Opt-out-Modelle für die Elektronische Patientenakte aus datenschutzrechtlicher Perspektive

STIFTUNG MÜNCH

BertelsmannStiftung

Rechtswissenschaftliche Studie zum Thema

Opt-out-Modelle für die Elektronische Patientenakte aus datenschutzrechtlicher Perspektive

Autor
Univ.-Prof. Dr. Christoph Krönke
Vorstand des Instituts für Öffentliches Recht,
Nachhaltigkeits- und Technologierecht (IONTech)
an der Wirtschaftsuniversität Wien (WU)

unter Mitwirkung von
Elissa Tschachler, LL.M. (WU)

Mai 2022

Zusammenfassung in Thesen

Die Ergebnisse der rechtswissenschaftlichen Studie lassen sich in den folgenden Thesen summieren. Sie stellen lediglich eine Zusammenfassung dar, keine Ersetzung oder Ergänzung der Studie.

1 Bei der Einführung eines **Opt-out-Systems für eine elektronische Patientenakte (ePA)** bestehen nach Maßgabe der Datenschutzgrundverordnung (DSGVO) und der ergänzend heranzuziehenden Wertungen der grundrechtlichen Datenschutzgewährleistungen des Grundgesetzes sowie der europäischen Grundrechtecharta diverse **Ausgestaltungsspielräume**, von denen ein Gesetzgeber Gebrauch machen kann – aber nicht muss. Die Spielräume beziehen sich auf die Anlage und **Befüllung der ePA** mit Gesundheitsdaten (dazu nachfolgend die Punkte 2. bis 10.), die Einräumung von **Berechtigungen** bestimmter Akteure zum **Zugriff auf die ePA** (dazu nachfolgend die Punkte 11. bis 18.) sowie die Möglichkeiten der Patienten und Dritter zur **Steuerung der Inhalte der ePA** (dazu nachfolgend die Punkte 19. bis 25.).

2 Bei der Ausgestaltung der Anlage und **Befüllung** der ePA im Rahmen eines Opt-out-Modells – also unabhängig von einer Einwilligung der Patientin oder des Patienten – könnte der deutsche Gesetzgeber im Wesentlichen folgende **drei Entscheidungen** treffen: Er könnte die automatische, einwilligungsunabhängige Anlage und Befüllung an ein gesondertes **Registrierungserfordernis** für den Patienten knüpfen oder auf eine Registrierungspflicht verzichten. Er könnte 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 nur unter qualifizierten Voraussetzungen gespeichert werden könnten. Und schließlich müsste der Gesetzgeber 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 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. Für ein Opt-out-Modell, das die Anlage und Befüllung der ePA ohne vorherige Einwilligung der Patientinnen und 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 Gesundheit) zur Verfügung. Deren tatbestandlichen Voraussetzungen sind prinzipiell erfüllt, ein darüber hinausgehender Vorrang einer Einwilligungslösung besteht nicht.

4 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** ist vor allem für solche Opt-out-Gestaltungen relevant, mit denen der durchschnittliche Patient nicht ohne Weiteres rechnet – etwa die automatische, einwilligungsunabhängige Anlage und Befüllung ohne Registrierungserfordernis. Selbst der Verzicht auf ein gesondertes **Registrierungs-**

erfordernis wäre 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 Patientinnen und Patienten in zumutbarer Weise Kenntnis von der Befüllung ihrer ePA nehmen können.

5 Mit Blick auf den Grundsatz der **Zweckfestlegung und -bindung** ginge mit einer Befüllung **„ex tunc“** zwar eine gesondert rechtfertigungsbedürftige Zweckänderung einher; allerdings bestünde insoweit eine Zweckvereinbarkeit, weshalb die Zweckänderung in keinem Widerspruch zum Datenschutzgrundsatz stehen dürfte. Des Weiteren ist festzuhalten, dass in den Opt-out-Gestaltungen für die ePA **keine unzulässige „Vorratsgesundheitsdatenspeicherung“** gesehen werden könnte. Die Einspeisung und Speicherung von Gesundheitsdaten im Kontext der Anlage und Befüllung dienen in erster Linie dazu, künftige ordnungsgemäße und qualitativ hochwertige Behandlungen sowie andere Maßnahmen, die zum Zeitpunkt der Erhebung sicherlich noch nicht im Detail feststehen, überhaupt erst zu ermöglichen oder zumindest informationell zu unterstützen.

6 Im Zusammenhang mit den Datenschutzgrundsätzen der **Datenminimierung** einerseits sowie der **Speicherbegrenzung** andererseits müssen alle Gestaltungsoptionen die Anforderungen der Geeignetheit, Erforderlichkeit und Angemessenheit erfüllen. Vor allem mit Blick auf die Angemessenheit der Verarbeitungen dürfte eine nach der Sensibilität der Gesundheitsdaten **differenzierende Befüllung** gegenüber einer unterschiedslosen „All-in-Lösung“ den Vorzug verdienen. Sie erweist sich als deutlich schonendere Gestaltungsoption, weil sie angemessen auf die unterschiedliche Sensibilität der Daten Bezug nehmen kann. Da die Verarbeitung „auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein“ muss, wird zudem in **prozeduraler** Hinsicht der Einsatz von **Fachpersonal** empfohlen, das die Einschätzung vornimmt, welche Gesundheitsdaten potenziell für die Gesundheitsversorgung der Patientin oder des Patienten vonnöten sein werden. Mit Blick auf die **Datensparsamkeit** in zeitlicher Hinsicht ist schließlich in Bezug auf sämtliche Gestaltungsoptionen zu erwähnen, dass keine allzu strengen Maßgaben an dieses Kriterium gestellt werden dürfen, da vor allem im Gesundheitsbereich nicht vorhersehbar ist, wann welche Informationen aus der ePA benötigt werden.

7 Zur Gewährleistung des Datenschutzgrundsatzes der **Richtigkeit** erscheint der Einsatz von **Fachpersonal** bei der Anlage und Befüllung in allen Gestaltungsvarianten unabdinglich. Bei einer **„ex tunc“-Befüllung** ist vom 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 erfolgt 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, weil sie eine besondere Berücksichtigung der gesteigerten Sensibilität erlaubt.

8 Aus dem Grundsatz der **Vertraulichkeit und Integrität** ergibt sich vor allem bei einem Verzicht auf ein **Registrierungserfordernis** die Forderung nach einer Etablierung von effektiven Instrumenten zur Identifikation und Authentifizierung der eingebundenen Akteure und von Protokollierungen. Das Registrierungserfordernis als solches ist unseres Erachtens aus datenschutzrechtlicher Perspektive gleichwohl nicht zwingend erforderlich.

9 Ergänzend zu den aus den Datenschutzgrundsätzen folgenden einschränkenden Vorgaben lassen sich den **Grundrechten** des Grundgesetzes und der Grundrechtecharta vor allem Impulse zur Wahl **ermöglichender Gestaltungsoptionen** entnehmen. Um künftige gesundheitsbezogene Entscheidungen selbstbestimmt vornehmen zu können, benötigt der bzw. die Einzelne eine hinreichende informationelle Entscheidungsgrundlage. Diese dürfte sich durch den **Verzicht** auf ein **gesondertes Registrierungserfordernis** sowie durch eine **umfassende, obligatorische Befüllung der ePA „ex tunc“** deutlich effektiver schaffen lassen.

10 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.

11 In Bezug auf die Frage, wer neben der Patientin und dem Patienten im Allgemeinen und im Konkreten Zugriff auf die ePA haben soll, steht der Gesetzgeber im Wesentlichen vor **vier Gestaltungsentscheidungen**. Zum einen hat er über die **Modalitäten** der Erteilung der Zugriffsberechtigungen zu bestimmen – hier kann er einerseits automatische Berechtigungen 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 vor der Frage, welchen **sachlichen Umfang** die Zugriffsberechtigungen haben sollten. So könnte er insbesondere umfassende Berechtigungen oder typisiert beschränkte, gruppenspezifische Berechtigungen vorgeben – sei es als starre, zwingende gesetzliche Festlegung, sei es als dispositive, flexible Voreinstellung, die vom Patienten nachträglich geändert werden kann. Zudem muss der Gesetzgeber über eine etwaige (wiederum starr oder flexibel festsetzbare) Beschränkung der **Dauer** der Zugriffsberechtigungen entscheiden und überdies die Modalitäten des **Entzugs** der Berechtigungen regeln.

12 Wie schon im Kontext der Anlage und Befüllung der ePA dargelegt, unterliegen die Ausgestaltungen der Zugriffe datenschutzrechtlichen Vorgaben in Bezug auf die Zulässigkeit des **„Ob“** des Zugriffs und 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** 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 beschriebenen Gestaltungsoptionen muss der Gesetzgeber somit spezifische Bedingungen und Garantien vorsehen, die dem jeweiligen Charakter der gewählten Option bezüglich der Zugriffsberechtigung hinreichend Rechnung tragen. Vorgaben für die nähere Ausgestaltung dieser Bedingungen und Garantien ergeben sich vor allem aus den Datenschutzgrundsätzen sowie den grundrechtlichen Vorgaben.

13 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 in einem Modell mit automatisch erteilten Berechtigungen hinreichend über diesen Umstand sowie die damit verbundenen Verarbeitungen informiert werden und entsprechende Möglichkeiten der Einsicht in die ePA haben, ferner ein Protokollierungssystem für die Nachvoll-

ziehbarkeit der Zugriffe eingerichtet ist und effektive Möglichkeiten zum Entzug von Zugriffsberechtigungen bestehen, sind automatische Zugriffsberechtigungen mit dem Datenschutzgrundsatz der Transparenz vereinbar.

14 Im Kontext der Grundsätze der **Zweckbindung und -festlegung** sowie der **Datenminimierung** konnte zunächst herausgearbeitet werden, 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 materiell-rechtlich zusteht, weil sie die betreffenden Informationen typischerweise z. B. für konkrete Behandlungs- bzw. Versorgungszwecke benötigen. Bei umfassend ausgestalteten Zugriffsberechtigungen wären demgegenüber keine standardmäßig beschränkten Berechtigungen vorgesehen – auch nicht für Akteure, 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 geändert, also erweitert oder auch eingeschränkt werden könnten. Gleiches dürfte für die gesetzliche Vorgabe **zeitlicher Beschränkungen** der Zugriffsmöglichkeiten gelten – auch sie schränken übermäßige Verarbeitungen in zeitlicher Hinsicht ein, sollten aber **flexibel** gestaltet sein, damit der Patient nötigenfalls auch verlängerte, verkürzte oder unbegrenzte Zugriffe auf seine ePA gestatten kann. Ungeachtet der gewählten Option 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 Angehörige des **Fachpersonals** entscheiden können.

15 Der Grundsatz der **Richtigkeit** der Verarbeitungen gemäß Art. 5 Abs. 1 lit. d) DSGVO ist ebenfalls für sämtliche Gestaltungsoptionen relevant. Er verlangt zwar keine eigenhändige Kontrolle und / oder Korrektur von ePA-Informationen, gibt den derzeit verantwortlichen Krankenkassen 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 dürfen die Verantwortlichen – derzeit die Krankenkassen – freilich auch auf die Kompetenz des Fachpersonals vertrauen, das zum Zugriff auf die Informationen berechtigt ist.

16 Der Grundsatz der **Vertraulichkeit und Integrität** entfaltet zwar Vorgaben für die Einrichtung **automatischer Zugriffsberechtigungen**, steht diesen aber nicht prinzipiell entgegen. Solange lediglich registrierte bzw. authentifizierte zugriffsberechtigte Akteure einen Zugriff auf die ePA erhalten und überdies ein hinreichender Kontakt zu den betreffenden Patienten besteht – besonders 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 technischen 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 Berechtigten von vornherein nur ein begrenztes Zeitfenster für den Zugriff bietet.

17 Für diese beiden Gestaltungsoptionen – also die **Gruppenzugriffsberechtigungen** sowie die **zeitliche Beschränkung** der Zugriffsmöglichkeiten – sollte mit Rücksicht auf das **Selbstbestimmungsrecht** der Patientinnen und Patienten eine **dispositive**, also flexible gesetzliche Voreinstellung vorgesehen werden. Eine zwingende, starre Vorgabe würde über das Ziel hinausschießen.

18 Von den übrigen datenschutzrechtlichen Regelungen erscheint vor allem das Erfordernis einer **Widerspruchsmöglichkeit** höchst relevant. Dies betrifft insbesondere die Gestaltungen bezüglich der Modalitäten des **Entzugs** von Zugriffsberechtigungen. Entscheidend ist unseres Erachtens, dass der Gesetzgeber für den Entzug eine **multimodale** Gestaltungsoption wählt, also nicht einseitig auf eine bestimmte Modalität setzt. In jedem Falle vorgesehen sein sollte eine elektronische Entzugsmöglichkeit über ein eigenes Endgerät (z. B. Smartphone-App, webbasierte Lösungen etc. mit jeweils geeigneten Zugangsmechanismen). Darüber hinaus sollte mindestens eine Möglichkeit vorgesehen sein, die auch Menschen ohne eigenes Endgerät unkompliziert zur Verfügung steht.

19 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 ePA-Befüllung 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 „angemessene[n] und spezifische[n] Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person“ verlangen. Dabei sind auch die Datenschutzgrundsätze, allen voran das Transparenzgebot (Art. 5 Abs. 1 lit. a) DSGVO), sowie das Recht auf informationelle Selbstbestimmung maßstäblich.

20 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 den **technischen Zugang** der Patientinnen und Patienten zur Steuerung der Inhalte zu gestalten. Außerdem muss er den **Umfang** der Steuerungsmöglichkeiten festlegen (mit feingranularen oder mittel- bis grobgranularen Steuerungsmöglichkeiten). Ferner hat er die **Modalitäten der Entfernung** von Inhalten vorzugeben (mit der Möglichkeit zur Löschung und / oder der vollständigen oder beschränkten Ausblendung der entfernten Daten). Er könnte sich überdies entschließen, nicht nur den Patienten selbst, sondern auch anderen Zugriffsberechtigten eine **Steuerungsberechtigung** zuzuordnen. Und schließlich muss der Gesetzgeber über Gestaltungselemente zur **informationellen Unterstützung** der Patienten bei der Steuerung der ePA-Inhalte nachdenken, insbesondere über Hinweise und Kontrollfunktionen für die betroffenen Personen.

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

22 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 er in einer insgesamt als Opt-out-Modell gestalteten ePA die feingranularen Steuerungsmöglichkeiten auf **sämtlichen Zugriffswegen** implementieren.

23 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 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 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 kann er aber auch eine Verschattung ausgeblendeter Informationen sowie einen „Notfallmodus" für bestimmte Zugriffsberechtigte einführen.

24 Im Kontext **weitreichender Steuerungsentscheidungen**, die dazu führen können, dass für gesundheitsbezogene Entscheidungen der Patientinnen und Patienten in der Zukunft keine hinreichende informationelle Basis besteht, ist der Gesetzgeber verpflichtet, **Warnhinweispflichten** vorzusehen; dies betrifft, wie oben dargelegt, insbesondere die vollständige **Löschung** punktueller ePA-Daten. Eine „Preview-Funktion" sollte der Gesetzgeber lediglich als optionale Maßnahme zur Optimierung der ePA-Transparenz erwägen.

25 Eine Berechtigung zugunsten von **anderen Zugriffsberechtigten** (z. B. Ärzten) zur **Löschung**, **Änderung** und / oder **Ausblendung** von ePA-Daten zum Zwecke der Vermeidung von Fehlern bei der künftigen Versorgung des betreffenden Patienten infolge einer unrichtigen Datengrundlage ist datenschutzrechtlich unzulässig. Als milderes Mittel – gegenüber der vollständigen Löschung oder Ausblendung – 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 richtigen Informationen enthält.

Inhalt

1 Einführung

1.1 Hintergrund der Studie

Mit dem 1. Januar 2021 wurde die elektronische Patientenakte (ePA) als Angebot für die rund 73 Millionen gesetzlich Versicherten in Deutschland eingeführt. Entsprechend der gesetzlichen Definition in § 341 Abs. 1 SGB V handelt es sich bei der ePA um eine versichertengeführte elektronische Akte, die den Versicherten von den Krankenkassen auf Antrag zur Verfügung gestellt werden muss. Dabei wurde die ePA vom deutschen Gesetzgeber unter das Leitbild der 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 die Einwilligung dazu erteilt hat (sog. Opt-in).

Im Gegensatz zu einem sogenannten Opt-out-Modell, wie es im Bereich der Gesundheitsdatennutzung zu Versorgungszwecken beispielsweise in Österreich vorgesehen ist, bietet das derzeitige Regelungskonzept in Deutschland keine Möglichkeit 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/der 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 gespeicherten Informationen.

Diese gegenwärtige, vergleichsweise umständliche Ausgestaltung der ePA als „Einwilligungskaskade" wurde unter anderem durch den Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen in seinem Gutachten 2021 unter gesundheitswissenschaftlichen Gesichtspunkten deutlich kritisiert.[1] Das Einwilligungssystem entspreche insbesondere nicht der Idee eines – gegebenenfalls über einen längeren Zeitraum – fach- und sektorenübergreifenden Behandelns durch mehrere Leistungserbringer. Bei dem derzeitigen Einwilligungsverfahren sei unter anderem zu befürchten, „dass selbst bei teilnahmewilligen Patientinnen und Patienten ein vollständiger Datenbestand der ePA häufig nicht zustande kommt, weil die Überlagerung von multiplen Einwilligungen dieses

1 *Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen*, Digitalisierung für Gesundheit. Ziele und Rahmenbedingungen eines dynamisch lernenden Gesundheitssystems, 2021, S. 85 ff., verfügbar unter https://www.svr-gesundheit.de/fileadmin/Gutachten/Gutachten_2021/SVR_Gutachten_2021.pdf.

Ergebnis unwahrscheinlich macht."[2] Des Weiteren haben verschiedene vergleichende Studien[3] aufgezeigt, dass die elektronischen Patientenaktensysteme anderer, zumal europäischer Länder ohne vergleichbar diffizile Einwilligungsmodelle operieren und dabei die wesentlichen Vorteile, die eine ePA mit sich bringen kann – z.B. die Vermeidung von Doppeluntersuchungen[4], einer Doppelvorhaltung von Gesundheitsinformationen sowie der zahlreichen Fehlermöglichkeiten an den Informationsschnittstellen – in höherem Maße nutzbar machen.

Erst jüngst betonte schließlich auch der Corona-Expertenrat der Bundesregierung, dass Deutschland eine umfassende Digitalisierung des Gesundheitswesens benötige, und verlangte, die Einführung der ePA „mit höchster Priorität" umzusetzen. Empfohlen wurde die „umgehende Umsetzung der Empfehlungen aus dem 2021 erstellten Gutachten des Sachverständigenrats zur Begutachtung der Entwicklung im Gesundheitswesen. 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.[5] Zu Recht sei der Sachverständigenrat in seinem Gutachten 2021 zu dem Ergebnis gelangt, dass die Implementierung eines autonomiesichernd ausgestalteten Opt-out-Modells den Bedürfnissen eines modernen Gesundheitssystems besser Rechnung trage als ein striktes Opt-in-Modell, wie es bislang in Deutschland vorgesehen ist.

Die an der gegenwärtigen Ausgestaltung der ePA geäußerte Kritik hat offenbar Gehör seitens der Bundesregierung gefunden. 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 elektronischen Patientenakte (ePA) und des E-Rezeptes sowie deren nutzenbringende Anwendung und binden beschleunigt sämtliche Akteure an die Telematikinfrastruktur an. Alle Versicherten bekommen DSGVO-konform eine ePA zur Verfügung gestellt; ihre Nutzung ist freiwillig (opt-out). Die gematik bauen wir zu einer digitalen Gesundheitsagentur aus. Zudem bringen wir ein Registergesetz und ein Gesundheitsdatennutzungsgesetz zur besseren wissenschaftlichen Nutzung in Einklang mit der DSGVO auf den Weg und bauen eine dezentrale Forschungsdateninfrastruktur auf."

2 So der *Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen*, Digitalisierung für Gesundheit. Ziele und Rahmenbedingungen eines dynamisch lernenden Gesundheitssystems, 2021, S. 86. Vgl. ebenso die rechtsvergleichende Studie im Auftrag der Stiftung Münch von *C. Krönke/V. Aichstill*, in: Stiftung Münch (Hrsg.), Die elektronische Patientenakte und das europäische Datenschutzrecht, 2021, S. 96. Erwähnenswert ist in diesem Zusammenhang überdies, 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.

3 Siehe z. B. *P. Haas*, in: Bertelsmann Stiftung (Hrsg.), Elektronische Patientenakten, 2017, S. 18 ff. Vgl. die rechtsvergleichende Studie im Auftrag der Stiftung Münch von *C. Krönke/V. Aichstill*, in: Stiftung Münch (Hrsg.), Die elektronische Patientenakte und das europäische Datenschutzrecht, 2021, S. 3 ff.

4 Vgl. auch *J. Eichenhofer,* NVwZ 2021, 1090 (1092).

5 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-4expertenrat-data.pdf?download=1.

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 sollen im Folgenden die Möglichkeiten zur Ausgestaltung von Opt-out-Modellen der ePA aufgezeigt werden, die sich im Rahmen der Vorgaben des europäischen Datenschutzrechts sowie grundrechtlicher Datenschutzgehalte bewegen.

Zum Zwecke der Veranschaulichung der wesentlichen Gestaltungsoptionen und ihrer Unterschiede möchten wir auf folgendes einfaches Fallbeispiel zurückgreifen, das bereits im Kontext einer rechtsvergleichenden Studie zur ePA verwendet wurde:[6]

Fallbeispiel: Anna aus der Stadt A erleidet während eines Aufenthalts bei ihren Eltern in der Stadt B aus vermeintlicher voller Gesundheit heraus eine heftige, einige Stunden andauernde und nur über mehrere Tage hinweg langsam abklingende Schwindelattacke. Im Krankenhaus in B werden eine MRT-Untersuchung ihres Kopfes und eine Blutuntersuchung durchgeführt, ferner erfolgen dort über 24 Stunden EKG- und Blutdruckmessungen sowie HNO- und logische Untersuchungen. Die Befunde sind jeweils unauffällig. Innerhalb des darauffolgenden Jahres wird Anna zweimal in anderen Zusammenhängen Blut abgenommen – einmal bei ihrem Hausarzt in der Stadt A, ein weiteres Mal bei einem Arzt in der Stadt B. Ein Jahr später verspürt Anna starken Schwindel und sucht ihren Hausarzt in der Stadt A auf. Dieser diagnostiziert in Anbetracht der jeweils unauffälligen Befunde und unter dem Eindruck von Annas länglicher Schilderungen eine Angststörung.

Vorüberlegungen: Den Schlüssel zu einer sachrichtigen Diagnose bildet vielfach eine sorgfältige Erhebung der Krankheitsgeschichte (Anamnese), einschließlich körperlicher Untersuchungen. Dies gilt gerade auch für das Symptom des Schwindels – nach dem Kopfschmerz eines der häufigsten Leitsymptome überhaupt. Die Verfügbarkeit vollständiger und hochwertiger Gesundheitsinformationen zur Krankheitsgeschichte von Anna kann für den Hausarzt in dem Ausgangsfall daher 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.

