschutzkonformität des derzeit in Deutschland vorgesehenen Konzepts – bei welchem die feingranulare Steuerungsmöglichkeit den betroffenen Personen *nur* auf ihrem Endgerät zusteht – einerseits und kritisch den Musterbescheid des Bundesbeauftragten für den Datenschutz und die Informationssicherheit (BDI) vom 9. September 2021, verfügbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/AccessForAll/2021/2021_Musterbescheid-Gesetzliche-Krankenkasse.pdf?__blob=publicationFile&v=3; andererseits und befürwortend D. Heckmann, Gutachterliche Stellungnahme für den Gesundheitsausschuss des Deutschen Bundstages. Sachverständigen-Anhörung vom 27. Mai 2020 zum Entwurf Drucks. 19/18793, S. 11 ff., verfügbar unter https://www.bundestag.de/resource/blob/697802/331a534d9bc78f93c3fc5644fa172bee/19_14_0165-25-_ESV-Prof-Heckmann_PDSG-data.pdf.

Im Kontext von *weitreichenden Steuerungsentscheidungen,* die dazu führen können, dass für gesundheitsbezogene Entscheidungen des Patienten in der Zukunft keine hinreichende informationelle Basis besteht, sehen wir den Gesetzgeber zudem in der Pflicht, *Warnhinweispflichten* vorzusehen; dies betrifft, wie soeben dargelegt, insbesondere die vollständige *Löschung* punktueller ePA-Daten. Eine „Preview-Funktion" sollte der Gesetzgeber lediglich als optionale Maßnahme zur Optimierung der Transparenz der ePA erwägen.

Eine Berechtigung zugunsten von *anderen Zugriffsberechtigten* (z.B. Ärzten) zur *Löschung, Änderung* und/oder *Ausblendung* von ePA-Daten[32] zum Zwecke der Vermeidung von Fehlern bei der künftigen Versorgung des betreffenden Patienten infolge unrichtiger Datengrundlage (z.B. einer veralteten, überholten Diagnose) ist unseres Erachtens eine eigenständige, allerdings datenschutzrechtlich unzulässige Datenverarbeitung. Als gegenüber der vollständigen Löschung oder Ausblendung milderes Mittel zur Erreichung dieses Zwecks kommt vielmehr eine *Ergänzung und Markierung* bestehender, gegebenenfalls unrichtiger Gesundheitsdaten durch einen Zusatz in Betracht, der deutlich auf die Unrichtigkeit der betreffenden Daten hinweist (z.B. durch einen Mark-up in roter Farbe) und die entsprechenden richtigen Informationen enthält.

6 Fazit

Den Schlüssel zu einer sachrichtigen Gesundheitsbehandlung bildet vielfach eine sorgfältige Erhebung der Krankheitsgeschichte. Die Verfügbarkeit vollständiger und hochwertiger Gesundheitsinformationen des Patienten kann unter anderem für Leistungserbringer von ganz besonderer Bedeutung sein, um sie zeitnah und angemessen behandeln zu können. In Anbetracht der mit der Digitalisierung auch von Gesundheitsdaten eröffneten Möglichkeiten der Informationsverarbeitung liegt es auf der Hand, dass elektronischen Patientenaktensystemen eine Schlüsselrolle bei der Gewährleistung einer Gesundheitsversorgung nach dem „State of the Art" zukommt. Mit Blick auf das gegenwärtige, umständlich ausgestaltete Opt-in-Modell für die ePA bleiben allerdings substanzielle datenschutzrechtliche Gestaltungsspielräume ungenutzt. Um dem Ziel einer effektiven, effizienten Gesundheitsversorgung auf möglichst breiter und vollständiger Informationsbasis näher zu kommen, scheint die Einführung eines Opt-out-Modells für die ePA-Nutzung zu Versorgungszwecken unabdingbar. Welche wesentlichen denkbaren Gestaltungsentscheidungen der deutsche Gesetzgeber hierbei zu treffen hat, konnte im Kontext der Anlage und Befüllung der ePA mit Gesundheitsdaten, der Berechtigung zum Zugriff auf die ePA sowie der einzelnen abrufbaren Inhalte der ePA aufgezeigt werden. Der Ball liegt nun im Spielfeld des Gesetzgebers.

32 Lediglich im Rahmen des estnischen Opt-out-Modells der ePA besteht die Möglichkeit, dass Gesundheitsdiensteanbieter zum Schutze des Lebens und der Gesundheit der betroffenen Personen einzelne Daten für eine Dauer von bis zu sechs Monaten ausblenden und diese lediglich durch einen Angehörigen der Gesundheitsberufe eingesehen werden können. Vgl. C. Krönke/V. Aichstill, in: Stiftung Münch (Hrsg.), Die elektronische Patientenakte und das europäische Datenschutzrecht, 2021, S. 113.