6 Vgl. *C. Krönke/V. Aichstill*, in: Stiftung Münch (Hrsg.), Die elektronische Patientenakte und das europäische Datenschutzrecht, 2021, S. 4.

1.2 Gegenstand, Methodik und Aufbau der Studie

Gegenstand der vorliegenden Studie ist somit die Frage, welche wesentlichen Gestaltungsoptionen der deutsche Gesetzgeber bei der Einführung eines Opt-out-Modells für die ePA hat, und zwar in Bezug auf die Nutzung zu Versorgungszwecken unter Einhaltung der Vorgaben, die sich aus der Datenschutzgrundverordnung sowie grundrechtlichen Datenschutzgewährleistungen ergeben. Mit Blick auf die zur Beantwortung der Forschungsfrage zu Gebote stehenden **methodischen** Instrumente soll diese Studie zunächst rechtsdogmatisch vorgehen, das heißt am geltenden europäischen und nationalen Verfassungsrecht in seinem tatsächlichen Kontext arbeiten. Zuvörderst sollen primär die sowohl datenschutzrechtlichen – insbesondere die Datenschutzgrundverordnung – als auch die Maßgaben der grundrechtlichen Datenschutzgewährleistungen bei der Einführung eines Opt-out-Modells für die ePA abgesteckt werden.[7]

Dabei soll die Studie – zweitens – auch rechtspolitische Handlungsoptionen erarbeiten und im Rahmen des erworbenen Erkenntnisgewinns – aus den unions- und verfassungsrechtlichen Vorgaben der Regelungen zur ePA – dem deutschen Gesetzgeber bei der Einführung eines Opt-out-Modells in Bezug auf die Nutzung zu Versorgungszwecken die wesentlichen Gestaltungsoptionen aufzeigen, wie die ePA deutscher Provenienz unter Ausschöpfung der unionsrechtlichen Gestaltungsspielräume und Beachtung des deutschen Verfassungsrechts ausgestaltet werden könnte. Nicht Gegenstand der Studie soll dagegen die Einführung eines Opt-out in Bezug auf die Nutzung von ePA-Daten zu sekundären Zwecken sein. Im Übrigen kann die vorliegende Studie eine Bewertung lediglich aus rechtswissenschaftlicher Perspektive leisten; Stellungnahmen zu nicht juristischen, insbesondere medizinischen, ökonomischen, technischen oder gesundheitswissenschaftlichen Fragen, werden nicht abgegeben.

Aus diesen Überlegungen ergibt sich die folgende **Grundstruktur** der Studie. Zu Beginn werden nach der Einführung (»1.) die unions- und verfassungsrechtlichen Rahmen der Regelungen zur ePA (»2) aufgezeigt, die für die Herausarbeitung der wesentlichen Gestaltungsoptionen bei der Einführung eines Opt-out-Modells relevant sein werden. Hierbei wird ein Überblick über die konkreten Maßgaben der DSGVO (»2.1) zur Anlage und Befüllung, zur Berechtigung und zum Zugriff sowie zu einzelnen abrufbaren Inhalten der ePA gegeben. Es folgt ein Überblick über die einschlägigen grundrechtlichen Datenschutzgewährleistungen (»2.2) des Grundgesetzes (»2.2.1) sowie aus der europäischen Grundrechtecharta (»2.2.2). Die daraus gewonnenen Erkenntnisse lassen sich für die Herausarbeitung der wesentlichen Gestaltungsräume im Rahmen der Einführung eines Opt-out-Modells nutzen: Hierbei werden zunächst die Anlage und Befüllung der ePA (»3.) in den Blick genommen, gefolgt von der Berechtigung zum Zugriff auf die ePA (»4.) sowie den Steuerungsmöglichkeiten in Bezug auf die einzelnen abrufbaren Inhalte der ePA (»5.). Dabei soll jeweils auf die wesentlichen denkbaren Gestaltungsoptionen (»5.1) und ihre datenschutzrechtliche Bewertung (»5.2) eingegangen sowie abschließend eine Zusammenfassung (»5.3) gegeben werden.

7 Nicht Gegenstand der Studie sind die privatrechtlichen und sonstigen medizin- und gesundheitsrechtlichen Vorgaben. Vgl. zu diesen im Überblick etwa *C. Herles/R. Wiring/S. Schreiber*, MMR 2021, 615 (616).

2 Unions- und verfassungsrechtlicher Rahmen der Regelungen zur ePA

Die in Deutschland geltenden rechtlichen Maßstäbe für die Verarbeitung von personenbezogenen Daten sind in hohem Maße durch unionsrechtliche Vorgaben bestimmt. Bereits der Vorläufer des heutigen Bundesdatenschutzgesetzes (BDSG)[8] setzte im Wesentlichen die Vorgaben der Datenschutzrichtlinie 95/46/EG[9] um.[10] Diese wurde durch die **Datenschutzgrundverordnung**[11] (im Folgenden: DSGVO) ersetzt, 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 (»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 **Charta der Grundrechte der Europäischen Union** (im Folgenden: GRC) sowie aus Art. 16 Abs. 1 des Vertrags über die Arbeitsweise der Europäischen Union (im Folgenden: 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** (»2.2).

2.1 Datenschutzgrundverordnung

Zur Eröffnung des **sachlichen Anwendungsbereichs** der DSGVO muss es sich bei den Vorgängen im Kontext der ePA gemäß Art. 1 und 2 DSGVO zunächst um die Verarbeitung von **personenbezogenen Daten** handeln. Personenbezogene Daten sind nach Art. 4 Nr. 1 DSGVO „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden ‚betroffene Person‘) beziehen“. Im Rahmen von medizinischen Behandlungen und Untersuchungen (z.B. der Erstellung eines großen Blutbildes) weisen

8 Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), das durch Artikel 10 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1858) geändert worden ist.

9 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23. November 1995, S. 31–50.

10 Vgl. *S. Polenz*, in: J. Taeger/J. Pohle (Hrsg.), Computerrechts-Handbuch, 2021, Teil 13 Rn. 1.

11 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 vom 4. Mai 2016, S. 1–88.

nahezu alle generierten Informationen einen Personen- und Gesundheitsbezug auf und machen die dahinterstehende Person zumindest „identifizierbar“ im Sinne des Art. 4 Nr. 1 DSGVO. Unstrittig dürften vor allem jene medizinischen Behandlungen einen derart individuellen – „identifizierbaren“ – Bezug zur dahinterstehenden Person aufweisen, dass es auch technisch kaum möglich ist, den Personenbezug zu eliminieren. Die Nichtanwendung des Datenschutzrechts aufgrund von anonymisierten sowie nicht mehr zu „re-anonymisierenden“ Daten erscheint daher unter den technischen Gegebenheiten sehr illusorisch. Insoweit ist zutreffend, dass „anonyme Daten“ im Gesundheitswesen in der Regel nicht bestehen können.[12]

Der Begriff der **Verarbeitung** wird in Art. 4 Nr. 2 DSGVO definiert und zählt enumerativ Vorgänge „im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“ auf.[13] Demzufolge fallen darunter in der Regel alle wesentlichen Arbeitsschritte im Umgang mit den ePA.

Zudem handelt es sich bei den in den ePA dargestellten Informationen überwiegend um **Gesundheitsdaten** im Sinne des Art. 4 Nr. 15 DSGVO[14]. Diese werden definiert als „personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen“.[15] Dass dementsprechend Informationen „höchstpersönlicher“ Natur mit (kontextbedingt) besonders hohem Schadens- und Diskriminierungspotenzial[16] und zudem sehr ausgeprägter Identifikationskraft[17] strikteren Vorgaben – sei es beim (1) „Ob“ der Verarbeitung oder beim (2) „Wie“ der Verarbeitungsmodalitäten – als „lediglich“ reguläre personenbezogene Daten bei ihrer Verarbeitung unterliegen, scheint treffend. Folglich werden die in **Art. 9 DSGVO engeren Verarbeitungstatbestände** aktiviert und ziehen bereits beim „Ob“ der Gesundheitsdatenverarbeitung striktere Grenzen als die in Art. 6 DSGVO verankerten Regelungen zur „Rechtmäßigkeit der Datenverarbeitung“.

Explizite Verschärfungen erschließen sich unter anderem aus Art. 6 Abs. 4 lit. c) (Zweckänderungen), Art. 22 Abs. 4 (automatisierte Entscheidungen), Art. 30 Abs. 5

12 *M. Martini/M. Hohmann*, NJW 2020, 3573 (3574).

13 Nach der vollständigen Definition stellt eine „‚Verarbeitung‘ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“ dar.

14 Für die vorliegende Studie erweisen sich insbesondere die sogenannten „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).

15 Vgl. zudem Erwägungsgrund 35 DSGVO.

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

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

(Dokumentationspflicht), Art. 35 Abs. 3 lit. b) (Datenschutz-Folgenabschätzung) und Art. 37 Abs. 1 lit. c) (obligatorischer Datenschutzbeauftragter) DSGVO.[18] Neben den soeben benannten expliziten Verschärfungen können allerdings auch implizite miteinhergehen, etwa wenn Verarbeitungsregeln die Berücksichtigung der Schwere der mit der Verarbeitung verbundenen Risiken für die Betroffenen einfordern (z.B. Art. 24 Abs. 1 sowie Art. 25 Abs. 1 und 2 DSGVO) – diese Schwere hängt u.a. auch von der Art der verarbeiteten Daten ab.[19]

Ob die DSGVO auf die Verarbeitung von Daten im Zusammenhang mit digitalen Anwendungen im Gesundheitswesen wie der ePA, der eGK oder der Telematikinfrastruktur 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, da die Festlegung der Gesundheitspolitik sowie die Organisation des Gesundheitswesens und die medizinische Versorgung aus Art. 168 Abs. 7 Satz 1 und 2 AEUV ersichtlich Sache der Mitgliedstaaten sei und die Verarbeitung von ePA-Daten somit gemäß dem kompetenzrechtlich zu interpretierenden Ausnahmetatbestand in Art. 2 Abs. 2 lit. a) DSGVO nicht in den Anwendungsbereich des Unionsrechts falle.[20] Auch wenn diese Frage mit Rücksicht auf die sehr enge, von den Regelungskompetenzen des Unionsgesetzgebers gelöste Interpretation jenes Ausnahmetatbestands durch den EuGH richtigerweise zu bejahen sein dürfte,[21] kann ihre Beantwortung vorliegend letztlich offenbleiben, da die DSGVO jedenfalls mittelbar über die Verweisung in § 35 Abs. 2 Satz 2 SGB I Anwendung findet.[22]

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. Auf nähere Einzelheiten wird an dieser Stelle verzichtet, da diese den Kern der datenschutzrechtlichen Beurteilungen der wesentlichen Gestaltungsoptionen bilden werden.

18 Vgl. die Aufzählung bei *M. Albers/R. Veit*, in: H. A. Wolff/S. Brink (Hrsg.), BeckOK Datenschutzrecht, Stand 1.11.2021, Art. 9 DSGVO Rn. 3.

19 Vgl. allgemein etwa *M. Martini*, in: B. Paal/D. A. Pauly (Hrsg.), DSGVO/BDSG, 3. Aufl. 2021, Art. 24 Rn. 32b.

20 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).

21 Vgl. bereits die Ausführungen 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. 83, Fn. 168: Nach den schon zur Datenschutzrichtlinie ergangenen Grundsatzentscheidungen des EuGH (dazu grundlegend EuGH, Urteil vom 20.5.2003 – C-465/00, C-138/01 und C-139/01, EU:C:2003:294, Rn. 39 ff.; Urteil vom 6.11.2003 – C-101/01, EU:C:2003:596, Rn. 37 ff.), deren Aussagen der Gerichtshof mittlerweile auch auf die DSGVO überträgt (dazu EuGH, Urteil vom 22.6.2021 – C-439/19, EU:C:2021:504, Rn. 54 ff.), setzt die Anwendbarkeit des europäischen Datenschutzrechts im Einzelfall keine positive Zuweisung der Datenverarbeitung zum Anwendungsbereich des Unionsrechts voraus, etwa durch einen konkreten Bezug zu den Grundfreiheiten; vielmehr sollen durch Art. 2 Abs. 2 lit. a) DSGVO nur Verarbeitungen ausgenommen werden, die spezifischen, den Fällen von Art. 2 Abs. 2 lit. b) DSGVO (gemeinsame Außen- und Sicherheitspolitik der Union) oder Art. 2 Abs. 2 lit. d) DSGVO (Strafrecht und Strafvollzug, Gefahrenabwehr) vergleichbaren Tätigkeiten der Union oder Mitgliedstaaten zuzuordnen sind (z. B. die nationale Sicherheit betreffende Tätigkeiten).

22 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.

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 zu beachten.

2.2.1 Grundrechte des Grundgesetzes

2.2.1.1 Anwendbarkeit grundgesetzlicher Grundrechte

Als Quelle für diese Wertungen kommen zunächst die Grundrechte des Grundgesetzes in Betracht. Zwar genießt das primäre und sekundäre Unionsrecht prinzipiell Vorrang gegenüber nationalem Recht, einschließlich des nationalen Verfassungsrechts. Allerdings hat das Bundesverfassungsgericht 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.[23] Denn wo das Unionsrecht den Mitgliedstaaten rechtliche Gestaltungsspielräume einräumt, zielen die Unionsgrundrechte regelmäßig nicht auf eine Einheitlichkeit des Grundrechtsschutzes ab, sondern lassen „Grundrechtsvielfalt“ zu. Es gilt dann die Vermutung, dass das Schutzniveau der Charta der Grundrechte der Europäischen Union durch die Anwendung der Grundrechte des Grundgesetzes mitgewährleistet wird.

Die sachlich einschlägigen Grundrechte der **Grundrechtecharta** sind allerdings **subsidiär** danach zu befragen, ob sie über die Gewährleistungen des Grundgesetzes hinaus ein „Mehr an Schutz“ bieten. Die Grundrechte des Grundgesetzes und die Charta-Grundrechte sind bei unionsrechtlich nicht vollständig determinierten staatlichen Maßnahmen somit – im Unterschied zur früheren Rechtsprechung[24] – grundsätzlich **parallel anwendbar**. Praktisch dürfte sich aus den Charta-Grundrechten freilich nur selten ein weitergehender Grundrechtsschutz ergeben.

Im Kontext von Datenverarbeitungen in der ePA ist den mitgliedstaatlichen Gesetzgebern in der Tat ein deutlicher Regelungsspielraum eröffnet. So überlassen es die für die Operationalisierung der ePA relevanten Erlaubnistatbestände des Art. 9 Abs. 2 lit. b) sowie lit. g) bis j) DSGVO weitgehend dem nationalen Recht, wie die Verarbeitungsgrundlagen zu gestalten sind. Maßgaben für das mitgliedstaatliche Recht enthalten sie in erster Linie in Form von ihrerseits ausgestaltungsbedürftigen unbestimmten Rechtsbegriffen (z.B. „in angemessenem Verhältnis zu dem verfolgten Ziel“, „angemessene und spezifische Maß-

23 Vgl. BVerfG, 6.11.2019 – 1 BvR 16/13 (1. Leitsatz).

24 Früher galt insoweit ein strenges „Trennungsprinzip“: Soweit die unionsrechtliche Determinierung reichte, sollten allein die Unionsgrundrechte maßgeblich sein; soweit das Unionsrecht den Mitgliedstaaten Spielräume überließ, sollten allein die Grundrechte des Grundgesetzes maßgeblich sein. Vgl. dazu BVerfGE 118, 79 (Rn. 95 ff.) – „Emissionshandel“; für eine Maßgeblichkeit ausschließlich der Unionsgrundrechte wohl EuGH, Urteil vom 24.3.1994 – C-2/92, EU:C:1994:116, Rn. 16.

nahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person", „Bedingungen und Garantien").[25] Relevant erscheint auch Art. 9 Abs. 4 DSGVO, wonach das mitgliedstaatliche Recht für die Verarbeitung von Gesundheitsdaten auch zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten kann. Die genannten Verarbeitungsgrundlagen stellen insoweit „nur" einen Mindeststandard dar: Daher hat die DSGVO bei abweichenden (strengeren) Regelungen der mitgliedstaatlichen Gesetzgeber zurückzutreten. Für die Anwendbarkeit grundrechtlicher Wertungen des Grundgesetzes dürfte somit ein hinreichender Spielraum bestehen.

2.2.1.2 Recht auf informationelle Selbstbestimmung und Recht auf körperliche Unversehrtheit

Maßgeblich dürfte dabei vor allem das Grundrecht auf informationelle Selbstbestimmung sein, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.[26] 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".[27] 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. Diesbezüglich hat das Bundesverfassungsgericht ausgeführt, dass

„Einschränkungen […] im überwiegenden Allgemeininteresse zulässig [sind]. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken."[28]

Für die Ausgestaltung der ePA bedeutet dies – erstens –, dass der deutsche Gesetzgeber auch aus grundrechtlichen Gründen besondere Sorgfalt auf eine **für den Patienten transparente** Nutzung der ePA verwenden muss. Darüber hinaus hat er – zweitens – jede konkrete Gestaltungsoption einer **Verhältnismäßigkeitsprüfung** zu unterziehen, die die Intensität von Beeinträchtigungen der informationellen Selbstbestimmung und die Gewichtigkeit der Eingriffsziele in Bezug zueinander setzt. Und schließlich muss er – drittens – gleichsam einen „Grundrechtsschutz durch Verfahren" gewährleisten, indem er **spezifische organisatorische und technische Vorkehrungen** trifft, um das Risiko unverhältnismäßiger und damit verfassungswidriger Eingriffe im Einzelfall von vornherein zu minimieren.

Von besonderer Relevanz für die datenschutzrechtliche Beurteilung der denkbaren ePA-Gestaltungen dürfte vor allem der **Verhältnismäßigkeitsgrundsatz** sein. Dieser verlangt insbesondere eine Beschränkung von Beeinträchtigungen der informationellen

25 *D. Kampert*, in: G. Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 9 Rn. 58 ff.

26 Vgl. auch *J. Eichenhofer*, NVwZ 2021, 1090 (1093 f.).

27 BVerfGE 65, 1 (Rn. 146 f.).

28 BVerfGE 65, 1 (2. Leitsatz).

Selbstbestimmung auf das **erforderliche Maß** sowie ein **angemessenes Verhältnis** zwischen der Eingriffsintensität und dem Gewicht der Eingriffszwecke.

Die **Eingriffsintensität** hängt dabei von verschiedenen Faktoren ab. Relevant ist zunächst in subjektiver Hinsicht, in welchem Ausmaß der Einzelne über seine Daten **bestimmen** kann beziehungsweise über die Erhebung und Verarbeitung seiner Daten **Kenntnis** erlangt. Demzufolge besteht etwa eine tendenziell hohe Intensität des Grundrechtseingriffs, wenn der Einzelne schon gar nicht über die Verarbeitung seiner Daten in Kenntnis gesetzt wird, da er keine Möglichkeit der „Mitbestimmung" innehat (Nichtwissen). Die geringste Eingriffstiefe weist demgegenüber die Freiwilligkeit der Preisgabe der Daten auf.[29]
Neben diesem subjektiven Element sind weitere, mehr objektive Gesichtspunkte für die Eingriffstiefe von Relevanz. Entscheidend ist insbesondere, um welche **Art von Daten** es sich handelt. Gesundheitsdaten dürften bereits per se als besonders sensibel einzuordnen sein. Innerhalb der Gesundheitsdaten wird man überdies weiter differenzieren können und müssen, etwa mit Blick auf Informationen zu besonders persönlichkeitsrelevanten Krankheitsbildern (z.B. HIV-Infektionen, psychischen Erkrankungen oder Geschlechtskrankheiten). Relevant ist überdies der Umfang der verarbeiteten Informationen, ferner die **Art der Verarbeitung** und die **Dauer** der Speicherung der Daten, die vorgesehenen und denkbaren **Verwendungszwecke** sowie die konkreten und abstrakten **Missbrauchsgefahren**.[30]

Der auf diese Weise ermittelten Intensität eines Eingriffs in die informationelle Selbstbestimmung muss jeweils ein hinreichend **gewichtiger Eingriffszweck** gegenüberstehen. In Betracht kommen dabei einerseits hochrangige öffentliche Interessen, insbesondere die Gewährleistung einer **qualitativ hochwertigen Gesundheitsversorgung** auf möglichst vollständiger und breiter informationeller Basis, die neben individuellen Verbesserungen für den einzelnen Patienten auch Vorteile für die Allgemeinheit generiert: Eine hochwertige Gesundheitsversorgung unter allgemein verfügbarer Nutzung einer ePA kann mittel- und langfristig erhebliche finanzielle Entlastungen für das **Gesundheitssystem insgesamt** bewirken (Stichworte sind etwa: die Vermeidung unnötiger Doppeluntersuchungen[31] und unnötiger Therapiemaßnahmen durch frühzeitige Krankheitserkennung und gezielte, auch vorsorgende Behandlung).

Andererseits und zumindest ergänzend lassen sich auch individuelle Belange anführen, die konkrete Gestaltungsoptionen der ePA rechtfertigen können. Eine erhöhte Verfügbarkeit von Informationen über die eigene Gesundheit kann zunächst eine **verbesserte individuelle Behandlung** jedes Einzelnen ermöglichen. Des Weiteren ist in diesem Zusammenhang darauf zu verweisen, dass das Recht auf informationelle Selbstbestimmung nicht nur als ein Abwehrrecht gegen die Verarbeitung der eigenen Gesundheitsdaten in der ePA in Stellung gebracht werden muss, sondern auch als ein **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 Recht korrespondiert letztlich mit der viel zitierten **Patientensouveränität**: Um das letztlich im Recht auf körperliche Unversehrtheit aus Art. 2 Abs. 2 Satz 1 GG wur-

29 Vgl. *S. Polenz*, in: J. Taeger/J. Pohle (Hrsg.), Computerrechts-Handbuch, 2021, Teil 13 Rn. 15 ff.

30 Siehe Näheres in *S. Polenz*, in: J. Taeger/J. Pohle (Hrsg.), Computerrechts-Handbuch, 2021, Teil 13 Rn. 17.

31 Vgl. *J. Eichenhofer*, NVwZ 2021, 1090 (1092).

zelnde Selbstbestimmungsrecht bezüglich der eigenen Gesundheit[32] 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 dem Aspekt der Patientensouveränität. Diese beiden Prinzipien sollten insoweit keineswegs nur als gegenläufige Handlungszwecke begriffen werden.

2.2.1.3 Recht auf Dateneigentum?

In Anbetracht der sehr weitreichenden, auf eine – wenn auch keineswegs unbeschränkte – „Herrschaft" des Einzelnen „über ‚seine' Daten"[33] hinauslaufenden Gewährleistungen, die bereits mit dem Recht auf informationelle Selbstbestimmung verbunden sind, kann letztlich dahinstehen, ob darüber hinaus auch ein (vermögensrechtliches) „Recht auf Dateneigentum" des Einzelnen an seinen Gesundheitsdaten in der ePA anzuerkennen ist. Denn ungeachtet der konzeptionellen Schwierigkeiten bei der Konstruktion eines im Schrifttum jedenfalls *de lege lata* wohl überwiegend abgelehnten gesonderten Rechts auf Dateneigentum[34] dürften sich daraus jedenfalls keine weitergehenden Einschränkungen für die Ausgestaltung der ePA ergeben, als sie bereits aus der informationellen Selbstbestimmung folgen.

2.2.2 Charta der Grundrechte der Europäischen Union

Parallel und subsidiär zu den Grundrechten des Grundgesetzes kommen nach der Rechtsprechung des Bundesverfassungsgerichts auch in unionsrechtlich nicht vollständig determinierten Fragen zusätzlich die Rechte der europäischen Grundrechtecharta zur Anwendung. Die Charta schützt in Art. 7 GRC zunächst ein mit Art. 8 EMRK wortlautidentisches Recht auf Achtung des Privatlebens.[35] Der Gewährleistungsgehalt des Charta-Rechts entspricht insoweit grundsätzlich demjenigen des Art. 8 EMRK.[36]

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

33 So unter Hinweis auf die Einschränkbarkeit der informationellen Selbstbestimmung bereits BVerfGE 65, 1 (Rn. 148 f.).

34 Bei der Diskussion um ein „Dateneigentum" geht es bei genauerem Hinsehen um teils sehr unterschiedliche Konzepte einer – in aller Regel nicht *de lege lata* vorgefundenen, sondern *de lege ferenda* vorgeschlagenen – privatrechtlichen Zuordnung von Daten zu einer Person, die in Ansehung dieser Daten – in gewisser Parallelisierung zum Sacheigentum – umfassend ausschluss-, verfügungs- und/oder nutzungsberechtigt sein soll. Vgl. zum Ganzen etwa *N. Härting*, CR 2016, 646 (646 ff.); *T. Hoeren*, MMR 2019, 5 (5 ff.); *J. Kühling/F. Sackmann*, ZD 2020, 24 (24 ff.); aus verfassungsrechtlicher Perspektive *C. Krönke*, in: ders./M. W. Müller/W. Yu/W. Tian (Hrsg,), Paradigms of Internet Regulation in the European Union and China, 2018, S. 83 (90 ff.). In der (mittlerweile wieder abgeflachten) rechtspolitischen Diskussion konnte sich – unseres Erachtens zu Recht – keines dieser Konzepte durchsetzen.

35 Vgl. dazu und zum Folgenden auch *D. Lorenz/C. Krönke*, in: Bonner Kommentar, 213. Aktualisierung 2021, Art. 2 Rn. 7.

36 Vgl. *H. D. Jarass*, Charta der Grundrechte der EU, 4. Aufl. 2021, Art. 7 Rn. 1 f.; 9; *I. Augsberg*, in: H. von der Groeben/J. Schwarze/A. Hatje (Hrsg.), Europäisches Unionsrecht, 7. Aufl. 2015, Art. 7 GRC Rn. 5.

Einen Teilschutzbereich dieses Rechts bildet die Selbstbestimmung des Einzelnen in informationeller Hinsicht. Hier zeigen sich mittlerweile beachtliche Parallelen zwischen der Rechtsprechung des Bundesverfassungsgerichts und des EGMR. So hat der Gerichtshof beispielsweise in seiner Entscheidung in der Sache „Satakunnan Markkinapörssi“ (2017) in Bezug auf die Veröffentlichung massenhafter Steuerdaten explizit festgehalten, dass Art. 8 EMRK „das Recht auf eine Art informationeller Selbstbestimmung“ gewährleiste und es Personen gestatte, sich auf ihr Recht auf Privatheit zu berufen, wenn eine Verarbeitung personenbezogener Daten im Raume steht, die das Privatleben im Sinne der Konvention betreffen.[37]

Zusätzlich enthält die Charta überdies ein eigenständiges explizites Grundrecht auf Schutz der personenbezogenen Daten in Art. 8 GRC. Dessen Schutzbereich ist denkbar umfassend gezogen, da von Art. 8 GRC nicht nur Daten geschützt sind, die die Privatsphäre betreffen, sondern darüber hinaus auch jedwede sonstigen personenbezogenen Daten. Mit Blick auf die Verarbeitung von Gesundheitsdaten in elektronischen Patientenakten ergeben sich aus Art. 7 und 8 GRC allerdings, soweit ersichtlich, keine weitergehenden Gewährleistungen als aus dem grundgesetzlichen Recht auf informationelle Selbstbestimmung.[38]

37 EGMR, U 27.6.2017, *Satakunnan Markkinapörssi Oy u a*, Nr 931/13, Rn. 136 f.

38 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“.

3 Anlage und Befüllung der ePA

Vor dem Hintergrund dieser rechtlichen Rahmenbedingungen lässt sich im Folgenden untersuchen, 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 (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.[39] Nach Darstellung der wesentlichen denkbaren Gestaltungsoptionen (»3.1) werden diese datenschutzrechtlich bewertet (»3.2).

3.1 Wesentliche denkbare Gestaltungsoptionen

Als Gestaltungsoptionen im Kontext der Anlage und Befüllung der ePA erscheinen insbesondere erwägenswert die automatische, einwilligungsunabhängige Anlage und Befüllung mit gesondertem Registrierungserfordernis oder ohne Registrierungserfordernis (»3.1.1), eine unterschiedslose Befüllung mit sämtlichen Gesundheitsdaten (im Folgenden: „All-in-Lösung") oder eine nach Datenkategorien differenzierte Befüllung (»3.1.2) sowie eine Befüllung lediglich „ex nunc" oder eine Befüllung auch „ex tunc" (»3.1.3). Dabei ist zu berücksichtigen, dass die genannten Optionen gesondert voneinander zu betrachten sind und jeweils miteinander kombiniert werden können.

3.1.1 Automatische Anlage und Befüllung ohne / mit Registrierungserfordernis

Im logisch ersten Schritt geht es um die Frage, wie die Anlage und in weiterer Folge die Befüllung des leeren virtuellen „Aktenordners" vonstattengehen kann. Zum einen

39 Mit Blick auf den Terminus „Befüllung" lässt sich differenzieren zwischen der Erstbefüllung und allen nachgelagerten Befüllungen. Lediglich die erstmalige Einspeisung bzw. Übermittlung von (medizinischen) Daten in die ePA wird als Erstbefüllung bezeichnet. Alle danach stattfindenden Einspeisungen von (Gesundheits-)Daten werden unter dem Oberbegriff der Befüllung zusammengefasst. Siehe zur Differenzierung zwischen Erstbefüllung und allen nachgelagerten Befüllungen die Vereinbarung über die Abrechnungsvoraussetzungen und -verfahren zur Erstbefüllung der elektronischen Patientenakte gemäß § 346 Abs. 6 SGB V (ePA-Erstbefüllungsvereinbarung) vom 25.8.2021.

ist eine vollständige Operationalisierung der ePA ohne Zutun des Patienten vorstellbar. In dieser Konstellation wird ein leerer virtueller „Aktenordner“ für die Versicherten ohne ihr gesondertes Zutun angelegt und beim Kontakt mit schreibberechtigten Leistungserbringern mit Gesundheitsdaten (erst-)befüllt. Ob diese Befüllung in der Gestaltungsoption des „All-in“ oder im Rahmen einer differenzierten Befüllung erfolgt, steht offen und bedarf einer gesonderten Betrachtung (siehe unten Punkt »3.1.2). Der Patient bzw. die Patientin erhält damit ohne eigenes Zutun eine für ihn oder sie angelegte ePA, die auch **ohne gesonderte Registrierung** befüllt wird.

Auf den ersten Blick könnte dies zu einer Beeinträchtigung des informationellen Selbstbestimmungsrechts der Patienten führen, da gleichsam „hinter ihrem Rücken“ ihre Patientenakte von Leistungserbringern mit sensiblen, gesundheitsbezogenen Daten befüllt würde und die Identität des/der Versicherten ohne Registrierung zudem nicht gesondert geprüft würde. Doch gerade die automatische ePA-Befüllung ohne weiteres aktives Zutun der Patientinnen und Patienten schafft eine weitgehend vollständige gesundheitsinformationelle Basis für eine qualitativ hochwertige, allgemein zugängliche und langfristig selbstbestimmte individuelle Gesundheitsversorgung, wie sie jedem modernen elektronischen Patientenaktensystem vorschwebt. Vor dem Hintergrund einer effektiven Ausgestaltung der ePA scheint diese Gestaltungsoption – vorbehaltlich ihrer datenschutzrechtlichen Bewertung – grundsätzlich vorzugswürdig.

Zum anderen und alternativ könnte daran gedacht werden, die Befüllung der ePA an ein Registrierungserfordernis zu knüpfen. Die ePA würde dann nach erfolgter Anlegung zunächst in einem „Schlafmodus“ belassen. Um sie „aufzuwecken“, bedürfte es einer **aktiven Registrierung** des jeweiligen Patienten. Es erfolgte demnach keine an die Anlegung anschließende automatische (Erst-)Befüllung; vielmehr wird die ePA erst nach der Registrierung befüllt. Möglichkeiten zur Registrierung könnten bei ausgewählten Registrierungsstellen eingerichtet werden – etwa bei Leistungserbringern, Krankenkassen, bei Behörden oder rein digital mittels eines mobilen Endgerätes. Sicherzustellen wäre, dass eine sichere Identifizierung[40] der Person stattfindet und auch nur diese die Zugangsschlüssel für die ePA erhält. Diese Gestaltungsoption käme letztlich einem stillen Opt-out bzw. einem „unechten“ Opt-in gleich: Wenn und solange die betroffene Person keine Registrierung vornimmt, kann die ePA nicht genutzt werden. Ein solcher „unechter“ Opt-in würde der ePA folglich – wie auch das derzeit vorgesehene „echte“ Opt-in-Konzept – keine hohe Effektivität verleihen. Zu denken ist dabei etwa an jene Menschen ohne (Vor-)Erkrankung, die sich nicht intensiv mit der ePA bzw. ihrer Gesundheit auseinandersetzen, da sie keinen Mehrwert für sich darin erblicken, und keinen Aufwand für das Aktivieren („Aufwecken“) der ePA betreiben möchten. Dass für eine optimale Versorgung auch dieser Menschen auf eine weitgehend vollständige gesundheitsinformationelle Basis zurückgegriffen werden kann, lässt sich nur durch eine von Beginn an vollständige ePA

40 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 sogenannte **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 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.

gewährleisten, deren Befüllung von möglichst wenigen aktiven Handlungen der Patienten (wie insbesondere einer Registrierung) abhängig gemacht wird.[41]

Fallbeispiel: Nach Einführung der ePA muss für Anna zunächst ein virtueller „Aktenordner" angelegt werden, der dann mit ihren (Gesundheits-)Daten befüllt werden kann – insbesondere etwa mit ihren Befunden aus der Stadt B (MRT, Blut, EKG, Blutdruck, HNO, Neurologie). Hierbei bestünde zum einen die Möglichkeit, dass die Akte für sie ohne ihr gesondertes Zutun angelegt und beim Kontakt mit dem schreibberechtigten Leistungserbringer in B automatisch mit den Gesundheitsdaten befüllt wird. Zum anderen könnte die Akte zwar angelegt werden, die Befüllung mit ihren Befunden aus B allerdings an ein gesondertes Registrierungserfordernis ihrerseits geknüpft sein. Wenn Anna sich für ihre ePA vor dem Besuch in B nicht registriert hat und ihre ePA noch nicht aus dem „Schlafmodus" geweckt hat, werden die Befunde in B nicht in die ePA eingespeist. Eine gesonderte Registrierung müsste Anna dann zunächst bei ausgewählten Registrierungsstellen (z. B. bei ihren Leistungserbringern in A und B oder digital über ihr mobiles Endgerät) vornehmen.

3.1.2 „All-in-Lösung" oder differenzierte Befüllung

Unabhängig vom ersten Schritt – der Anlage der ePA – stellt sich im zweiten Schritt die Frage, wie die Befüllung des leeren virtuellen „Aktenordners" ausgestaltet sein kann. Dabei sind insbesondere bei der Befüllung der ePA mit Gesundheitsdaten mehrere Gestaltungsoptionen denkbar, um der Idee eines fach- und sektorenübergreifenden Behandelns durch mehrere Leistungserbringer gerecht werden zu können. Im Wesentlichen kann zwischen einer „All-in-Lösung" (»3.1.2.1) und einer differenzierten Befüllung (»3.1.2.2) unterschieden werden.

3.1.2.1 „All-in-Lösung"

Im Rahmen einer „All-in-Lösung" (zu Deutsch: „alles inbegriffen") könnte das Prinzip verfolgt werden, nach der Anlage der ePA **unterschiedslos** alle Gesundheitsdaten (Arztbriefe, Befunde, MRT-Bilder etc.) einzuspeisen. Dies schafft eine für die Versicherten ohne Zutun weitgehend vollständige gesundheitsinformationelle Basis.

Fallbeispiel: Nachdem für Anna der „Aktenordner" angelegt wurde, würden bei Einführung einer „All-in-Lösung" alle ihre Gesundheitsdaten – also die Befunde aus B (MRT, Blut, EKG, Blutdruck, Neurologie) sowie die Daten aus A (Blut, Diagnose einer Angststörung) – unterschiedslos in ihre ePA eingespeist.

41 Vgl. hierzu etwa die im Auftrag der Bertelsmann Stiftung abgegebene Expertise von *P. Haas*, in: Stiftung Münch (Hrsg.), Elektronische Patientenakten, 2017, 143 f.

3.1.2.2 Differenzierte Befüllung

Um etwaigen Bedürfnissen des Datenschutzes Rechnung zu tragen, beststeht alternativ die Möglichkeit einer **differenzierten Befüllung**.[42] Anders als bei der „All-in"-Gestaltungsoption erfolgt keine unterschiedslose Befüllung der ePA mit sämtlichen Gesundheitsdaten, sondern – je nach Sensibilität der einzuspeisenden Daten – eine differenzierte Befüllung. Dabei sind verschiedene Suboptionen vorstellbar. Vor der Einspeisung besonders sensibler Gesundheitsdaten (z.B. die Diagnose einer psychischen Erkrankung oder einer HIV-Infektion) könnte der Leistungserbringer beispielsweise dazu verpflichtet werden, der betroffenen Person einen **punktuellen Hinweis auf die Möglichkeit eines situativen Opt-out** bezüglich der besonders sensiblen Informationen zu erteilen.[43] Ebenso denkbar wäre die Möglichkeit, für solche Situationen das Erfordernis eines **punktuellen Opt-in** vorzusehen.

Ferner könnte die differenzierte Befüllung der ePA über **punktuelle Verschattungen oder Ausblendungen** erfolgen, d.h. bestimmte, besonders sensible Gesundheitsdaten würden „verschattet" oder ausgeblendet und könnten in der Folge lediglich vom Patienten selbst eingesehen werden; andere Zugriffsberechtigte könnten diese Informationen entweder gar nicht einsehen (völlige Ausblendung) oder allenfalls sehen, *dass* Daten gespeichert wurden, hätten aber keinen Zugriff auf die konkreten Inhalte („Verschattung"). Erst durch die Aufhebung der punktuellen Ausblendung bzw. „Verschattung" durch die Patientin oder den Patienten wäre etwa eine sensible Diagnose für alle Teilnahmeberechtigten der ePA einsehbar. Ob bei punktuell durchgeführten „Verschattungen" z.B. andere Leistungserbringer, wie beispielsweise in Spanien[44], einen Warnhinweis über die „Verschattung" erhalten – allerdings keine nähere Information über die dahinterstehenden Gesundheitsdatensätze –, kann hier offenbleiben (siehe zur Thematik möglicher Ausblendungen bzw. „Verschattungen" ausführlich Punkt »5.1.3.2).

Die Spielart einer punktuellen Ausblendung bzw. „Verschattung" kann auch mit den anderen beiden Gestaltungsoptionen der differenzierten Befüllung verknüpft werden. Denkbar wäre beispielsweise eine Variante, bei der der Patient die Ausblendung bzw. „Verschattung" nach entsprechendem obligatorischem Hinweis des Leistungserbringers gesondert anordnen müsste.

Fallbeispiel: Im Unterschied zur „All-in-Lösung" wäre ebenso denkbar, dass Annas Gesundheitsdaten nicht unterschiedslos, sondern differenziert, je nach Sensibilität der Daten, in ihre ePA eingespeist würden. Anders als etwa mit Blick auf die Blutbefunde könnte ihr Hausarzt in der Stadt A beispielsweise gesetzlich dazu angehalten werden, Anna vor einem Eintrag der

42 Die „punktuelle[n] Hinweise auf Opt-out" sowie die „punktuelle[n] Opt-ins" bzw. die punktuellen Verschattungen sind nicht nur mit Bezug auf die Informationen von Relevanz, sondern auch für die Teilnahmeberechtigten. Der Übersichtlichkeit halber wird allerdings auf Letztere unter „4. Berechtigung zum Zugriff auf die ePA" näher eingegangen.

43 Zum Vergleich: In Österreich bestehen im Opt-out-Modell drei Möglichkeiten des Widerspruchs: generell (Hinausoptierung aus allen ELGA-Anwendungen), partiell (Hinausoptierung aus einer oder mehreren ELGA-Anwendungen) sowie situativ (die Teilnehmer können beim Besuch eines Gesundheitsdiensteanbieters situativ der Registrierung von Dokumenten widersprechen – gilt für alle Dokumente des Besuches). Siehe *ELGA GmbH*, ELGA-Gesamtarchitektur, 2017, S. 322 f.

44 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. 114.

Diagnose einer Angststörung in ihre ePA darauf hinzuweisen, dass sie die Möglichkeit hat, diesem Eintrag zu widersprechen. Da eine Angststörung als psychische Erkrankung in besonderer Weise Annas Persönlichkeitsrechte berührt, könnte es angemessen sein, ihr vor dem Speichern diesbezüglicher Informationen und der damit möglicherweise verbundenen Einsichtsmöglichkeit anderer Leistungserbringer die Gelegenheit zu geben, der Speicherung und weiteren Verwendungen zu widersprechen.

3.1.3 Befüllung „ex nunc“ oder „ex tunc“

Unbeschadet der dargelegten Gestaltungsoptionen könnte eine Befüllung der ePA mit Gesundheitsdaten überdies **„ex nunc“** oder **„ex tunc“**[45] erfolgen. Während eine Befüllung „ex nunc“ erst ab Inkrafttreten der gesetzlichen Bestimmungen zur ePA – bzw. ab Registrierung – in der Form eines Opt-out-Modells vollzogen wird, erfolgt die Befüllung „ex tunc“ mit den Gesundheitsdaten(-sätzen) der Patienten auch rückwirkend. Zu überlegen wäre bei der „ex tunc“-Option, ob die rückwirkende Befüllung freiwillig oder obligatorisch erfolgen soll. Vorstellbar wäre etwa, dass die rückwirkende Befüllung auf **Freiwilligkeit** basiert – also entweder auf Verlangen der Patientinnen und Patienten oder aus eigenem Antrieb der Leistungserbringer erfolgt. Zweifelsfrei kann dies zu einem Spannungsverhältnis zwischen den Interessen der Patienten einerseits sowie den Interessen der Leistungserbringer andererseits führen.

Während der Patient beispielsweise an einer vollständigen gesundheitsinformationellen Basis in seiner ePA interessiert sein könnte, ist denkbar, dass der Leistungserbringer aufgrund des mit der rückwirkenden Befüllung verbundenen Aufwandes[46] einer Befüllung der ePA mit schon lange zurückliegenden Befunden eher abgeneigt gegenübersteht. In diesem Kontext ist daher zu überlegen, ob den Patienten ein Recht auf die rückwirkende Eintragung ihrer Gesundheitsdaten zukommen bzw. dem Leistungserbringer hierzu eine Pflicht treffen soll. Alternativ könnte eine **unbedingte gesetzliche Verpflichtung** zur Befüllung „ex tunc“ vorgegeben werden, ohne Wahlmöglichkeit für Patienten und Leistungserbringer.

Fallbeispiel: Wird Annas ePA erst nach ihrem Besuch in B eingerichtet, würden ihre Befunde aus B (MRT, Blut, EKG, Blutdruck, Neurologie) im Falle einer Befüllung „ex nunc“ nicht in der

45 Die Befüllung „ex tunc“ spricht insbesondere die Erstbefüllung der ePA an, d. h. jene Fälle, in denen bisher für die betroffene Person noch keine ePA angelegt wurde. Im Folgenden ausgeblendet werden jene Fälle, in denen schon eine ePA für den Patienten angelegt und befüllt wurde, dieser sich aber im Nachhinein für einen gänzlichen Opt-out entschied. In solchen Situationen wird z. B. in Österreich von einer „ELGA-freien Zeit“ gesprochen. Beispielsweise haben in Österreich gemäß § 15 Abs. 4 GTelG 2012 die betroffenen Personen nach Widerruf des getätigten Widerspruches keinen Rechtsanspruch auf eine nachträgliche Rückerfassung der Gesundheitsdaten während der „ELGA-freien Zeit“. Dennoch kann eine Rückerfassung stattfinden, sofern sich der Gesundheitsdiensteanbieter dazu bereiterklärt. Vgl. im internationalen Schrifttum *C. Milisits/E. Pfandlsteiner*, in: G. Aigner/A. Kletečka/M. Kletečka-Pulker/M. Memmer (Hrsg.), Handbuch Medizinrecht Kap. I. 9, Stand 1.5.2022, Kap. I. 9.5.9.3.

46 Anzunehmen ist in diesem Kontext, dass Leistungserbringer mit einem digitalen Patientensystem in ihrer Praxis weniger Aufwand bei der rückwirkenden Befüllung der ePA mit Gesundheitsdaten haben werden als jene mit Papieraktenordnern für ihre Patienten.

ePA gespeichert. Erst die Blutbefunde und die Diagnose ihres Hausarztes in A würden eingespeichert. Bei einer Befüllung „ex tunc“ könnten bzw. – je nach Ausgestaltung – müssten dagegen auch die Befunde aus B in die ePA eingespeist werden.

3.2 Datenschutzrechtliche Bewertung

Mit der Implementierung der ePA als Opt-out-Modell wird für die Versicherten automatisch eine ePA eingerichtet. Zuvörderst erfolgt deren Anlage im Sinne eines leeren virtuellen „Aktenordners“. Damit geht noch nicht zwingend die Verarbeitung von Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DSGVO einher. Relevant wird deren Verarbeitung allerdings spätestens bei der Befüllung des „Aktenordners“, d.h. mit der Einspeisung von Gesundheitsdaten(-sätzen) in die ePA. Diese Vorgänge müssen, neben den Rahmenvorgaben des Grundgesetzes sowie den Rechten aus Art. 8 EMRK sowie Art. 7 und 8 GRC, in erster Linie den konkreten Gehalten der DSGVO[47] Rechnung tragen, weshalb auf diese im Folgenden primär eingegangen wird.

In Bezug auf die Anlage und Befüllung der ePA muss, wie allgemein bereits dargelegt wurde, zwischen den Vorgaben in Bezug auf das **„Ob“** und das **„Wie“** der Datenverarbeitung differenziert werden. Bevor die Modalitäten der Anlage und Befüllung nach Maßgabe zumal der Datenschutzgrundsätze – also das „Wie“ der Verarbeitung – bewertet werden, sind zunächst die einschlägigen Grundlagen – betreffend das „Ob“ der Verarbeitung – zu benennen.

3.2.1 Verarbeitungsgrundlage („Ob“)

3.2.1.1 Maßgeblichkeit der gesetzlichen Verarbeitungstatbestände in Art. 9 Abs. 2 DSGVO

Spätestens beim **Befüllen** der ePA mit (vorrangig) Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DSGVO werden mit Blick auf das „Ob“ der Verarbeitung zusätzlich zu Art. 6 DSGVO bzw. stattdessen die strikten Anforderungen des **Art. 9 DSGVO** aktiviert, die nach einer qualifizierten Verarbeitungsgrundlage verlangen. Insbesondere die Verarbeitung von personenbezogenen Gesundheitsdaten erweist sich aufgrund der Informationen „höchstpersönlicher Natur“ mit (kontextbedingt) besonders hohem Schadens- und Diskriminierungspotenzial[48] und zudem sehr ausgeprägter Identifikationskraft aus datenschutzrechtlicher Sicht als besonders delikat. Der Verordnungsgeber scheint die spezifische Schutzbedürftigkeit der Gesundheitsdaten schon in ihrer Existenz und in den Aussageinhalten selbst begründet zu sehen und verbietet folglich die unmittelbare Verarbeitung dieser Daten prinzipiell.[49] Die Annahme beruht unter anderem auf einer Typisierung der Ver-

47 Dass der Anwendungsbereich der DSGVO im Falle der Verarbeitung von (Gesundheits-)Daten im Rahmen der ePA eröffnet ist, wurde bereits unter Punkt »2.1 dargelegt und wird daher an dieser Stelle nicht nochmals näher ausgeführt.

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

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

arbeitungskontexte einerseits sowie der Verwendungsmöglichkeiten der Daten andererseits.[50]

Unbeschadet des **prinzipiellen Verarbeitungsverbots** in Art. 9 Abs. 1 DSGVO ist die Verarbeitung von Gesundheitsdaten ausweislich der **vorgegebenen Verarbeitungstatbestände** des Art. 9 Abs. 2 DSGVO und unter Berücksichtigung der differenzierten Ausführungen in ErwGr 51 ff. der DSGVO trotz der besonderen Sensibilität rechtlich zulässig. Dabei muss freilich der gesteigerten Schutzbedürftigkeit von Gesundheitsdaten angemessen Rechnung getragen werden, wie etwa durch die Vorgabe von geeigneten Garantien und Schutzvorkehrungen aller Art.[51]

Im Kontext der Einführung der ePA als Opt-out-Modell ist die Verarbeitung – hier konkret: die Anlage und Befüllung – unter Verwendung der gesundheitsrelevanten personenbezogenen Daten demnach nur dann zulässig, wenn diese auf einen der Verarbeitungstatbestände des Art. 9 Abs. 2 DSGVO gestützt werden kann. Mit Blick auf die gewünschte Effektivität der ePA in Form eines Opt-out-Modells zu Versorgungszwecken ist die **einwilligungsabhängige** Verarbeitungsgrundlage des **Art. 9 Abs. 2 lit. a) DSGVO** von vornherein auszublenden.[52] Richtigerweise wird man in einer (möglicherweise gesetzlich vorgesehenen) erstmaligen Registrierung oder in der Vorlage der Gesundheitskarte bei einem Leistungserbringer schon keine „eindeutige bestätigende Handlung" im Sinne des Art. 4 Nr. 11 DSGVO sehen dürfen. Jene Handlungen können auch andere Erklärungsgehalte transportieren, etwa den (irrigen) Willen zur Erfüllung einer vermeintlichen Registrierungsobliegenheit, um in den Genuss einer Behandlung zu kommen, oder die schlichte Absicht, dem Arzt die Gesundheitskarte zu Behandlungszwecken vorzulegen.

Selbst wenn man die Eindeutigkeit bejahte, wäre eine Einwilligung nur dann wirksam und tragfähig, wenn der Patient vorab über die wesentlichen Eckpunkte der Datenverarbeitungen unterrichtet würde („in informierter Weise") und eine echte Wahlmöglichkeit auch im Sinne eines Opt-out hätte („freiwillig").[53] Dabei trügen die verantwortlichen Stellen für jeden Einzelfall die Beweislast bezüglich der Wirksamkeit der Einwilligung. Eine rechtssichere flächendeckende Implementierung der ePA auf Einwilligungsbasis erscheint vor diesem Hintergrund schwer vorstellbar.

Bei den **gesetzlichen einwilligungsunabhängigen Verarbeitungstatbeständen** kommen insbesondere Art. 9 Abs. 2 lit. g), h) (i.V.m. Abs. 3) und lit. i) DSGVO in Betracht. Freilich sind diese, trotz des vorhandenen einwilligungsabhängigen Ausnahmetatbestands des

50 Vgl. *M. Albers/R. Veit*, in: H. A. Wolff/S. Brink (Hrsg.), BeckOK Datenschutzrecht, Stand 1.11.2021, Art. 9 DSGVO Rn. 46.

51 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 bewertenden Einführung eines Opt-out-Modells im Kontext der ePA allerdings zu verneinen sein und kann im Folgenden daher ausgeblendet werden.

52 Laut einer Umfrage, die Bitkom Research im November 2021 durchführte, wurde festgestellt, dass zwar 76 % die ePA gern benutzen möchten, allerdings erst 0,5 % der Befragten davon Gebrauch machten. Siehe die Ergebnisse der Umfrage im Auftrag des Digitalverbands Bitkom unter https://www.bitkom-research.de/de/pressemitteilung/dreiviertel-der-deutschen-wollen-elektronische-patientenakte-nutzen.

53 Vgl. hierzu schon die *Artikel 29-Datenschutzgruppe*, Arbeitspapier zur Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA), 00323/07/DE WP 131, 2007, S. 15, die zwischen der „Zustimmung" einerseits sowie der „Einwilligung" im Sinne des Art. 8 Abs. 2 lit. a) der RiL 95/46/EG andererseits differenziert.

Art. 9 Abs. 2 lit. a) DSGVO, für den Gesetzgeber bei der Einführung eines Opt-out-Modells **nicht gesperrt**. Vielmehr stehen, ungeachtet der genannten Reihenfolge in der DSGVO, die Verarbeitungstatbestände prinzipiell gleichberechtigt nebeneinander. Ein über die in den gesetzlichen Verarbeitungsgrundlagen genannten besonderen Tatbestandsvoraussetzungen hinausweisender **„Vorrang von Einwilligungslösungen"** oder ein pauschaler „Vorrang des Opt-in" lässt sich dem geltenden Datenschutzrecht nach herrschender Meinung **nicht** entnehmen.[54] Zwar wird insoweit aus grundrechtlicher Perspektive, welche die Eingriffe in die informationelle Selbstbestimmung sowie in die Rechte aus Art. 7 und 8 GRC auf das notwendige Maß beschränkt, darauf hingewiesen, dass die Einholung einer Einwilligung gegenüber einer Verarbeitung auf rein gesetzlicher Basis ein milderes Mittel sei.[55] Dem ist allerdings entgegenzuhalten, dass eine Einwilligungslösung in Anbetracht der dabei grundsätzlich bestehenden Möglichkeit des Einzelnen, von einer Einwilligung abzusehen und die Verarbeitung damit zu verhindern – und sei es nur aus Bequemlichkeit –, im Vergleich zu einer einwilligungsunabhängigen Verarbeitung auf gesetzlicher Grundlage denknotwendig kein gleich effektives Mittel zur Erreichung der Verarbeitungszwecke darstellt. Die Wahl der Verarbeitungsgrundlage liegt daher richtigerweise im **Gestaltungsspielraum des Gesetzgebers**.

3.2.1.2 Verhältnis der Tatbestände in Art. 9 Abs. 2 lit. g), h) und i) DSGVO

Mit Blick auf die in Betracht kommenden Ausnahmetatbestände des Art. 9 Abs. 2 lit. g), h) (i.V.m. Abs. 3) sowie lit. i) DSGVO ist zunächst auf deren **Verhältnis** zueinander einzugehen. Während **Art. 9 Abs. 2 lit. g) DSGVO** für die Zulässigkeit der Verarbeitung von sensiblen Daten im Allgemeinen ein **erhebliches** öffentliches (unions- und mitgliedstaatliches) Interesse fordert, verlangen die Bestimmungen in Art. 9 Abs. 2 lit. h) und i) DSGVO jeweils nach **spezifischen** Belangen des öffentlichen Interesses.[56] Der Rechtfertigungstatbestand des **Art. 9 Abs. 2 lit. h) i.V.m. Abs. 3 DSGVO** trägt insbesondere der Bedeutung der Gesundheit für die Patienten und der Gesellschaft **insgesamt** Rechnung. Er hat primär die **individuellen Interessen** an einer funktionierenden Gesundheitsversorgung im Blick („Zwecke der Gesundheitsversorgung", „medizinische Diagnostik", „Versorgung oder Behandlung im Gesundheitsbereich").

Demgegenüber legitimiert **Art. 9 Abs. 2 lit. i) DSGVO** die Verarbeitung aus Gründen des genuin **öffentlichen** Gesundheitsinteresses im Bereich der „öffentlichen Gesundheit" (außerdem: „zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung").[57] Art. 9 Abs. 2 lit. i) DSGVO ist daher prinzipiell im Bereich der Gefahrenabwehr bzw. Risikovorsorge sowie der „Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung" einzureihen und gilt als *lex specialis*

54 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; *J. Kühling/B. Buchner*, in: dies. (Hrsg.), DS-GVO BDSG, 3. Aufl. 2020, Art. 7 DSGVO Rn. 16; für einen „Vorrang der Selbstbestimmung" noch *A. Roßnagel/A. Pfitzmann/H. Garstka*, Modernisierung des Datenschutzrechts, 2001, S. 72.

55 Vgl. *P Schantz*, in: S. Simitis/G. Hornung/I. Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 6 DSGVO Rn. 10 f., der die Einwilligung grundsätzlich als milderen Eingriff wertet, allerdings von einer niedrigen Begründungsschwelle für den Rückgriff auf gesetzliche Verarbeitungsgrundlagen ausgeht.

56 Siehe *M. Albers/R. Veit*, in: H. A. Wolff/S. Brink (Hrsg.), BeckOK Datenschutzrecht, Stand 1.11.2021, Art. 9 DSGVO Rn. 88.

57 Vgl. dazu *T. Petri*, in: S. Simitis/G. Hornung/I. Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 9 DSGVO Rn. 78; *M. Albers/R. Veit*, in: H. A. Wolff/S. Brink (Hrsg.), BeckOK Datenschutzrecht, Stand 1.11.2021, Art. 9 DSGVO Rn. 95.

gegenüber dem allgemeinen Tatbestand in Art. 9 Abs. 2 lit. g) DSGVO.[58] Betreffend das Verhältnis zwischen Art. 9 Abs. 2 lit. g) und h) DSGVO zeigt sich mit Blick auf deren Gehalte, dass lit. g) im Wesentlichen dem Schutz des Allgemeininteresses dient und lit. h) insbesondere den Schutz für die Gesundheitsversorgung des Individuums gewährleisten möchte. Die beiden Verarbeitungstatbestände stehen ungeachtet ihrer Reihung prinzipiell gleichberechtigt nebeneinander. Die hinsichtlich der beiden konkretisierungsbedürftigen Begriffe des „öffentlichen Interesses" sowie der „öffentlichen Gesundheit" bestehende tatbestandliche Unbestimmtheit des lit. i) wird insbesondere dadurch entschärft, dass einerseits ErwGr 54 eine Definition[59] des Begriffs der „öffentlichen Gesundheit" inkorporiert und andererseits im Tatbestand selbst bestimmte schutzwürdige „öffentliche Interessen" aufgezählt werden, etwa die Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung.[60] Beachtenswert erscheint zudem, dass ErwGr 54 der DSGVO ausdrücklich festsetzt, dass es „aus Gründen des öffentlichen Interesses in Bereichen der öffentlichen Gesundheit [...] notwendig sein [kann], besondere Kategorien personenbezogener Daten auch ohne Einwilligung der betroffenen Person zu verarbeiten."

Unter Berücksichtigung dieser Maßgaben wird man annehmen können, dass die Anlage der ePA und ihre Befüllung mit (Gesundheits-)Daten zu Versorgungszwecken im Rahmen eines Opt-out-Modells aufgrund des daran bestehenden erheblichen spezifischen öffentlichen Interesses tatbestandlich sowohl durch Art. 9 Abs. 2 lit. g), h) (i.V.m. Abs. 3) DSGOV als auch durch Art. 9 Abs. 2 lit. i) DSGVO legitimiert werden kann. Das **erhebliche spezifische öffentliche Interesse** resultiert mit Blick auf die Anlage und Befüllung der ePA vor allem aus der zu erwartenden Verbesserung der fach- und sektorenübergreifenden Gesundheitsversorgung insgesamt und zu erwartender Effizienz- und Effektivitätsvorteile für das Gesundheitssystem, der Erhöhung der Adhärenz einer Behandlung *lege artis*, der mittel- und langfristigen Stärkung der Patientensouveränität, der Reduktion von Medikationsfehlern bzw. unerwünschten Arzneimittelwirkungen sowie der leichteren und in Echtzeit abrufbaren Verfügbarkeit von (Gesundheits-)Informationen der Versicherten, wodurch eine Verbesserung der diagnostischen und therapeutischen Entscheidungen zu erwarten ist. Zudem scheint ein Arztwechsel leichter vollzogen werden zu können, da die betroffenen Personen ihre Gesundheitsdaten in elektronischer Form immer „bei sich haben".

Diese Verarbeitungszwecke passen gleichermaßen unter die nach lit. h) vorausgesetzten Zwecke der „Gesundheitsversorgung" und der „Diagnostik" wie auch die in lit. i) genannte „Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung". Es steht dem Gesetzgeber somit prinzipiell zunächst **offen**, auf der Basis welcher der beiden Normen – sprich Art. 9 Abs. 2 lit. h) (i.V.m. Abs. 3) oder lit. i) DSGVO – er tätig wird. Auf welche Grundlage die Ausgestaltung eines Opt-out für die Anlage und Befüllung der ePA konkret gestützt werden soll, muss dabei jedenfalls dann

58 Vgl. *M. Albers/R. Veit*, in: H. A. Wolff/S. Brink (Hrsg.), BeckOK Datenschutzrecht, Stand 1.11.2021, Art. 9 DSGVO Rn. 95.

59 Diese lautet: „In diesem Zusammenhang sollte der Begriff ‚öffentliche Gesundheit' im Sinne der Verordnung (EG) Nr. 1338/2008 des Europäischen Parlaments und des Rates [Verordnung (EG) Nr. 1338/2008 des Europäischen Parlaments und des Rates vom 16. Dezember 2008 zu Gemeinschaftsstatistiken über öffentliche Gesundheit und über Gesundheitsschutz und Sicherheit am Arbeitsplatz (ABl. L 354 vom 31.12.2008, S. 70).] ausgelegt werden und alle Elemente im Zusammenhang mit der Gesundheit wie den Gesundheitszustand einschließlich Morbidität und Behinderung, die sich auf diesen Gesundheitszustand auswirkenden Determinanten, den Bedarf an Gesundheitsversorgung, die der Gesundheitsversorgung zugewiesenen Mittel, die Bereitstellung von Gesundheitsversorgungsleistungen und den allgemeinen Zugang zu diesen Leistungen sowie die entsprechenden Ausgaben und die Finanzierung und schließlich die Ursachen der Mortalität einschließen."

60 Vgl. *M. Albers/R. Veit*, in: H. A. Wolff/S. Brink (Hrsg.), BeckOK Datenschutzrecht, Stand 1.11.2021, Art. 9 DSGVO Rn. 95 f.

nicht entschieden werden, wenn die aus diesen beiden Tatbeständen folgenden Anforderungen an die Datenverarbeitungen im Wesentlichen gleichwertig sind. Daher sind jene Anforderungen einander im Folgenden gegenüberzustellen.

Mit Blick auf **Art. 9 Abs. 2 lit. i) DSGVO** wird gefordert, dass die Verarbeitung der sensiblen Daten „aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit […] auf der Grundlage des Unionsrechts oder Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person […] vorsieht, erforderlich" ist. **Art. 9 Abs. 2 lit. h) DSGVO** verlangt demgegenüber, dass „die Verarbeitung […] für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, […], für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich [ist]." Was „angemessene und spezifische Maßnahmen" i.S.v. Art. 9 Abs. 2 lit. i) DSGVO bzw. „Bedingungen und Garantien" sind, wie es in Art. 9 Abs. 2 lit. h) i.V.m. Abs. 3 DSGVO festgeschrieben ist, hängt nicht nur von der Art und Vielzahl der Daten, sondern auch vom jeweiligen Verarbeitungskontext und den eingesetzten Verarbeitungsverfahren sowie Verarbeitungstechniken ab.

Gewiss ist, dass den Gesundheitsdaten eine relativ **hohe Schutzbedürftigkeit** zugeschrieben werden muss. Neben den in Art. 9 Abs. 2 DSGVO jeweils verankerten materiellen Voraussetzungen sind daher unter anderem in Art. 9 Abs. 2 lit. h) und lit. i) DSGVO gewisse Vorbehalte implementiert worden. Diesbezüglich knüpft der Tatbestand des Art. 9 Abs. 2 lit. i) DSGVO an weitergehende legislative Maßnahmen an, nämlich „angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person", und der Tatbestand des Art. 9 Abs. 2 lit. h) i.V.m. Abs. 3 DSGVO fordert unter Verweis auf Absatz 3 „Bedingungen und Garantien".[61] Aufgrund der fehlenden näheren Ausgestaltung der Vorbehalte öffnet dies der Union und den Mitgliedstaaten insoweit einen gewissen **Gestaltungsspielraum**.[62] Diese Öffnung der DSGVO für Gestaltungsoptionen erscheint in der Sache angemessen, denn die Einstufung als „angemessene und spezifische Maßnahme" kann weder abstrakt noch ungeachtet des konkreten Regelungssachverhalts vorgenommen werden.[63] Einen möglichen Anhaltspunkt, was unter einer geeigneten „Garantie" zu verstehen ist, gibt freilich Art. 9 Abs. 2 lit. h) i.V.m. Abs. 3 DSGVO selbst. Dort ist festgesetzt, dass die Verarbeitung nur durch „Fachpersonal oder unter dessen Verantwortung" vorgenommen werden darf. Jedenfalls im Kontext der Gesundheitsversorgung wird man diese Garantie auch bei den anderen Ausnahmetatbeständen des Art. 9 Abs. 2 DSGVO entsprechend zur Anwendung bringen müssen – insbesondere eine „angemessene und spezifische Maßnahme" im Sinne der lit. i) dürfte es sein, Verarbeitungen wie etwa die Befüllung der ePA lediglich „Fachpersonal oder unter dessen Verantwortung" stehenden Personen vorzubehalten. Richtigerweise ist diese Vorgabe somit nicht nur auf den Bereich der individuellen Versorgung im Gesundheitsbereich beschränkt.

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

62 Auch Art. 9 Abs. 4 DSGVO wird trotz der – möglichen – Überschneidungen mit Art. 9 Abs. 3 DSGVO dadurch nicht redundant, vgl. *M. Albers/R. Veit*, in: H. A. Wolff/S. Brink (Hrsg.), BeckOK Datenschutzrecht, Stand 1.11.2021, Art. 9 DSGVO Rn. Rn. 112; *T. Weichert*, in: J. Kühling/B. Buchner (Hrsg.), DS-GVO BDSG, 3. Aufl. 2020, Art. 9 Rn. 150. Aufgrund seiner tatbestandlich-offenen Formulierung behält Abs. 4 seinen eigenständigen Anwendungsbereich bei.

63 So auch *M. Albers/R. Veit*, in: H. A. Wolff/S. Brink (Hrsg.), BeckOK Datenschutzrecht, Stand 1.11.2021, Art. 9 DSGVO Rn. 105 ff.

Bei der Ausfüllung der durch Art. 9 Abs. 2 lit. h) i.V.m. Abs. 3 und lit. i) DSGVO eröffneten **Gestaltungsspielräume** („angemessenen und spezifischen Maßnahmen“ bzw. „Bedingungen und Garantien“) ist der deutsche Gesetzgeber nicht völlig frei. Vielmehr hat er die **Datenschutzgrundsätze** im Sinne des Art. 5 DSGVO einerseits sowie – wie bereits in Abschnitt »2.2 dargelegt – die **Grundrechte** des Grundgesetzes (insbesondere das Recht auf informationelle Selbstbestimmung) sowie ergänzend die Unionsgrundrechte andererseits zu berücksichtigen. Erwägenswert ist zudem, dass die Vorgabe der „angemessenen und spezifischen Maßnahmen“ nicht nur die Anlage und Befüllung selbst betrifft, sondern auch die **nachgelagerten** Verarbeitungen bzw. die nachgelagerten Vorgänge im Blick behalten muss.

3.2.1.3 Zwischenergebnis

Als **Zwischenergebnis** kann daher festgehalten werden, dass es dem deutschen Gesetzgeber bei der Einführung des Opt-out-Modells für die ePA in Bezug auf die Nutzung zu Versorgungszwecken mit Blick auf die Frage des „Ob“ der Verarbeitung im Kontext der Anlage und Befüllung grundsätzlich freistehen dürfte, auf welchen gesetzlichen Verarbeitungstatbestand (Art. 9 Abs. 2 lit. h) i.V.m. Abs. 3 oder lit. i) DSGVO) er sich stützt. Dabei müssen mit Blick auf die Frage des „Wie“ der Datenverarbeitung die jeweiligen gesetzlichen Ausgestaltungen „angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person“ enthalten. Mangels einer exakten Definition von „angemessenen und spezifischen Maßnahmen“ ergibt sich deren Gehalt aus der Zusammenschau der Datenschutzgrundsätze einerseits und der Grundrechte andererseits.

3.2.2 Datenschutzgrundsätze („Wie“)

Im Rahmen der Verarbeitung von (Gesundheits-)Daten müssen ferner vor allem die folgenden **Datenschutzgrundsätze** des Art. 5 DSGVO Beachtung finden: das Gebot der Transparenz der Verarbeitung im Sinne des Abs. 1 lit. a) (dazu »3.2.2.1), der Grundsatz der Zweckfestlegung und -bindung gemäß Abs. 1 lit. b) (dazu »3.2.2.2), die Prinzipien der Datenminimierung nach Abs. 1 lit. c) sowie der Speicherbegrenzung nach Abs. 1 lit. e) (dazu »3.2.2.3), die Richtigkeit der Verarbeitung gemäß Abs. 1 lit. d) (dazu »3.2.2.4), und das Gebot der Integrität und der Vertraulichkeit gemäß Abs. 1 lit. f) (dazu »3.2.2.5). Diese Grundsätze müssen bei jeder Datenverarbeitung erfüllt werden und sind folglich auch für die Befüllung einer ePA im Rahmen eines Opt-out-Modells maßgeblich.[64]

3.2.2.1 Transparenz

Die Anlage und Befüllung der ePA muss zunächst für den Patienten in transparenter Weise erfolgen. Der Grundsatz der Transparenz verlangt im Wesentlichen, dass die Patienten die Datenverarbeitung ihrer (sensiblen) Daten **nachvollziehen** können müssen. Sie sollen in zumutbarer Weise einsehen können, welche Daten von wem, wofür und wie lange verarbeitet werden. Hierbei wird ein prospektiver Ansatz gefordert, d.h. die betrof-

64 Vgl. *P. Schantz*, in: H. A. Wolff/S. Brink (Hrsg.), BeckOK Datenschutzrecht, Stand 1.11.2021, Art. 5 DSGVO Rn. 2.

fenen Personen – Patientinnen und Patienten – müssen schon vorab Kenntnis über die Datenverarbeitung haben. Diese Gehalte entsprechen auch den Anforderungen des grundgesetzlichen Rechts auf informationelle Selbstbestimmung: Bereits im Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahr 1983 wurde die Gefahr benannt, dass die Verhaltensfreiheit des Einzelnen grundlegend gehemmt werden könne, wenn dieser nicht wisse, wer in welcher Weise welche Informationen über ihn besitzt und verarbeitet.[65]

Transparenz verlangt vor diesem Hintergrund zunächst im Rahmen sämtlicher unter Punkt »3.1 dargelegter Gestaltungsoptionen, insbesondere im Kontext der „automatischen Anlage und Befüllung ohne/mit Registrierungserfordernis " sowie der Befüllung „ex nunc" oder „ex tunc", vor allem **Information**. Neben Informationen zum Verantwortlichen i.S.v. Art. 4 Nr. 7 DSGVO – hier: den Krankenkassen –, zu den Empfängern i.S.v. Art. 4 Nr. 9 DSGVO – hier: v.a. den Leistungserbringern – und zu den Verarbeitungszwecken können für die Gewährleistung einer fairen und transparenten Datenverarbeitung auch Informationen relevant sein, die über den Katalog in Art. 13 f. DSGVO hinausgehen.[66] Zudem ist dafür zu sorgen, dass die Informationen für die betroffenen Personen in verständlicher, klarer und einfacher Sprache zur Verfügung gestellt werden. Denkbar wäre etwa, dass die Informationen in verschiedenen Sprachfassungen und/oder mittels „standardisierter Bildsymbole"[67] verfasst werden. Es wird eine adressatengerechte Informationsvermittlung gefordert, wobei keine übermäßigen Anforderungen gestellt werden dürfen, um den Grundsatz nicht gänzlich unerfüllbar zu machen. Insoweit können Informationen z.B. auch von den jeweiligen Krankenkassen bereitgestellt werden.[68]

Dabei wird man die einzelnen Patienten gerade bei solchen Opt-out-Gestaltungen besonders sorgfältig informieren müssen, die zu einer Befüllung der ePA mit Gesundheitsdaten führen, mit der der durchschnittliche Patient nicht ohne Weiteres rechnet. Dies dürfte vor allem dann geboten sein, wenn die ePA **ohne gesonderte Registrierung** gleichsam „hinter dem Rücken" des Patienten beschrieben wird. Denn in einem solchen Falle besteht ein erhöhtes Risiko, dass der Patient von der Anlage und der Befüllung der ePA mit seinen Gesundheitsdaten schlichtweg nicht Kenntnis nimmt. Um den geforderten prospektiven Ansatz der Informationsvermittlung zu wahren, sollte berücksichtigt werden, dass die Patienten schon **vor** der automatischen, einwilligungsunabhängigen Anlage und Befüllung, d.h. vor der Verarbeitung ihrer (Gesundheits-)Daten, ausreichend informiert werden.

65 Das Gericht hielt dort fest: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß" (BVerfGE 65, 1 (Rn 146)).

66 Vgl. *Artikel 29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 17/DE WP 260 rev. 01, 2018, S. 42 sowie *P. Schantz*, in: H. A. Wolff/S. Brink (Hrsg.), BeckOK Datenschutzrecht, Stand 1.11.2021, Art. 5 DSGVO Rn. 10.

67 Gemäß Art. 12 Abs. 7 DSGVO können die Informationen (Art. 13 f. DSGVO) den Patienten auch „in Kombination mit standardisierten Bildsymbolen bereitgestellt werden, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln": Sodann gilt allerdings, dass die in elektronischer Form zur Verfügung gestellten Bildsymbole „maschinenlesbar sein" müssen.

68 Vgl. *Artikel 29-Datenschutzgruppe*, Arbeitspapier zur Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA), 00323/07/DE WP 131, 2007, S. 22.

Aber auch im Falle einer **automatischen Befüllung „ex tunc“** wird man den Patienten schon im Vorfeld der Verarbeitung seiner (Gesundheits-)Daten explizit darauf hinweisen müssen, dass auch bei früheren Gelegenheiten erzeugte Gesundheitsinformationen in die ePA aufgenommen werden (können). Da der Patient in beiden Gestaltungsvarianten indes in zumutbarer Weise von der Befüllung seiner ePA Notiz nehmen kann, dürften sie mit dem Grundsatz der Transparenz der Datenverarbeitung prinzipiell durchaus vereinbar sein.

Zudem scheint mit Blick auf die Gestaltungsoption der **differenzierten Befüllung** – mit den Suboptionen „punktueller Hinweis auf Opt-out“ bzw. „punktuelle Opt-ins“ sowie „punktuelle Verschattungen“ – erwägenswert, dass der Patient die diesbezüglichen Informationen zumeist unmittelbar vor der Verarbeitung seiner (Gesundheits-)Daten erhält. Es erscheint daher, vor allem aufgrund der zumeist besonders schützenswerten Gesundheitsdatensätze, empfehlenswert, die zur Verfügung gestellten Informationen sowohl schriftlich zu übermitteln als auch mündlich anzusprechen. Die schriftliche Informationsvermittlung kann hierbei nicht nur zu Dokumentationszwecken dienen, sondern ebenso der besseren Verständlichkeit und Nachvollziehbarkeit für die Patientinnen und Patienten (ggfs. in Kombination mit einer mündlichen Erörterung der Informationen). Insoweit erhält der Patient, sei es in mündlicher und/oder schriftlicher Form, bereits vorab entsprechende Informationen zur Verarbeitung seiner (Gesundheits-)Daten und kann sich z.B. im Rahmen der differenzierten Befüllung mit „punktuellen Hinweis auf Opt-out“ nach einer entsprechenden Informationsvermittlung auch gegen diese aussprechen.

Solange der Patient seine Entscheidung dabei auf einer transparenten Informationsbasis treffen kann, die ihm in „verständlicher, klarer und einfacher Sprache“ bereitgestellt wird, besteht unseres Erachtens auch dann kein Widerspruch zum Grundsatz der Transparenz, wenn die Informationen erst unmittelbar vor der Verarbeitung der (besonders) sensiblen (Gesundheits-)Daten bereitgestellt werden, der Patient in der Folge möglicherweise unter Zeitdruck gerät und sich im Vorfeld gegebenenfalls nur mit Mühe einen Überblick über die Verarbeitungen verschaffen kann. Denn es bleibt ihm in diesem Falle auch die Möglichkeit, die betreffenden Informationen zumindest **nachträglich** auszublenden bzw. zu verschatten (dazu noch eingehend unter Punkt »5.1.3).

Darüber hinaus muss den betroffenen Personen grundsätzlich eine möglichst einfache und niedrigschwellige **Einsichtsmöglichkeit** in die Verarbeitung ihrer personenbezogenen (Gesundheits-)Daten gegeben werden. Mit Blick auf die oben dargelegten Gestaltungsoptionen könnte diese Anforderung vor allem problematisch sein, wenn die Befüllung der ePA **ohne vorangehende Registrierung** durch den Patienten erfolgt. Verzichtet man auf ein solches Registrierungserfordernis, ist der einzelne Patient bei unterbliebener Registrierung technisch nicht in der Lage, die in seiner ePA automatisch abgelegten Gesundheitsdaten einzusehen. Dies steht in einem gewissen Spannungsverhältnis zur Vorstellung informationeller Selbstbestimmung. Allerdings steht es dem Patienten auch bei Nichtbestehen eines Registrierungs*erfordernisses* durchaus frei, eine Registrierung vorzunehmen und Einsicht in die in seiner ePA abgelegten Informationen zu nehmen. Solange er über den Umstand der automatischen Befüllung der ePA informiert wurde und der tatsächliche Registrierungsaufwand nicht übermäßige Anstrengungen einfordert, erscheint die mit der Befüllung einer nicht aktivierten ePA verbundene Beeinträchtigung der informationellen Selbstbestimmung des Patienten vergleichsweise geringfügig. Ihr steht das gewichtige Interesse gegenüber, die ePA effektiv auszugestalten und die Nachteile eines mit der zwingenden Registrierung einhergehenden „unechten“ Opt-in möglichst zu vermeiden.

Unseres Erachtens ist diese Gestaltung somit durchaus mit dem Transparenzgebot vereinbar.

3.2.2.2 Zweckfestlegung und -bindung

Die dargelegten Gestaltungen müssten ferner mit dem Grundsatz der Zweckfestlegung und -bindung vereinbar sein, also dem „Grundstein des Datenschutzrechts".[69] Maßstäblich ist insoweit zuvörderst das **Gebot der Zweckfestlegung** im Sinne des Art. 5 Abs. 1 lit. b) DSGVO, wonach die personenbezogenen Daten nur „für festgelegte, eindeutige und legitime Zwecke erhoben werden" dürfen. Das daran anschließende Gebot der **Zweckbindung im engeren Sinne** gebietet, dass die personenbezogenen Daten „nicht in einer mit diesen Zwecken [gemeint sind die Erhebungszwecke] nicht zu vereinbarenden Weise weiterverarbeitet werden [dürfen]". Die Bedeutung dieses Grundsatzes wird durch seine Verankerung in Art. 8 Abs. 2 Satz 1 GRC unterstrichen. Eine Speicherung personenbezogener Daten „auf Vorrat zu unbestimmten und noch nicht bestimmbaren Zwecken" ist somit nicht nur nach deutschem Verfassungsrecht[70], sondern auch unionsrechtlich[71] seit jeher unzulässig – auch dann, wenn es – wie hier – um Verarbeitungen in Erfüllung einer öffentlichen Aufgabe geht.[72]

Eine **unzulässige „Vorratsgesundheitsdatenspeicherung"** wird man bei der geplanten Einführung des Opt-out-Modells für die ePA gleichwohl aber **nicht** sehen können. Die Einspeisung und Speicherung der Gesundheitsdaten im Rahmen der Anlage und Befüllung der ePA dienen primär dazu, ordnungsgemäße und qualitativ hochwertige, zum Zeitpunkt der Erhebung gewiss noch nicht im Einzelnen feststehende künftige Behandlungen und sonstige Maßnahmen überhaupt erst zu ermöglichen oder zumindest informationell zu unterstützen. Diese Zweckfestlegung wird man unter Berücksichtigung der jedem abstrakt-generellen Gesetz eigenen relativen Unschärfe genügen lassen, zumal damit die denkbaren Verarbeitungskontexte für alle Beteiligten hinreichend klar abgesteckt sind.[73]

Dabei sollten insbesondere auch die spezifischen praktischen Bedürfnisse im Gesundheitsbereich Berücksichtigung finden. So entspricht es dem Wesen gesundheitsbezogener Informationen, dass ihre Relevanz für eine spätere Versorgung vielfach noch nicht im Zeitpunkt ihrer Erhebung konkret absehbar ist, sondern sich erst nachträglich – dann aber oftmals mit besonderer Vehemenz – offenbart. In solchen Situationen kann es zur Gewährleistung einer hochwertigen und kosteneffizienten Gesundheitsversorgung essenziell sein, auf eine lückenlos dokumentierte Informationsbasis zurückgreifen zu können. Im Wesentlichen besteht der Zweck der Verarbeitung der personenbezogenen (Gesundheits-)Daten – freilich nicht nur im Kontext der Anlage und Befüllung – in der Realisierung der Ziele der erheblichen öffentlichen Interessen, allen voran die Verbesserungen der Qualität[74] und Effizienz in der sektoren- und fachübergreifenden Gesundheitsversorgung. Schon im Zeitpunkt der Erhebung und spätestens im Zeitpunkt der Aufnahme der Ver-

69 *P. Schantz*, in: H. A. Wolff/S. Brink (Hrsg.), BeckOK Datenschutzrecht, Stand 1.11.2021, Art. 5 DSGVO Rn. 12.

70 Vgl. dazu BVerfGE 125, 260 (Rn. 317) mit den zitierten Formulierungen.

71 Vgl. nur EuGH, Urteil vom 8.4.2014 – C-293/12 und C-594/12, EU:C:2014:238.

72 A. A. und großzügiger offenbar *H. A. Wolff*, in: P. Schantz/H. A. Wolff (Hrsg.), Das neue Datenschutzrecht, 2017, Rn. 404.

73 Vgl. zu diesem Maßstab in Bezug auf die Bestimmtheit der Zweckfestlegung etwa *T. Herbst*, in: J. Kühling/B. Buchner (Hrsg.), DS-GVO BDSG, 3. Aufl. 2020, Art. 5 Rn. 35.

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

arbeitung haben z.B. die Leistungserbringer dafür zu sorgen, dass die betroffenen Personen über die ausdrückliche Festlegung informiert werden. Dies kann beispielsweise im Rahmen der Informationen nach Art. 13 f. DSGVO erfolgen.

Vor allem im Kontext der Gestaltungsoption der Befüllung der ePA **„ex tunc"** gilt es mit Blick auf die Gebote der Zweckfestlegung und -bindung zu erörtern, ob eine nachträgliche Einschreibung der Informationen in die ePA möglicherweise eine **Zweckänderung** darstellt. Während der ursprüngliche **Erhebungszweck** der (Gesundheits-)Daten insbesondere im konkreten Behandlungszweck bestand, das heißt: dem konkreten Anlassfall diente (z.B. der Durchführung der konkreten Therapie oder etwaigen Dokumentationspflichten der Behandlung), besteht der geänderte Zweck (Sekundärzweck) vor allem darin, eine weitgehend vollständige gesundheitsinformationelle Basis in der ePA der Patienten zu etablieren. Dadurch sollen Verbesserungen hinsichtlich der Qualität und Effizienz in der fach- und sektorenübergreifenden Gesundheitsversorgung erlangt werden. Die Verarbeitung mit Blick auf die Gestaltungsoption der Befüllung „ex tunc" dient daher nicht mehr nur unmittelbar einem konkreten Anlassfall (z.B. einer Behandlung), sondern zielt auf eine spätere, qualitativ hochwertige und kosteneffiziente Versorgung ab, die durch den Rückgriff auf nahezu lückenlos dokumentierte (Gesundheits-)Datensätze gewährleistet werden kann. Insbesondere in jenen Krankheitsfällen, die in der Regel eine langjährige Vorgeschichte aufweisen (z.B. Schilddrüsenerkrankungen oder Diabetes), kann sich eine weitgehend vollständige gesundheitsinformationelle Basis als essenziell erweisen. Auch wenn daher abstrakt gesehen der sachliche Verarbeitungszweck (die Gesundheitsversorgung) der gleiche bleibt, stellen diese Vorgänge **Zweckänderungen** dar „und nicht etwa Verarbeitungen, die noch in einem breiter verstandenen Rahmen des ursprünglichen Zwecks eingeordnet würden".

Bei der Verarbeitung von Gesundheitsdaten sind Zweckänderungen allerdings nur zulässig, wenn die in Art. 6 Abs. 4 DSGVO verankerten **Voraussetzungen** erfüllt sind. Die Zulässigkeit ist daher gegeben, wenn entweder eine (ausdrückliche) Einwilligung der betroffenen Person (vgl. Art. 9 Abs. 2 lit. a) DSGVO) erfolgt oder auf der Grundlage eines Grundes gemäß Art. 9 Abs. 2 DSGVO, mit einer zusätzlich durchgeführten Verträglichkeitsprüfung im Sinne des Art. 6 Abs. 4 DSGVO. Da im Zuge der Einführung der ePA als Opt-out-Modell mit Blick auf eine Befüllung „ex tunc" prinzipiell keine (ausdrückliche) Einwilligung der betroffenen Personen gefordert wird, muss im Folgenden zusätzlich zur gesetzlichen Verarbeitungsgrundlage des Art. 9 Abs. 2 DSGVO eine **Verträglichkeitsprüfung** gemäß Art. 6 Abs. 4 DSGVO durchgeführt werden. Soweit dabei eine „Zweckvereinbarkeit" besteht, ist die Zweckänderung ausnahmsweise mit dem „Grundsatz der Zweckbindung" vereinbar.[75]

Gerade diese geforderte „Zweckvereinbarkeit" dürfte mit Blick auf die Gestaltungsoption der Befüllung der ePA „ex tunc" gegeben sein, da der neue Zweck (Etablierung einer nahezu lückenlos dokumentierten ePA, um eine qualitativ hochwertige und kosteneffiziente fach- und sektorenübergreifenden Gesundheitsversorgung zu gewährleisten) nach Maßgabe der Kriterien in Art. 6 Abs. 4 DSGVO mit dem ursprünglichen Erhebungszweck vereinbar ist. Zum einen geht es nach wie vor um Zwecke der Gesundheitsversorgung, wenn auch mit geringfügig abweichendem Zweckgegenstand. Der Erhebungszweck und der neue Zweck weisen damit nicht nur eine enge inhaltliche Verbindung (Art. 6 Abs. 4 lit. a)) DSGVO) auf, sondern scheinen auch mit Blick auf die anderen Gehalte des Abs. 4

75 Siehe *M. Albers/R. Veit*, in: H. A. Wolff/S. Brink (Hrsg.), BeckOK Datenschutzrecht, Stand 1.11.2021, Art. 6 DSGVO Rn. 98.

vereinbar zu sein. Die inhaltliche Verbindung (lit. a)) zeichnet sich insbesondere im Ziel einer qualitativ hochwertigen und effizienten Gesundheitsversorgung aus, aber nun losgelöst von einem konkreten Anlassfall. Dabei kann der hinzutretende Zweck (Etablierung einer nahezu lückenlosen ePA) im Übrigen sehr wohl im Kontext des Erhebungszwecks (optimale Versorgung des Anlassfalls) stehen, wenn etwa Krankheiten erst im Nachhinein zum Vorschein kommen.

Zum anderen handelt es sich zwar zweifellos um sensible Daten, für die eine besonders strenge Zweckbindung besteht (vgl. Art. 6 Abs. 4 lit. c) DSGVO). Unseres Erachtens können allerdings „geeignete Garantien" im Sinne des Art. 6 Abs. 4 lit. e) DSGVO insoweit Abhilfe schaffen und auch Zweckänderungen bei der Weiterverarbeitung sensibler Daten legitimieren. Dazu dürften insbesondere auch besonders deutliche Hinweise auf die Befüllung der ePA „ex tunc" zählen.

Hinzu tritt der Umstand, dass die beabsichtigte Weiterverarbeitung der (Gesundheits-) Daten prinzipiell nicht zum Nachteil der Patientinnen und Patienten erfolgen soll. Vielmehr zielt sie, wie die Befüllung der ePA im Allgemeinen, auf eine qualitativ hochwertige fach-, einrichtungs- und sektorenübergreifende Gesundheitsversorgung ab.

Solange der allgemeine medizinische Zweck der Datenverarbeitung daher nicht aufgegeben wird, dürfte die Kompatibilitätsprüfung sowohl für individualdiagnostische als auch für kollektive Analyse- und Auswertungszwecke prinzipiell positiv ausfallen – zumindest dann, wenn das große Interesse des Einzelnen an der Leistungsfähigkeit seiner eigenen ePA berücksichtigt wird. Da der „Grundsatz der Zweckbindung" in Art. 5 Abs. 1 lit. b) DSGVO somit keine „strikte" Bindung an den ursprünglich festgelegten Zweck fordert, ist die Gestaltungsoption der ePA-Befüllung „ex tunc" unseres Erachtens mit diesem vereinbar.[76]

3.2.2.3 Datenminimierung und Speicherbegrenzung

Im Lichte des Grundsatzes der Datenminimierung gemäß Art. 5 Abs. 1 lit. c) DSGVO hat die Befüllung der ePA außerdem prinzipiell drei Anforderungen zu genügen. Zur Erreichung der bereits erörterten Verarbeitungszwecke, insbesondere der Verbesserung der Qualität und Effizienz der Gesundheitsversorgung, muss die angedachte Befüllung in den beschriebenen Ausgestaltungsoptionen jeweils geeignet, erforderlich und angemessen sein. Das Kriterium der **Erheblichkeit** ist bei der Anlage und Befüllung der ePA unstreitig erfüllt. Jedes Mehr an gesundheitsinformationeller Basis über den Patienten kann potenziell die Entscheidungsgrundlage für die Versorgung verbessern und folglich die Sicherheit diagnostischer und therapeutischer Maßnahmen steigern.

3.2.2.3.1 Erforderlichkeit

Bei der Prüfung des Kriteriums der **Erforderlichkeit** ist zu beachten, dass die Verarbeitung der personenbezogenen Daten „auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein" muss. Es geht dabei insbesondere um die Frage, ob das Ziel (also vor allem die Verbesserungen der Qualität und Effizienz in der Gesundheitsversorgung) ebenso

76 Vgl. *T. Herbst*, in: J. Kühling/B. Buchner (Hrsg.), DS-GVO BDSG, 3. Aufl. 2020, Art. 5 Rn. 43 ff.

mit einem **weniger intensiven** Eingriff in die Rechte der Patientinnen und Patienten erreicht werden kann, und ob dieser geringere Eingriff dabei **gleich effektiv** ist. Insofern besteht eine klare Ausrichtung am Zweck der Datenverarbeitung. Mithin umfasst der „Grundsatz der Datenminimierung" keine absolute normative Begrenzung des Umfangs der Datenverarbeitung,[77] d.h. bei der Anlage und Befüllung der ePA wird prinzipiell keine strikte normative Begrenzung des Datenverarbeitungsumfangs gefordert, sondern vielmehr eine relationale Ausrichtung am Zweck (wie insbesondere der Verbesserungen der Qualität und Effizienz in der Gesundheitsversorgung).

Da vor allem im Gesundheitsbereich im Zeitpunkt der Erhebung der Daten zumeist noch nicht deren konkreter Bedarf vorhersehbar ist, darf die Verarbeitung nicht per se als nicht erforderlich bewertet werden. Vielmehr muss man sich im Zeitpunkt der Verarbeitung der (Gesundheits-)Daten die Frage stellen, ob dieser konkrete Verarbeitungsvorgang für den Zweck der Etablierung einer nahezu vollständigen gesundheitsinformationellen Basis in der ePA erforderlich ist, um Verbesserungen hinsichtlich der Qualität und Effizienz in der fach- und sektorenübergreifenden Gesundheitsversorgung zu erlangen.

Vor allem mit Blick auf die Gestaltungsoption einer **gesetzlich verpflichtenden Befüllung „ex tunc"** – im Gegensatz zu einer auf Freiwilligkeit beruhenden Befüllung „ex tunc" oder gar einer Befüllung ausschließlich „ex nunc" – stellt sich die Frage, ob die Einspeisung von „älteren" (Gesundheits-)Daten noch „auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt" ist. Unseres Erachtens ist, um das Ziel einer nahezu lückenlosen gesundheitsinformationellen Basis in der ePA erreichen zu können, kein geringerer, dabei aber gleich effektiver Eingriff in die Rechte der Patienten denkbar. Freilich würde die auf Freiwilligkeit beruhende Befüllung „ex tunc" einen geringeren Eingriff in die Patientenrechte darstellen, aber gleichzeitig zum Problem einer möglicherweise lückenhaften gesundheitsinformationellen Basis in der ePA führen, wenn sich beispielsweise der Leistungserbringer gegen die rückwirkende Befüllung ausspricht. Mithin besteht – sofern sich der Gesetzgeber prinzipiell dazu entschließt, eine Befüllung „ex tunc" anzuordnen – kein geringerer Eingriff in die Rechte der Patienten, der gleich effektiv wäre. Dabei wäre gewiss zu beachten, dass die rückwirkende Einspeisung der (Gesundheits-)Daten in die ePA von dem entsprechenden Fachpersonal durchgeführt werden sollte, um sichergehen zu können, dass nur jene Daten eingespeist werden, die für die Zwecke der ePA auch tatsächlich erforderlich sind (also z.B. keine überholten und korrigierten Diagnosen). Vor diesem Hintergrund wäre mit Blick auf die Erforderlichkeit auch eine gesetzlich verpflichtende Befüllung „ex tunc" datenschutzrechtlich darstellbar.

3.2.2.3.2 Angemessenheit

Im Rahmen der **Angemessenheit** der Datenverarbeitung ist schließlich zu erörtern, ob die zu verarbeitenden personenbezogenen Daten dem Zweck nach angemessen sind. Es geht dabei insbesondere um die auch grundrechtlich relevante Frage, ob sich die Intensität der mit der Verarbeitung verbundenen Beeinträchtigungen bzw. Risiken in Relation zu dem angestrebten Verarbeitungszweck als verhältnismäßig erweist.

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

Aus dem Gebot der Beschränkung von Datenverarbeitungen auf ein angemessenes Maß könnten sich Vorgaben vor allem für die Frage ergeben, ob ein Opt-out bei der Befüllung der ePA einer **„All-in-Lösung"** folgen darf oder auf eine **differenzierte Befüllung** setzen sollte. Für eine differenzierte Befüllung könnte einerseits sprechen, dass bestimmte besonders sensible Informationen (z.B. zu psychischen Erkrankungen oder HIV-Infektionen) die Persönlichkeitsrechte des Patienten derart intensiv berühren, dass eine Speicherung dieser Informationen (und eine Abrufbarkeit für zugriffsberechtigte Dritte) nur unter qualifizierten Voraussetzungen zulässig sein könnte – etwa dann, wenn der Patient von seinem Arzt nochmals explizit auf eine Widerspruchsmöglichkeit hingewiesen wurde, oder wenn die Speicherung ausnahmsweise nur nach einem entsprechenden Opt-in erfolgen darf. Andererseits streitet für eine voraussetzungslose „All-in-Befüllung" die Überlegung, dass nur so eine von Beginn an weitgehend vollständige gesundheitsinformationelle Basis etabliert werden kann. Berücksichtigt man indes, dass die in Frage stehenden besonders sensiblen Informationen einen sehr geringen Anteil an den ePA-Daten ausmachen dürften, scheint es für eine möglichst breite Informationsbasis kaum abträglich zu sein, wenn einzelne hochsensible Gesundheitsdatenfelder nur unter besonderen Voraussetzungen in die ePA eingespielt werden. Umgekehrt steigert die besondere Rücksichtnahme in Bezug auf die hochsensiblen Daten den Schutz der Persönlichkeitsrechte betroffener Patienten punktuell ganz erheblich. Bei der Abwägung der gegenläufigen Belange dürfte einem **differenzierten Befüllungskonzept** als **deutlich schonendere Gestaltungsoption** der Vorzug zu geben sein.

Des Weiteren muss, ungeachtet der gewählten Gestaltungsoptionen, im Einzelfall beurteilt werden, welche gesundheitsbezogenen Daten potenziell für die zukünftige Gesundheitsversorgung des Patienten vonnöten sind. Eine fachlich treffende Einordnung bezüglich der Erforderlichkeit der Speicherung von Gesundheitsinformationen in der ePA werden insbesondere Angehörige des **Fachpersonals** treffen können. Aus diesem Grunde und mit Blick auf die unter dem Recht auf informationelle Selbstbestimmung geltenden Verfahrensanforderungen sollte in jedem Falle als **prozedurales Erfordernis** eine Übermittlung von Gesundheitsdaten ausschließlich durch Angehörige des Fachpersonals erfolgen. Dies genügt nicht nur den Ansprüchen des Grundsatzes der Datenminimierung, sondern auch jenen der „angemessenen und spezifischen Maßnahmen" im Sinne des Art. 9 Abs. 2 lit. i) DSGVO sowie den geeigneten „Bedingungen und Garantien" entsprechend Art. 9 Abs 2 lit. h) i.V.m Abs. 3 DSGVO. Dies ist deshalb erwägenswert, da für die Verarbeitung der (Gesundheits-)Daten nicht nur das „Ob", sondern ebenso das „Wie" der Verarbeitung für die Rechtfertigung relevant ist.

3.2.2.3.3 Speicherbegrenzung

Schließlich ist in diesem Kontext auch der **Grundsatz der Speicherbegrenzung** zu berücksichtigen, d.h. der Datensparsamkeit in zeitlicher Hinsicht. Die Speicherdauer der Daten soll demnach und aus ErwGr 39 DSGVO ersichtlich „auf das unbedingt erforderliche Mindestmaß beschränkt" werden. Da es allerdings bereits im Wesen der Gesundheitsversorgung liegt, dass nicht vorhersehbar ist, wann eine bestimmte gesundheitliche Vorgeschichte des Patienten relevant werden kann, dürfen unseres Erachtens nicht allzu strenge Maßgaben an diesen Grundsatz gestellt werden. Ein Blick nach Österreich zeigt beispielsweise, dass die ELGA-Gesundheitsdaten gemäß § 18 Abs. 9 GTelG 2012 zehn Jahre nach Kenntnis des Sterbedatums (!) automatisch zu löschen sind. Wenngleich das Recht

auf Datenschutz nach der DSGVO[78] der betroffenen Personen mit deren Tod prinzipiell endet, können sich die in der ePA gespeicherten Datensätze gewiss auch über den Tod hinaus als relevant erweisen, um z.B. etwaige übertragbare Krankheiten im Nachhinein feststellen zu können.

Bedenkenswert erscheint in diesem Kontext, dass – obzwar die DSGVO kein postmortales Datenschutzrecht kennt –, in Deutschland dem „Schutz der Menschenwürde" in Art. 1 GG ein postmortales Persönlichkeitsrecht entnommen werden kann.[79] Da – wie bereits erwähnt – erst aus der Zusammenschau der Datenschutzgrundsätze in der DSGVO in Verbindung mit den (vorliegend auch nationalen) Grundrechten ausgemacht werden kann, was „angemessene und spezifische Maßnahmen" bzw. „Bedingungen und Garantien" sind, ist der „Schutz der Menschenwürde" in Art. 1 GG mitzuberücksichtigen.[80] Dass indes die Menschenwürde durch Erhalten der (Gesundheits-)Daten in der ePA über das Sterbedatum hinaus verletzt werden könnte, erschließt sich uns nicht. Dies zeigt insbesondere der Vergleich mit der analogen Welt: Auch die Aufbewahrungspflicht von ärztlichen Aufzeichnungen ist für mindestens „zehn Jahre […] nach Abschluss der Behandlung" zu Dokumentationszwecken in § 10 Abs. 3 MBO-Ä 1997 zulässig, und die klassische Akte der Ärzte in Papierform soll ohnehin unverändert weiterbestehen. Anzudenken wäre für die Zeit nach dem Tod des Patienten allenfalls ein Erhalt in anonymisierter Form, sofern dies im Einzelfall zweckmäßig erscheint.

Im Ergebnis dürfen (Gesundheits-)Daten bis zur Kenntnis des Sterbedatums in der ePA gespeichert werden. Allerdings sollte bei etwaigen Speicherungen über den Tod hinaus im Einzelfall beurteilt werden, ob für den verfolgten Zweck nicht auch die Verarbeitung von anonymisierten Daten ausreichend wäre.[81]

3.2.2.3.4 Zwischenergebnis

Im Zwischenergebnis lassen sich aus den Grundsätzen der Datenminimierung und Speicherbegrenzung gewisse Vorzüge von zwei Gestaltungsoptionen für die ePA in Bezug auf die Nutzung zu Versorgungszwecken ableiten. Zum einen bestehen mit Blick auf die Ausführungen zur Erforderlichkeit gewisse Effektivitätsvorteile einer – unseres Erachtens zulässigen – Befüllung der ePA „ex tunc" gegenüber der Befüllung „ex nunc", da lediglich

78 In Erwägungsgrund 27 der DSGVO ist festgeschrieben, dass „diese Verordnung […] nicht für die personenbezogenen Daten Verstorbener [gilt]. Die Mitgliedstaaten können Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener vorsehen." Letzterer Satz stellt eine Öffnungsklausel für die Mitgliedstaaten dar und verhindert mithin, dass dem Missbrauch von Daten „Tür und Tor" eröffnet wird. Deutschland hat von diesem Recht mit Blick auf das BDSG keinen Gebrauch gemacht. Siehe allerdings § 7 Abs. 1 HmbKHG, nach dem „der Datenschutz […] nicht mit dem Tode der Patientin oder des Patienten" endet.

79 Nach anderer Ansicht endet der „Schutz der Menschenwürde" als Grundrecht mit dem Absterben des Menschen als lebender Organismus, mithin sind nicht die Toten grundrechtsberechtigt, sondern die Überlebenden. Gegenüber Letzteren soll gemäß Art. 1 Abs. 1 GG eine nachwirkende Schutzpflicht zukommen. Vgl. *H. D. Jarass*, in H. D. Jarass/B. Pieroth (Hrsg.), GG, 16. Aufl. 2020, Art. 1 Rn. 10. Ferner wird die Ansicht vertreten, dass ein postmortales Persönlichkeitsrecht nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG besteht. Dieses lehnt das BVerfG allerdings ab, da nur der lebende Mensch der Grundrechtsträger nach Art. 2 Abs. 1 GG sein kann. Siehe BVerfGE 30, 173 (194).

80 Nicht treffend ist daher, dass der Landesbeauftragte für Datenschutz und Informationsfreiheit von Mecklenburg-Vorpommern eine Rechtsgrundlage für die Zulässigkeit der Datenverarbeitung in der DSGVO an sich fordert. Siehe Näheres in *Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern*, Fünfzehnter Tätigkeitsbericht zum Datenschutz und Siebenter Bericht über die Umsetzung des Informationsfreiheitsgesetzes, 2018/19, S. 89.

81 Siehe genauer und m.w.N. *P. Schantz*, in: H. A. Wolff/S. Brink (Hrsg.), BeckOK Datenschutzrecht, Stand 1.11.2021, Art. 5 DSGVO Rn. 32 ff.

durch eine rückwirkende Befüllung eine nahezu vollständige gesundheitsinformationelle Basis in der ePA etabliert werden kann. Zum anderen sollte hinsichtlich des Gebots der Beschränkung von Datenverarbeitungen auf ein angemessenes Maß ein **differenziertes Befüllungskonzept** favorisiert werden, da sich nach Abwägung der Gehalte zeigte, dass dieses im Gegensatz zur „All-in-Lösung“ deutlich schonender ist.

3.2.2.4 Richtigkeit

Nach dem **Datenschutzgrundsatz der Richtigkeit** gemäß Art. 5 Abs. 1 lit. d) DSGVO müssen die in der ePA eingespeicherten Gesundheitsdaten prinzipiell richtig sein. Eine wichtige Rolle spielt dabei sowohl die **sachliche Richtigkeit** der verarbeiteten Daten als auch die „erforderlichenfalls“ durchzuführende **Aktualisierung**, um die Richtigkeit der verarbeiteten Gesundheitsdaten zum jeweils aktuellen Zeitpunkt gewährleisten zu können. Vor allem im Gesundheitsbereich können unrichtige bzw. unvollständige Gesundheitsdaten in der ePA zu Fehlschlüssen bei der Diagnostik und/oder Behandlung führen. Dies würde insbesondere dem Ziel der Verbesserungen der Qualität und Effizienz in der Gesundheitsversorgung zuwiderlaufen.

Um die Richtigkeit der verarbeiteten Daten im Kontext der ePA gewährleisten zu können, ist ungeachtet der gewählten Gestaltungsoption in **prozeduraler** Hinsicht darauf zu achten, dass die Befüllung durch entsprechendes **Fachpersonal** bzw. durch Personen erfolgt, die unter der Verantwortung von Fachpersonal stehen. Allgemein ist davon auszugehen, dass mit Blick auf die Erhebung der Daten ein strengerer Maßstab bei der Kontrolle gilt als bei der Überprüfung der Richtigkeit von Bestandsdaten.[82] Dies spricht unseres Erachtens dafür, dass eine ePA-Befüllung **„ex tunc“** jedenfalls unter dem Gesichtspunkt der Richtigkeit der Datenverarbeitung einer Befüllung „ex nunc“ gegenüber keineswegs das Nachsehen haben muss. Entscheidend dürfte sein, dass das Fachpersonal sicherstellt, dass die Überführung der Bestandsdaten in die ePA gerade mit Blick auf die Semantik und die Formatierung der Daten nicht zu Qualitätsverlusten führt. Dies würde im Falle einer obligatorischen Befüllung „ex tunc“ freilich eine Belastung der Leistungserbringer nach sich ziehen, die der Gesetzgeber mit Rücksicht auf deren Berufsgrundrechte im Blick behalten müsste, gegebenenfalls unter Rückgriff auf Entlastungs- und Anreizinstrumente.

Zu bedenken ist zudem, dass bei besonders sensiblen (Gesundheits-)Daten (z.B. Diagnose einer psychischen Erkrankung oder HIV-Infektion) ein erhöhter Maßstab an die sachliche Richtigkeit der Daten zu setzen ist, da sich etwaige Unrichtigkeiten fatal auf die entsprechende Gesundheitsversorgung der Patienten auswirken könnten. Mit Blick auf die Gestaltungsoptionen der „All-in-Lösung“ einerseits sowie der differenzierten Befüllung andererseits liegt es nahe, dass im Falle einer **differenzierten Befüllung**, ungeachtet ihrer Suboptionen, den besonders sensiblen (Gesundheits-)Daten tendenziell mehr Aufmerksamkeit geschenkt werden dürfte als bei der unterschiedslosen Befüllung. Um der sachlichen Richtigkeit der zu verarbeitenden besonders sensiblen (Gesundheits-)Daten im Kontext der ePA in besonderem Maße Rechnung zu tragen, könnte der Gesetzgeber daher auf eine differenzierte Befüllung setzen.

82 *P. Schantz*, in: H. A. Wolff/S. Brink (Hrsg.), BeckOK Datenschutzrecht, Stand 1.11.2021, Art. 5 DSGVO Rn. 29.

3.2.2.5 Integrität und Vertraulichkeit

Besondere Bedeutung bei der Anlage und Befüllung der ePA gewinnt schließlich der in Art. 5 Abs. 1 lit. f) DSGVO verankerte **Grundsatz der Integrität und Vertraulichkeit**. Dieser fordert die Gewährleistung der angemessenen Sicherheit der personenbezogenen Daten sowie den Schutz vor „unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen". Es werden somit die Ziele der Integrität und Vertraulichkeit angesprochen, denen insbesondere die Gewährleistung der Datensicherheit im Sinne des Art. 32 DSGVO dient.[83] Dieser Schutz soll insoweit nicht nur bei gezielten Eingriffen, sondern ebenso beim unbeabsichtigten Verändern der Daten bestehen. Die vorzunehmenden Maßnahmen hängen dabei von der Art der Datenverarbeitung, der Wichtigkeit der Daten für die Rechte und Interessen der Patientinnen und Patienten sowie vom Risiko des unberechtigten Zugriffs ab.[84]

Um diese Vorgaben gewährleisten zu können, müssen insbesondere adäquate Instrumente zur **Identifikation** und **Authentifizierung**[85] der eingebundenen Akteure etabliert werden. Insofern müssen, zum einen, die Patienten absolut zweifelsfrei identifiziert werden,[86] und zum anderen muss garantiert werden können, dass nur jene Gesundheitsdiensteanbieter zur Befüllung zugriffsberechtigt sind, die an der Behandlung des Versicherten auch wirklich teilhaben.[87] Zudem muss eine **Protokollierung** darüber stattfinden, welche Gesundheitsdaten wann, zu welcher Gelegenheit und durch wen in die ePA eingeschrieben werden.[88]

Mit Blick auf die oben angesprochene Gestaltungsoption, wonach die ePA automatisch entweder mit oder ohne Registrierungserfordernis angelegt und befüllt werden könnte, bedarf insbesondere das Erfordernis der Registrierung einer näheren Erörterung. Insofern stellt sich aus datenschutzrechtlicher Perspektive die Frage, ob die Anlage und anschließende automatische Befüllung **ohne** Erfordernis eines **Registrierungsprozesses** für die betroffenen Patienten den datenschutzrechtlichen Vorgaben, im Speziellen den geforderten „angemessenen und spezifischen Maßnahmen" des Art. 9 Abs. 2 DSGVO und Art. 5 Abs. 1 lit. f) DSGVO, genügt und dergestalt eingeführt werden dürfte. Im Wesentlichen geht es darum, dass lediglich die zugriffsberechtigten Personen, d.h. im Kontext der ersten Gestaltungsoption insbesondere die betroffenen Patienten, Zugriff auf ihre ePA haben dürfen – und keine Unbefugten. Es soll unter anderem ein ausreichender Schutz vor „unbefugter oder unrechtmäßiger Verarbeitung" der personenbezogenen Daten sichergestellt werden.

Dabei ist es unseres Erachtens aus datenschutzrechtlicher Perspektive jedoch nicht zwingend notwendig, dass die ePA erst nach aktiver Registrierung bzw. Authentifizierung

83 Vgl. *J. Eichenhofer*, NVwZ 2021, 1090 (1093) und siehe ausführlicher unter Punkt »3.2.2.5.

84 Vgl. *P. Schantz*, in: H. A. Wolff/S. Brink (Hrsg.), BeckOK Datenschutzrecht, Stand 1.11.2021, Art. 5 DSGVO Rn. 35 f.

85 Siehe die begriffliche Unterscheiddung bereits oben unter Punkt »3.1.1.

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

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

88 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).

durch den Patienten nutzbar und für zugangsberechtigte Leistungserbringer beschreibbar und einsehbar ist, und zwar mit Blick auf Missbrauchsrisiken sowohl seitens der Leistungserbringer als auch seitens des Patienten selbst. Der Schutz vor „unbefugter oder unrechtmäßiger Verarbeitung“ auf Seiten der **Leistungserbringer** wird ohne Weiteres auch dann gewahrt, wenn lediglich die registrierten und authentifizierten zugriffsberechtigten Leistungserbringer die ePA einsehen bzw. befüllen können, losgelöst von einer zuvor erfolgten bzw. nicht erfolgten Registrierung der Patienten. Denn auch dann, wenn der Patient (noch) keine gesonderte Registrierung vorgenommen hat, kann seine Patientenakte nur von den registrierten und authentifizierten Leistungserbringern unter den entsprechenden Schutzvorkehrungen benutzt werden. Als Zugangsschlüssel auf Seiten des **Patienten** selbst kann bei einem Leistungserbringer vor Ort (z.B. in der Apotheke) die elektronische Gesundheitskarte in Kombination mit einem Lichtbildausweis vorgelegt werden. Die betroffenen Patienten würden aufgrund der Informationspflichten der Verantwortlichen, also der Krankenkassen, überdies ausreichend über die Möglichkeit zur Registrierung informiert und hätten jedenfalls das entsprechende Recht, sich mittels Registrierung Zugriff auf ihre Akte zu verschaffen.

Vor diesem Hintergrund müssten jedenfalls **robuste technische Maßgaben** für eine eindeutige Überprüfung der **Identität der Patienten** selbst sowie der **zugangsberechtigten Personen** (z.B. Ärzten) vorgesehen werden, wenn sie in die ePA Einsicht nehmen bzw. Informationen eingeben möchten. Darüber hinaus muss ein belastbares **Protokollierungssystem** etabliert werden, das die Nachvollziehbarkeit und Überprüfbarkeit der gespeicherten personenbezogenen Daten in der ePA gewährleistet.

3.2.3 Ergänzende grundrechtliche Vorgaben und Impulse

Da die Grundrechte des Grundgesetzes und der Grundrechtecharta bereits in die Interpretation der die Verarbeitungen in der ePA beschränkenden datenschutzrechtlichen Vorgaben der DSGVO hineinwirken, bleiben in Ergänzung jener Vorgaben an dieser Stelle vor allem diejenigen Grundrechtswirkungen zu betonen, die keine beschränkenden, sondern **ermöglichende Effekte** auf die Gestaltung der ePA haben. Von den drei wesentlichen Gestaltungsentscheidungen, die der Gesetzgeber zu treffen hat, betrifft dies vor allem den Verzicht auf ein gesondertes Registrierungserfordernis sowie die Befüllung der ePA „ex tunc“ auch mit bereits bestehenden Daten.

Der **Verzicht** auf ein gesondertes **Registrierungserfordernis** des Patienten ist mit den beschränkenden datenschutzrechtlichen Vorgaben – wie gezeigt – prinzipiell vereinbar, trotz der damit verbundenen potenziellen Einschränkungen zumal bezüglich der Transparenz der Verarbeitungen. Umgekehrt muss allerdings betont werden, wie wichtig die sofortige automatische Befüllung der ePA auch ohne vorherige Registrierung des Patienten für alle künftig zu treffenden gesundheitsbezogenen Entscheidungen des Patienten sein kann – denn ohne hinreichende Informationsgrundlage kann eine selbstbestimmte Entscheidung über das Schicksal des eigenen Körpers im Krankheitsfall nicht gewährleistet werden. Sofern man dem Recht auf informationelle Selbstbestimmung nicht nur ein Recht *gegen*, sondern auch ein Recht *auf* Datenverarbeitung entnimmt, und dieses Recht in Beziehung zum Selbstbestimmungsrecht des Einzelnen bezüglich seiner körperlichen Unversehrtheit setzt, ergibt sich aus diesen grundrechtlichen Gehalten unseres Erachtens ein verfassungsrechtlicher Impuls zum Verzicht auf ein Registrierungserfordernis.

Ähnliches dürfte für die Wahl zwischen einer Befüllung „ex nunc“ oder „ex tunc“ gelten. Berücksichtigt man den potenziellen Mehrwert, der mit einer **umfassenden Befüllung der ePA „ex tunc“** für das künftige Selbstbestimmungsrecht des Einzelnen einhergeht, sollte der Gesetzgeber im Zweifelsfall mit Rücksicht auf die Patientenrechte einer solchen Befüllung „ex tunc“ den Vorzug geben – möglicherweise gar in Gestalt einer **obligatorischen** nachträglichen Befüllung. Der Patient wird dadurch auch eher in die Lage versetzt, die Leistungserbringer frei zu wählen und so einem gesundheitsdatenbedingten „Lock-in“ zu entgehen. Ein solcher „Lock-in“ droht vor allem dann, wenn ein Patient bei einem Leistungserbringer über einen längeren Zeitraum hinweg große Datenmengen generiert und hinterlegt hat. Ein Wechsel des Leistungserbringers könnte für den Patienten dann mit einem erheblichen Verlust an Daten einhergehen – mit der Konsequenz, dass die Wechselkosten den Patienten möglicherweise von einem Wechsel abhalten und ihn gleichsam unfreiwillig an den betreffenden Leistungserbringer binden. Bei Einführung einer obligatorischen Befüllung „ex tunc“ würde ein möglicher gesundheitsdatenbedingter „Lock-in“ bei einem bestimmten Leistungserbringer, der bereits über besonders umfangreiche Gesundheitsdatenbestände des Patienten verfügt, dagegen aufgehoben. Dabei sind vom Gesetzgeber freilich, wie bereits ausgeführt, die zusätzlichen Belastungen zu berücksichtigen, die mit einer solchen obligatorischen „ex tunc“-Befüllung für die Leistungserbringer einhergehen. Der Gesetzgeber müsste mit Rücksicht auf deren Grundrechte gegebenenfalls Entlastungsmöglichkeiten und Anreize schaffen.

3.2.4 Sonstige Vorgaben

3.2.4.1 Informationspflichten (Art. 12 ff. DSGVO)

Über die aus den Datenschutzgrundsätzen selbst sowie den Grundrechten folgenden Vorgaben hinaus lassen sich der Datenschutzgrundverordnung eine Reihe weiterer, spezieller Anforderungen entnehmen, die letztlich die Datenschutzgrundsätze konkretisieren und weiter ausdifferenzieren. So treffen den Verantwortlichen gemäß Art. 12 ff. DSGVO **spezifische Informationspflichten**, um die betroffenen Personen in ausreichend verständlicher und präziser Weise über die Verarbeitung ihrer personenbezogenen (Gesundheits-)Daten sowie ihre diesbezüglichen Rechte in Kenntnis zu setzen. Insofern dienen jene Informationspflichten direkt dem Selbstbestimmungsrecht.[89] Wie schon im Kontext des Transparenzgrundsatzes festgestellt wurde, sind die Informationspflichten insbesondere im Zusammenhang mit dem **Registrierungserfordernis**, aber auch mit Blick auf die **Befüllung „ex tunc“** von besonderer Relevanz.

3.2.4.2 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Neben den Informationspflichten erscheinen **datenschutzfreundliche Voreinstellungen** gemäß Art. 25 Abs. 2 DSGVO von nicht unerheblicher Bedeutung im Kontext der Anlage und Befüllung der ePA. Generell steht Art. 25 DSGVO weder mit Blick auf das Gebot eines datenschutzfreundlichen Designs noch mit Blick auf datenschutzfreundliche Voreinstellungen einem Opt-out-Modell entgegen, da sich aus diesem Gebot insbesondere

89 *S. Quaas*, in: H. A. Wolff/S. Brink (Hrsg.), BeckOK Datenschutzrecht, Stand: 1.5.2022, Art. 12 DSGVO Rn. 4 f.

kein Vorrang der Einwilligung vor gesetzlichen Verarbeitungstatbeständen ableiten lässt.[90] Unter dem Gesichtspunkt der datenschutzfreundlichen Voreinstellungen bedarf es aufgrund der im Gegensatz zur „All-in-Lösung" deutlich schonenderen Gestaltungsoption insbesondere einer Akzentuierung der Vorzüge des **differenzierten Befüllungskonzepts**. Dieses nimmt anders als die „All-in-Lösung" Rücksicht auf die Sensibilität der verarbeiteten Daten und lässt die Speicherung von besonders sensiblen (Gesundheits-)Daten insoweit nur unter qualifizierten Voraussetzungen zu. Da die Vorzüge der differenzierten Befüllung bereits oben unter dem Gesichtspunkt der Datenminimierung und Speicherbegrenzung erläutert wurden, wird auf obige Stelle verwiesen.

3.2.4.3 Widerspruchsrecht (Art. 21 DSGVO)

Ferner kommt den Patientinnen und Patienten im Rahmen des Art. 21 DSGVO ein jederzeitiges **Widerspruchsrecht** in Bezug auf die Verarbeitung von sie betreffenden personenbezogenen (Gesundheits-)Daten zu. Auch dieses Recht ist Ausfluss des Rechts auf informationelle Selbstbestimmung; seine Ausübung muss niederschwellig und unbürokratisch möglich sein. Im Kontext von ePA-Systemen, die auf einer automatischen Einrichtung und Befüllung auf gesetzlicher Grundlage basieren, wird man sämtliche Opt-out-Möglichkeiten letztlich als Ausgestaltungen des Widerspruchsrechts begreifen müssen. Als in Art. 21 DSGVO niedergelegtes unbedingtes Recht ist ein Widerspruch nur bei bestimmten Verarbeitungen zwingend vorgesehen, etwa bei der Direktwerbung (Abs. 2 und 3). Trotzdem wird man bei Opt-out-Systemen, die Gesundheitsinformationen auf der Basis eines gesetzlichen Verarbeitungstatbestands nach Art. 9 Abs. 2 lit. g), h) und/oder i) DSGVO verarbeiten, als zwingende „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person" jedenfalls eine im Grundsatz unbedingte Widerspruchsmöglichkeit einfordern müssen, die nur ausnahmsweise bei gegebenen zwingenden schutzwürdigen Gründen i.S.v. Art. 21 Abs. 1 DSGVO überwunden werden kann (z.B. in Notfällen).

Diese Vorgaben könnten sich auf den ersten Blick insbesondere bei einem **Verzicht** auf ein gesondertes **Registrierungserfordernis** als problematisch erweisen, da die ePA im Rahmen einer automatischen, einwilligungsunabhängigen Anlage und Befüllung ohne Registrierungserfordernis gleichsam „hinter dem Rücken des Patienten" beschrieben werden kann. Bei solchen Opt-out-Gestaltungen – so könnte man argumentieren – würde ein durchschnittlicher Patient möglicherweise nicht ohne Weiteres mit der Verarbeitung seiner (Gesundheits-)Daten rechnen und wegen Unkenntnis der konkreten Verarbeitung möglicherweise nicht von seinem Widerspruchsrecht Gebrauch machen. Daher haben die betroffenen Personen im Falle eines zwingenden Widerspruchsrechts nach Art. 21 DSGVO neben sorgfältigen Informationen im Vorfeld der Datenverarbeitung gemäß Art. 21 Abs. 4 DSGVO „spätestens zum Zeitpunkt der ersten Kommunikation […] ausdrücklich […] in einer verständlichen und von den anderen Informationen getrennten Form" auf ihr Widerspruchsrecht hingewiesen zu werden.

90 Vgl. erneut *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; *J. Kühling/B. Buchner*, 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. 10 f., 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.

Da indes auch im Falle eines Verzichts auf ein gesondertes Registrierungserfordernis die betroffenen Personen jederzeit über eine niedrigschwellige Möglichkeit verfügen müssen, eine Registrierung vorzunehmen, dürfte jedenfalls dann kein Verstoß gegen die datenschutzrechtlichen Vorgaben zum Widerspruchsrecht vorliegen, wenn die Patientinnen und Patienten ausreichend über die Registrierungsmöglichkeit informiert wurden, der tatsächliche Registrierungsaufwand keine übermäßigen Anstrengungen erfordert und mithin eine niedrigschwellige Einsichtsmöglichkeit in die Verarbeitung ihrer personenbezogenen (Gesundheits-)Daten besteht.

3.3 Zusammenfassung

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 die automatische, einwilligungsunabhängige Anlage und Befüllung an ein gesondertes **Registrierungserfordernis** für den Patienten knüpfen oder auf eine Registrierungspflicht verzichten. Er könnte 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 nur unter qualifizierten Voraussetzungen gespeichert werden könnten. Und schließlich müsste der Gesetzgeber 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.

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. Für ein Opt-out-Modell, das die Anlage und Befüllung der ePA ohne vorherige Einwilligung der Patientinnen und Patienten vorsieht, stehen dem Gesetzgeber grundsätzlich die Verarbeitungstatbestände des **Art. 9 Abs. 2 lit. h) i.V.m. Abs. 3 DSGVO** sowie des **Art. 9 Abs. 2 lit. i) DSGVO** zur Verfügung. Deren tatbestandlichen Voraussetzungen sind prinzipiell erfüllt, ein darüber hinausgehender Vorrang einer Einwilligungslösung besteht nicht.

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** ist vor allem für solche Opt-out-Gestaltungen relevant, mit denen der durchschnittliche Patient nicht ohne Weiteres rechnet – etwa die automatische, einwilligungsunabhängige Anlage und Befüllung ohne Registrierungserfordernis. Selbst der Verzicht auf ein gesondertes **Registrierungserfordernis** wäre 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 ePA-Befüllung **„ex tunc“** wäre mit dem Grundsatz der Transparenz vereinbar, da die Patientinnen und Patienten in zumutbarer Weise Kenntnis von der Befüllung ihrer ePA nehmen können.

Mit Blick auf den Grundsatz der **Zweckfestlegung und -bindung** ginge mit einer Befüllung **„ex tunc“** zwar eine gesondert rechtfertigungsbedürftige Zweckänderung einher; allerdings bestünde insoweit eine Zweckvereinbarkeit, weshalb die Zweckänderung in keinem Widerspruch zu jenem Datenschutzgrundsatz stehen dürfte. Des Weiteren ist festzuhalten, dass in den Opt-out-Gestaltungen für die ePA **keine unzulässige „Vorrats-gesundheitsdatenspeicherung“** 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 Erhebung sicherlich noch nicht im Detail feststehen, überhaupt erst zu ermöglichen oder zumindest informationell zu unterstützen.

Im Zusammenhang mit den Datenschutzgrundsätzen der **Datenminimierung** einerseits sowie der **Speicherbegrenzung** andererseits müssen alle Gestaltungsoptionen die Kriterien der Erheblichkeit, Erforderlichkeit und Angemessenheit wahren. 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 Gestaltungsoption, 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, wird zudem in **prozeduraler** Hinsicht der Einsatz von **Fachpersona**l empfohlen, das die Einschätzung vornimmt, welche Gesundheitsdaten potenziell für die Gesundheitsversorgung des Patienten vonnöten sein werden. Mit Blick auf die **Datensparsamkeit** in zeitlicher Hinsicht gilt schließlich in Bezug auf sämtliche Gestaltungsoptionen zu erwähnen, dass keine allzu strengen Maßgaben an dieses Kriterium gestellt werden dürfen, da vor allem im Gesundheitsbereich nicht vorhersehbar ist, wann welche Informationen aus der ePA benötigt werden.

Zur Gewährleistung des Datenschutzgrundsatzes der **Richtigkeit** erscheint der Einsatz von **Fachpersonal** bei der Anlage und Befüllung in allen Gestaltungsvarianten unabdinglich. Bei einer **„ex tunc“-Befüllung** ist vom 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** ergibt sich vor allem bei einem Verzicht auf ein **Registrierungserfordernis** die Forderung nach einer Etablierung von effektiven Instrumenten zur Identifikation und Authentifizierung der eingebundenen Akteure und von Protokollierungen. Das Registrierungserfordernis als solches ist unseres Erachtens aus datenschutzrechtlicher Perspektive gleichwohl nicht zwingend erforderlich.

Ergänzend zu den aus den Datenschutzgrundsätzen folgenden einschränkenden Vorgaben lassen sich den **Grundrechten** des Grundgesetzes und der Grundrechtecharta vor allem Impulse zur Wahl **ermöglichender Gestaltungsoptionen** entnehmen. Um künftige gesundheitsbezogene Entscheidungen selbstbestimmt vornehmen zu können, benötigt der/die Einzelne eine hinreichende informationelle Entscheidungsgrundlage. Diese dürfte sich durch einen **Verzicht** auf ein **gesondertes Registrierungserfordernis** sowie durch eine **umfassende, obligatorische Befüllung der ePA „ex tunc“** deutlich effektiver schaffen lassen.

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.

4 Berechtigung zum Zugriff auf die ePA

Neben der Anlage und Befüllung der ePA bestehen auch bezüglich der **Berechtigungen zum Zugriff** auf sie unterschiedliche Gestaltungsoptionen des Gesetzgebers (dazu sogleich »4.1). 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 (dazu »4.2). 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“ dargelegt und diskutiert.

4.1 Wesentliche denkbare Gestaltungsoptionen

Bei der Ausgestaltung der Zugriffsberechtigungen müssen grundsätzlich folgende Aspekte bedacht und geregelt werden: die Modalitäten der Erteilung von Zugriffsberechtigungen (»4.1.1), die sachliche Reichweite der Zugriffsberechtigungen (»4.1.2), die Dauer der Zugriffsberechtigung (»4.1.3) sowie der Entzug von Zugriffsberechtigungen (»4.1.4).

4.1.1 Modalitäten der Erteilung von Zugriffsberechtigungen

Zunächst steht es dem Gesetzgeber offen, ob er die **Zugriff**e auf die ePA einwilligungsunabhängig, also auf der Basis einer gesetzlichen Regelung, oder auf der Grundlage einer Einwilligung der Patientinnen und Patienten gestattet. Denkbar sind insoweit insbesondere automatische Zugriffsberechtigungen einerseits sowie Zugriffsberechtigungen basierend auf einer gesonderten Freischaltung durch die betroffenen Personen andererseits. Vor allem im Kontext des Zugriffs sind im Folgenden die Verarbeitungsgrundlagen der Anlage und Befüllung im Zusammenhang mit der Gestaltungsoption einer automatischen, einwilligungsunabhängigen Anlage und Befüllung **ohne** Registrierungserfordernis mitzuberücksichtigen (also Art. 9 Abs. 2 lit. h) und i) DSGVO), da sich aus diesen Grundlagen Vorgaben für die Ausgestaltungen der Zugriffsberechtigungen ergeben (können).

4.1.1.1 Automatische Zugriffsberechtigung

Im Falle einer automatischen Zugriffsberechtigung würden Leistungserbringer oder sonstige zugriffsberechtige Personen **ohne Zutun**, d.h. ohne vorherige Freischaltung durch den Patienten, einen Zugriff auf die ePA erhalten. Denkbar ist hier, dass nähere Ausgestaltungen dahingehend vorgenommen werden, ob erstens für die automatische Zugriffsberechtigung eine (tatsächliche) **Beziehung** zwischen dem Leistungserbringer und dem Patienten erforderlich ist, und zweitens, für welche **zeitliche Dauer** nach einem Kontakt mit dem Patienten die Zugriffsberechtigung besteht.[91]

Mit Blick auf die gegebenenfalls erforderliche **Beziehung** zwischen dem Leistungserbringer und dem Patienten bestünde auf der einen Seite die Möglichkeit, dass diese lediglich sehr lose ausgestaltet wird. So könnte seitens eines Leistungserbringers etwa allein die Kenntnis der Versichertennummer des Patienten als ausreichend erachtet werden. Auf der anderen Seite wäre allerdings auch vorstellbar, dass eine **enge** Beziehung vorausgesetzt wird, insbesondere, dass ein tatsächlicher Behandlungskontakt zwischen dem Leistungserbringer und dem Patienten stattgefunden haben muss – sei es in Gestalt eines physischen Kontakts zu einem bestimmten Zeitpunkt und an einem bestimmten Ort zwischen Leistungserbringer und Patienten, sei es als lediglich virtueller (z.B. Videosprechstunde)[92] oder telefonischer Kontakt. Zu bedenken wäre dabei, dass ein allzu strenges Erfordernis die Erreichung des Ziels einer Verbesserung von Qualität und Effizienz in der fach-, einrichtungs- und sektorenübergreifenden Gesundheitsversorgung abschwächen könnte.

Schutzmechanismen zur Eingrenzung einer automatischen Zugriffsberechtigung nach Kontakt könnten eine **zeitliche Beschränkung**, eine Widerspruchsmöglichkeit sowie eine etwaige Sperrungsmöglichkeit sein. Mit Blick auf die zeitliche Dauer bzw. Beschränkung der automatischen Zugriffsberechtigung könnte eine datenschutzfreundliche Voreinstellung mit einer Berechtigung für – wie gegenwärtig gemäß § 342 Abs. 2 Nr. 1 lit. f) SGB V – 18 Monate eingerichtet werden. Der Patient hätte dann die Option, diese Dauer beliebig zu verändern. Ebenso könnte für die betroffene Person die Möglichkeit eingeführt werden, Widerspruch gegen die automatische Zugriffsberechtigung einzulegen oder eine Sperrung der automatischen Zugriffsberechtigung durchzuführen. Während sich die **Widerspruchsmöglichkeit** gegen die automatische Zugriffsberechtigung an sich richtet, betrifft die **Sperrungsmöglichkeit** die zeitlich nachgelagerte Ebene, nämlich den Fall, dass eine Zugriffsberechtigung bereits automatisch erteilt wurde und die betroffene Person sich in weiterer Folge gegen die Berechtigung eines Leistungserbringers zum Zugriff auf die ePA aussprechen möchte.

Fallbeispiel: Im Falle einer automatischen Zugriffsberechtigung könnten die berechtigten Angehörigen des medizinischen Personals im Krankenhaus in B grundsätzlich auf Annas ePA zugreifen und Daten auslesen, ohne dass Anna ihnen dazu gesondert eine Berechtigung erteilen müsste. Je nachdem, welche Nähebeziehung der Gesetzgeber zu den Zugriffsberechtigten verlangt, könnte eine automatische Zugriffsberechtigung beispielsweise sämtlichen berechtigten Krankenhausangehörigen mit dem Einstecken von Annas eGK in ein Lesegerät

91 In der gegenwärtigen Ausgestaltung der ePA als Opt-in-Modell dürfen die Patienten gemäß § 342 Abs. 2 Nr. 1 lit. f) SGB V der Arztpraxis maximal 18 Monate Zugriff auf die ePA gewähren.

92 Vgl. etwa die in § 291 i.V.m. § 87 Abs. 2k SGB V verankerte Möglichkeit zur Videosprechstunde.

in der Ambulanz des Krankenhauses B erteilt werden. Sofern von Gesetzes wegen eine zeitliche Beschränkung vorgesehen ist, könnten die berechtigten Angehörigen des Krankenhauses ab jenem Zeitpunkt beispielsweise 18 Monate lang auf Annas ePA-Daten zugreifen.

4.1.1.2 Gesonderte Freischaltung

Im Gegensatz zur automatischen Zugriffsberechtigung wäre denkbar, den Leistungserbringern und anderen zugriffsberechtigten Personen die Berechtigung zum Zugriff auf die ePA erst nach einer **gesonderten Freischaltung** durch die Patienten (oder deren Vertreter[93]) zu gestatten. Vor allem mit Blick auf die oben angesprochene Gestaltungsoption einer automatischen, einwilligungsunabhängigen Anlage und Befüllung **ohne Registrierungserfordernis** könnte sich die Einführung eines gesonderten Freischaltungserfordernisses allerdings als problematisch erweisen. Sofern die Anlage und Befüllung automatisch, einwilligungsunabhängig (und ohne Registrierung) erfolgen soll, wäre ein Freischaltungserfordernis auch bezüglich der **Schreibberechtigung** von Leistungserbringern schwerlich mit der Möglichkeit der Befüllung durch die Leistungserbringer vereinbar. Ein Freischaltungserfordernis dürfte daher sinnvoll nur in Bezug auf die **Leseberechtigung**[94] von Leistungserbringern eingeführt werden.

Gestaltungsoffen erscheint ferner die **Form** der vorzunehmenden Freischaltung für den Patienten bzw. dessen Vertreter. Diesbezüglich ist zum einen eine niedrigschwellige Freischaltung denkbar, etwa konkludent durch Vorzeigen der eGK und/oder Eingabe einer PIN in den Räumen des Leistungserbringers. Zum anderen ist auch das Erfordernis einer expliziten Erklärung vorstellbar, etwa über die ePA-App/Website.

Fallbeispiel: Im Falle eines gesonderten Freischaltungserfordernisses könnten die Angehörigen des medizinischen Personals im Krankenhaus B nicht automatisch auf die vorhandenen Daten in Annas ePA zugreifen. Vielmehr müsste Anna – je nach Ausgestaltung – beispielsweise jeden Akteur gesondert freischalten, indem sie sich etwa über ihr Endgerät in die ePA einloggt und die Freischaltung vornimmt, oder indem sie die Freischaltung über die IT-Infrastruktur des Krankenhauses erklärt.

4.1.1.3 Differenziertes Zugriffsberechtigungssystem

Ferner bestünde für den Gesetzgeber bei der Einführung der ePA als Opt-out-Modell zu Versorgungszwecken die Möglichkeit, sich für ein **differenziertes Zugriffsberechtigungssystem** zu entscheiden. Dieses würde eine Mischung darstellen aus der automatischen Vergabe der Zugriffsberechtigungen für bestimmte Gruppen (bzw. einzelne Leistungs-

93 Für die gegenwärtig als Opt-in-Modell ausgestaltete ePA beispielsweise der Techniker Krankenkasse können bis zu fünf Vertreterinnen bzw. Vertreter benannt werden, siehe https://www.tk.de/techniker/leistungen-und-mitgliedschaft/online-services-versicherte/elektronische-patientenakte-tk-safe/zugang-elektronische-patientenakte-epa-vertretung/patientenakte-tk-safe-vertretung-2120194?tkcm=aaus. Die Regelungen des SGB V sehen eine derartige zahlenmäßige Begrenzung freilich nicht vor.

94 Die Leseberechtigung umfasst lediglich den Abruf sowie das Lesen von (Gesundheits-)Daten.

erbringer) einerseits sowie der gesonderten Freischaltung der Zugriffsberechtigungen für bestimmte Gruppen (bzw. einzelne Leistungserbringer) andererseits. Erst durch die gesonderte Freischaltung der Zugriffsberechtigung hätte die bestimmte Gruppe bzw. der bestimmte Leistungserbringer Zugriff auf die ePA und könnte Gesundheitsinformationen abrufen oder in sonstiger Weise weiterverarbeiten und würde im Protokollierungssystem aufscheinen. Angemerkt sei an dieser Stelle, dass sich das gesonderte Freischaltungserfordernis im Kontext eines differenzierten Zugriffsberechtigungssystems sinnvollerweise ebenso nur auf die Leseberechtigung von Leistungserbringern beziehen dürfte.

Fallbeispiel: Je nach Ausgestaltung des differenzierten Zugriffsberechtigungssystems könnten beispielsweise die Ärztinnen und Ärzte im Krankenhaus B automatisch auf Annas ePA-Daten zugreifen, sobald Anna ihre eGK in ein Lesegerät im Krankenhaus eingesteckt hat. Die Pflegekräfte müsste Anna dagegen gesondert freischalten.

4.1.2 Reichweite der Zugriffsberechtigungen

Während in Punkt »4.1.1 vor allem die wesentlichen denkbaren Gestaltungsoptionen hinsichtlich der Frage aufgezeigt wurden, ob überhaupt eine Berechtigung zum Zugriff auf die ePA gewährt wird, geht es im Folgenden um den nachgelagerten Schritt, nämlich die Reichweite bzw. den Umfang einer bestehenden Zugriffsberechtigung. Im Wesentlichen denkbar sind hier eine umfassende Zugriffsberechtigung (»4.1.2.1) sowie eine starre (»4.1.2.2) bzw. flexible (»4.1.2.3) Gruppenzugriffsberechtigung.

4.1.2.1 Umfassende Zugriffsberechtigungen

Im Rahmen einer umfassenden Zugriffsberechtigung würden die zugriffsberechtigten Personen einen umfassenden Zugriff auf die (Gesundheits-)Daten in der ePA erlangen. Für sie bestünden daher **umfassende Möglichkeiten** mit Blick auf die Verarbeitungsarten (Abrufen, Lesen, Speichern etc.) der (Gesundheits-)Daten in der ePA. Lediglich durch den aktuellen Behandlungskonnex sowie die Erforderlichkeit würde die Zugriffsberechtigung eine (rechtliche, nicht: technische) Einschränkung erfahren. Solange daher eine aufrechte Zugriffberechtigung besteht und der aktuelle Behandlungskonnex dies erfordert, könnten sämtliche (Gesundheits-)Daten in der ePA, ungeachtet ihrer Sensibilität, unbegrenzt abgerufen, gelesen, gespeichert etc. werden.

Diese weitreichende Zugriffsberechtigung könnte allerdings durch zusätzliche technische Einschränkungen eingehegt werden. Vorstellbar wäre, dass die umfassende Zugriffsberechtigung neben dem aktuellen Behandlungskonnex und der Erforderlichkeit auch die physische oder virtuelle Anwesenheit der betroffenen Person und/oder das Vorzeigen der eGK und/oder eine sonstige tatsächliche Beziehung zwischen Leistungserbringer und Patienten bedingt. Zu berücksichtigen ist dabei freilich, dass zu weitgehende Einschränkungen wiederum einem Freischaltungserfordernis entsprechen könnten.

Fallbeispiel: Auf der Basis von umfassenden Zugriffsberechtigungen könnten alle berechtigten Angehörigen des medizinischen Personals des Krankenhauses B (Ärzte, Pflegekräfte etc.) auf sämtliche Daten in Annas ePA zugreifen.

4.1.2.2 Starre Gruppenzugriffsberechtigung

Im Gegensatz zu einer umfassenden Zugriffsberechtigung, die lediglich eine bereits bestehende Berechtigung zum Zugriff auf die ePA an sich sowie einen Behandlungskonnex und die Erforderlichkeit verlangt, wäre auch die Einführung von starren **Gruppenzugriffsberechtigungen** denkbar. Dadurch wären unterschiedliche **vorgegebene** Ausgestaltungen der **Reichweite** der Zugriffsberechtigungen mit Blick auf die **Art** der Daten, die **Dauer** ihrer Verarbeitung und den **Umfang** möglich. Erwähnenswert erscheint dabei, dass die (zeitliche) Dauer der Zugriffsberechtigung prinzipiell ein eigenes Gestaltungselement darstellt, das mit der (nach sachlichen Gesichtspunkten abgegrenzten) Gruppenzugriffsberechtigung zunächst einmal nicht direkt verknüpft wäre.

Freilich wäre bei einem System mit einer starren Gruppenzugriffsberechtigung denkbar, nicht nur die sachliche Reichweite, sondern ebenso die Dauer starr vorzugeben. Insofern könnte eine starre Einteilung der angedachten zugriffsberechtigten Personen (vor allem Leistungserbringer) in **Gruppen** erfolgen, verbunden mit einer im Vorhinein jeweils festgesetzten Reichweite der Zugriffsmöglichkeit auf die ePA. Im Rahmen **starrer** Gruppenzugriffsberechtigungen würden den Patienten **keine** Möglichkeiten zu **Änderungen** etwa hinsichtlich der Gruppe an sich oder der standardmäßig festgesetzten Zugriffsmöglichkeiten der Gruppe zustehen.

Eine **erste Gruppe** könnte beispielsweise umfassen – wie gegenwärtig im deutschen Recht vorgesehen – Ärztinnen und Ärzte, Zahnärzte, Psychotherapeutinnen sowie berufsmäßige Hilfskräfte und zur Vorbereitung auf den Beruf oder etwa – wie gegenwärtig im österreichischen Recht vorgesehen – Ärztinnen und Ärzte, Einrichtungen der Pflege, deren gesetzliche oder bevollmächtigte Vertreter sowie Mitarbeiter der Ombudsstelle. Mit der Gruppenzugehörigkeit, die vor allem zu Versorgungszwecken bestünde, wäre für den jeweiligen Leistungserbringer eine im Vorhinein festgesetzte, für ihn in seiner Funktion **typischerweise benötigte Reichweite** verbunden, die sich bei der soeben genannten Gruppe als umfassend darstellen würde. Für sie bestünden **vollumfängliche** Möglichkeiten zur Verarbeitung der Gesundheitsdaten (Abrufen, Lesen, Speichern etc.).

Eine oder mehrere **weitere Gruppe(n)**, die mit Versorgungsaufgaben betraut sind, könnten etwa lediglich Berechtigungen zum Lesen, Speichern und Verwenden von **bestimmten** Datensätzen erhalten, wie dies etwa gegenwärtig in Deutschland auf Gesundheits-, Krankenhaus- und Pflegepersonal, Hebammen, Physiotherapeuten sowie Apotheken zutrifft. Freilich ist auch denkbar, dass Gruppen bestehen, die zwar prinzipiell eine Zugriffsberechtigung erhalten, allerdings sodann keine Berechtigungen für eine **Verarbeitungsart** erteilt bekommen (z.B. haben in Österreich gegenwärtig „Dentisten“, also Zahntechniker, keine Zugriffsberechtigung). Im Übrigen wäre ebenso denkbar, dass eine Gruppe, die mit Aufgaben jenseits von Versorgungszwecken betraut ist (z.B. ein Mitarbeiter eines öffentlichen Gesundheitsdienstes), ebenfalls punktuelle Berechtigungen erhält.

Fallbeispiel: Bei starren Gruppenzugriffsberechtigungen könnten beispielsweise lediglich die Ärztinnen und Ärzte im Krankenhaus B auf sämtliche Daten in Annas ePA zugreifen. Den Pflegekräften könnte dagegen lediglich die Befugnis zum Auslesen der Medikationsinformationen zugewiesen sein. Anna könnte den Pflegekräften auch keine weitergehende Leseberechtigung erteilen.

4.1.2.3 Flexible Gruppenzugriffsberechtigung

In Abweichung von der Gestaltungsoption der starren Gruppenzugriffsberechtigungen bestünde für den Gesetzgeber die Möglichkeit, dass zwar **standardmäßig** durch **Voreinstellung** bestimmte Gruppeneinteilungen für die Patienten vorgesehen sind, verbunden mit Einschränkungen bezüglich des jeweiligen Umfangs des Zugriffs, den Patienten allerdings die Möglichkeit zukäme, **Veränderungen** vorzunehmen. Betreffen könnte dies etwa die Dauer, die Verarbeitungsart oder die Gruppenzugehörigkeit an sich. Dementsprechend könnte die betroffene Person einer Gruppe (bzw. einem Leistungserbringer), die (bzw. der) an sich nur auf das Abrufen, Lesen sowie Speichern von bestimmten Datensätzen oder nur für eine bestimmte Dauer zugriffsberechtigt wäre, eine erweiterte Zugriffsberechtigung erteilen. Die anfangs bestehenden (datenschutzfreundlichen) Voreinstellungen hinsichtlich der Zugriffsberechtigungen könnten demnach durch die betroffenen Personen flexibel in jede Richtung umgestellt werden.

Fallbeispiel: Im Falle flexibler Gruppenzugriffsberechtigungen könnten zwar grundsätzlich wiederum nur Ärztinnen und Ärzte umfassend auf Annas ePA zugreifen und die Pflegekräfte lediglich auf Medikationsdaten. Allerdings hätte Anna die Möglichkeit, einzelnen oder allen Pflegekräften eine Leseberechtigung auch bezüglich anderer ePA-Daten zu erteilen.

4.1.3 Dauer der Zugriffsberechtigung

Zudem bedarf die Dauer der Zugriffsberechtigungen im Rahmen der Einführung der ePA als Opt-out-Modell zu Versorgungszwecken als eigenes Gestaltungselement einer näheren Betrachtung. Denkbar wäre hierbei für den deutschen Gesetzgeber zum einen, dass er entweder eine zeitliche Begrenzung des Zugriffs **automatisch** oder erst durch **aktives Handeln** des Patienten vorsieht. Diesbezüglich dürfte der Gesetzgeber in seiner Entscheidung allerdings durch die gewählte Gestaltungsoption bezüglich der Modalitäten der Erteilung von Zugriffsberechtigungen eingeschränkt werden, da die Dauer der Zugriffsberechtigung sinnvollerweise mit deren Erteilung einhergehen müsste. Sofern sich der Gesetzgeber daher für die Einführung von automatischen Zugriffsberechtigungen entscheiden sollte, müsste er prinzipiell über eine automatische zeitliche Begrenzung des Zugriffs entscheiden.

Zum anderen bestünde für ihn die Möglichkeit, dass die zeitliche Begrenzung des Zugriffs als **zwingende** – sowohl hinsichtlich des „Ob“ als auch hinsichtlich der Dauer – oder etwa als **dispositive** Gestaltung vorgegeben wird. Hierbei dürfte für den Gesetzgeber auf den ersten Blick bei einer Entscheidung für die Einführung von automatischen zeitlichen Begrenzungen des Zugriffs vor allem im Lichte der Patientenautonomie eine dispositive Gestaltung erwägenswert sein.

Fallbeispiel: Im Falle einer bestehenden Zugriffsberechtigung könnten die berechtigten Angehörigen des medizinischen Personals im Krankenhaus in B auf Annas ePA zugreifen. Sofern von Gesetzes wegen eine starre zeitliche Beschränkung vorgesehen ist, könnten die berechtigten Angehörigen des Krankenhauses ab jenem Zeitpunkt beispielsweise 18 Monate lang auf Annas ePA-Daten zugreifen. Eine Verlängerung oder Verkürzung wäre bei einer starren Zeitgrenze nicht möglich. Der Gesetzgeber könnte allerdings auch vorsehen, dass Anna die voreingestellte zeitliche Grenze individuell und flexibel abändern kann – etwa auf drei Jahre verlängern könnte, falls sie oder ihr Hausarzt sich im Rahmen einer zwei Jahre später stattfindenden Behandlung in A mit einem behandelnden Arzt in B austauschen möchte.

4.1.4 Entzug von Zugriffsberechtigungen

Zuletzt müsste der Gesetzgeber entscheiden, wie der **Entzug** von bereits bestehenden bzw. erteilten Zugriffsberechtigungen ausgestaltet sein soll. Wie bereits erwähnt, kann eine von Beginn an voreingestellte **zeitliche Dauer** der Zugriffsberechtigung eingeführt werden, verbunden mit der Option, dass die betroffene Person diese entweder verkürzt oder verlängert. Beispielsweise könnte eine zeitliche Befristung von 18 Monaten voreingestellt werden, und der Patient hätte zusätzlich die Möglichkeit, diese zu verlängern oder zu verkürzen.

Ebenso wäre vorstellbar, nachträgliche Entziehungs- und Sperrmöglichkeiten einzuführen. Ein Leistungserbringer hätte nach der **Entziehung** der Zugriffsberechtigung keine Möglichkeiten mehr, in die ePA Einsicht zu nehmen bzw. Informationen abzurufen oder weiterzuverarbeiten. Vorstellbar wäre allerdings, dass im sogenannten „Notfallmodus“ dennoch (eingeschränkte) Einsichtsmöglichkeiten bestünden (dazu mehr unter Punkt »5.1.3.2.2.2). Hingegen würden im Rahmen einer nachträglichen **Sperrung** der Zugriffsberechtigungen – entweder von bestimmten Gruppen oder einzelnen Leistungserbringern oder anderen zugriffsberechtigten Personen – nicht nur keine Einsichts-, Abruf- oder sonstigen Weiterverarbeitungsmöglichkeiten gestattet werden, sondern es würde auch in einem potenziell vorgesehenen „Notfallmodus“ kein Zugriff auf die ePA gewährt.

Im Übrigen wäre wiederum zu überlegen, in welcher **Form** der Entzug von Zugriffsberechtigungen vorgenommen werden könnte. In niedrigschwelliger Weise könnten die betroffenen Personen dies direkt in der ePA-App/Website vornehmen. Höherschwellige Möglichkeiten könnten unter anderem die physische Anwesenheit der betroffenen Personen erfordern, etwa in den Räumlichkeiten des Zugriffsberechtigten, dem die Berechtigung entzogen werden soll, oder in den Räumlichkeiten eines anderen Leistungserbringers.

Fallbeispiel: Sofern sich Anna dazu entschließt, ihren Hausarzt in A zu wechseln, und deshalb nicht mehr möchte, dass dieser in ihre ePA-Daten Einsicht nehmen kann, könnte sie ihm seine Zugriffsberechtigung entziehen bzw. ihn sogar für einen gegebenenfalls vorgesehenen Notfallmodus sperren. Dies könnte sie entweder – niedrigschwellig – über die ePA-App auf ihrem Handy vornehmen oder – höherschwellig – in den Räumlichkeiten ihres alten oder neuen Hausarztes.

4.2 Datenschutzrechtliche Bewertung

Die Ausgestaltung der Zugriffsmöglichkeiten auf die in der ePA gespeicherten (Gesundheits-)Daten durch die beteiligten Akteure – insbesondere durch die Leistungserbringer sowie die Patientinnen und Patienten selbst – unterliegt im Grundsatz jenen datenschutzrechtlichen Vorgaben, die bereits oben unter Punkt »3.2. mit Blick auf die Anlage und Befüllung der ePA aufgezeigt wurden. Im Hinblick auf die Berechtigung zum Zugriff auf die ePA gilt es daher, im Folgenden ebenso die Vorgaben in Bezug auf die Zulässigkeit des **„Ob“** des Zugriffs von der Rechtmäßigkeit des **„Wie“** der Datenverarbeitung zu unterscheiden. Bevor die Modalitäten der Berechtigungen des Zugriffs auf die ePA nach Maßgabe zumal der Datenschutzgrundsätze – also das „Wie“ der Verarbeitung betreffend – bewertet werden, sind zunächst die einschlägigen Verarbeitungsgrundlagen – betreffend das „Ob“ der Verarbeitung – zu benennen.

4.2.1 Verarbeitungsgrundlage („Ob“)

Anknüpfend an die Überlegungen zur Anlage und Befüllung der ePA wird im Rahmen der Ausübung von Zugriffsberechtigungen sowohl beim Abruf als auch bei der sonstigen Weiterverarbeitung (z.B. Lesen) der gespeicherten personenbezogenen Gesundheitsdaten (Art. 4 Nr. 15 DSGVO) eine eigenständige Verarbeitungsgrundlage nach Art. 9 DSGVO benötigt. Denn die im vorgelagerten Schritt erfolgte Anlage und Befüllung der ePA stellt einen unabhängigen Datenverarbeitungsvorgang dar und bedarf prinzipiell einer strengen Trennung vom **Abruf** und von der (sonstigen) Weiterverarbeitung.[95] Bereits an dieser Stelle wird allerdings darauf hingewiesen, dass sich aus der/den gewählten Verarbeitungsgrundlage/n bei der Anlage und Befüllung Vorgaben für die Ausgestaltung mit Blick auf den Zugriff bzw. in weiterer Folge das Abrufen und die sonstige Weiterverarbeitung der ePA-Daten ergeben können. Dass einzelne Leistungserbringer zum Abruf und der (sonstigen) Weiterverarbeitung von in der ePA gespeicherten Gesundheitsinformationen berechtigt sind, setzt daher zunächst einen Erlaubnistatbestand nach **Art. 9 Abs. 2 DSGVO** voraus.

95 Dass der Begriff „Verarbeitung“ umfassend ist, zeigt die Begriffsbestimmung in Art. 4 Nr. 2 DSGVO, die wie folgt lautet: „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“.

Im Hinblick auf die **Verarbeitungsgrundlage** hat der Gesetzgeber grundsätzlich erneut die Wahl, eine explizite Einwilligung (Art. 9 Abs. 2 lit. a) DSGVO) zu fordern oder sich für einen einwilligungsunabhängigen gesetzlichen Verarbeitungstatbestand zu entscheiden. Mit Blick auf die gesetzlichen einwilligungsunabhängigen Verarbeitungstatbestände kämen auf den ersten Blick wiederum Art. 9 Abs. 2 lit. h) und lit. i) DSGVO in Betracht.[96] Trotz der Möglichkeit des Gesetzgebers, den expliziten Einwilligungstatbestand des Art. 9 Abs. 2 lit. a) DSGVO zu wählen, sind die – wie oben dargelegt – gesetzlichen einwilligungsunabhängigen Ausnahmetatbestände (Art. 9 Abs. 2 lit. h) und lit. i) DSGVO) bei der Einführung der ePA als Opt-out-Modell für ihn nicht gesperrt. Vielmehr stehen sich die in Art. 9 Abs. 2 DSGVO verankerten Ausnahmetatbestände **gleichberechtigt** gegenüber.

Während der Verarbeitungstatbestand in Art. 9 Abs. 2 lit. i) DSGVO die Verarbeitung aus Gründen des genuin **öffentlichen** Gesundheitsinteresses im Bereich der „öffentlichen Gesundheit" legitimiert und daher prinzipiell im Bereich der Gefahrenabwehr bzw. Risikovorsorge sowie der „Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung" einzureihen ist, trägt der Rechtfertigungstatbestand des Art. 9 Abs. 2 lit. h) i.V.m. Abs. 3 DSGVO insbesondere der Bedeutung der Gesundheit für die Patienten und der Gesellschaft insgesamt Rechnung (Belange der individuellen Gesundheit, insbesondere medizinische Diagnostik, Versorgung und Behandlung). Demzufolge stehen bei Art. 9 Abs. 2 lit. h) i.V.m. Abs. 3 DSGVO primär die **individuellen Interessen** an einer funktionierenden Gesundheitsversorgung im Vordergrund.[97]

Unter Berücksichtigung dieser Maßgaben erscheint daher für den Informationsabruf zu den hier allein relevanten Versorgungszwecken vor allem **Art. 9 Abs. 2 lit. h) i.V.m. Abs. 3 DSGVO** einschlägig zu sein, es sei denn, für die Leseberechtigung würde ein gesondertes, einer Einwilligung gleichkommendes Freischaltungserfordernis (Art. 9 Abs. 2 lit. a) DSGVO) eingeführt werden. Der Abruf von Gesundheitsinformationen des Patienten dient nicht nur der Verbesserung von präventiven und nachsorgenden diagnostischen, kurativen sowie therapeutischen Entscheidungen, sondern ermöglicht auch ein stärker interprofessionelles und effektives Zusammenwirken in der fach-, sektoren- und einrichtungsübergreifenden Gesundheitsversorgung.[98]

Vor allem durch die Möglichkeit der Zugriffsberechtigten, die Gesundheitsinformationen in Echtzeit abzurufen (bzw. sonstig weiterzuverarbeiten), kann die Qualität der Behandlung verbessert werden und können Behandlungs- bzw. Medikationsfehler oder unerwünschte Arzneimittelwirkungen vermieden werden. Diese Verarbeitungszwecke stellen primär auf die **individuellen Interessen** der Patientinnen und Patienten an einer funktionierenden Gesundheitsversorgung ab und passen mithin unter die nach Art. 9 Abs. 2 lit. h) i.V.m. Abs. 3 DSGVO vorausgesetzten Zwecke „Gesundheitsvorsorge", „medizinische Diagnostik" sowie „Versorgung oder Behandlung im Gesundheits- oder Sozialbereich". Da der Abruf (bzw. die sonstige Weiterverarbeitung) somit nicht primär aus Gründen des

96 Wie bereits oben unter Punkt »3.2.1.2 dargelegt, käme prinzipiell ebenso die Verarbeitungsgrundlage nach Art. 9 Abs. 2 lit. g) DSGVO in Betracht. Da Art. 9 Abs. 2 lit. i) DSGVO allerdings gegenüber Art. 9 Abs. 2 lit. g) DSGVO als *lex specialis* gilt, wird Art. 9 Abs. 2 lit. g) DSGVO im Folgenden ausgeblendet.

97 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.

98 Siehe m.w.N. *C. Dochow*, MedR 2021, 13 (16).

genuin öffentlichen Gesundheitsinteresses im Bereich der „öffentlichen“ Gesundheit“ erfolgt, sondern vielmehr die **individuellen** Interessen der Patienten an einer funktionierenden Gesundheitsversorgung im Vordergrund stehen, ist unseres Erachtens dem Ausnahmetatbestand des **Art. 9 Abs. 2 lit. h) i.V.m. Abs. 3 DSGVO** der Vorzug gegenüber Art. 9 Abs. 2 lit. i) DSGVO zu geben.

Zusätzlich zu den in Art. 9 Abs. 2 lit. h) DSGVO verankerten materiellen Voraussetzungen sind dort ebenso, wie bereits dargelegt, gewisse **Vorbehalte** implementiert worden. Der Ausnahmetatbestand des Art. 9 Abs. 2 lit. h) DSGVO knüpft nämlich an legislative Maßnahmen an und fordert unter Verweis auf Art. 9 Abs. 3 DSGVO „Bedingungen und Garantien“ zum Schutze der Betroffenenrechte ein.[99] Während **Art. 9 Abs. 3 DSGVO** konkretisiert, was *in jedem Falle* als „Bedingungen und Garantien“[100] vorzusehen ist – die Verarbeitung darf demnach prinzipiell nur durch **Fachpersonal** erfolgen –, eröffnet **Art. 9 Abs. 4 DSGVO** den Mitgliedstaaten die *weitergehende* Möglichkeit, „**zusätzliche Bedingungen**, einschließlich Beschränkungen, ein[zu]führen oder aufrecht[zu]erhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist“. Bei der Ausfüllung der eröffneten **Gestaltungsspielräume** ist der deutsche Gesetzgeber allerdings, wie bereits ausgeführt, nicht völlig frei. Neben den Datenschutzgrundsätzen im Sinne des Art. 5 DSGVO hat er ebenso die Grundrechte des Grundgesetzes und/oder die Unionsgrundrechte mitzuberücksichtigen.

Bei sämtlichen der oben unter Punkt »4.1 beschriebenen Gestaltungsoptionen muss der Gesetzgeber somit spezifische Bedingungen und Garantien vorsehen, die dem jeweiligen Charakter der gewählten Option bezüglich der Zugriffsberechtigung hinreichend Rechnung tragen. Aus Gründen der Übersichtlichkeit werden die im Einzelnen gebotenen spezifischen Bedingungen und Garantien im Kontext der Datenschutzgrundsätze behandelt (siehe sogleich Punkt »4.2.2)

4.2.2 Datenschutzgrundsätze („Wie“)

Mit Blick auf die Verarbeitung von Gesundheitsdaten müssen vor allem die Datenschutzgrundsätze des Art. 5 DSGVO berücksichtigt werden. Einer näheren Betrachtung bedürfen – wie bereits bei der Anlage und Befüllung der ePA – insbesondere die folgenden Datenschutzgrundsätze: die Transparenz der Verarbeitung im Sinne des Abs. 1 lit. a) (dazu »4.2.2.1), der Grundsatz der Zweckfestlegung und -bindung gemäß Abs. 1 lit. b) (dazu »4.2.2.2), die Prinzipien der Datenminimierung nach Abs. 1 lit. c) sowie der Speicherbegrenzung nach Abs. 1 lit. e) (dazu »4.2.2.3), die Richtigkeit der Verarbeitung gemäß Abs. 1 lit. d) (dazu »4.2.2.4) und das Gebot der Integrität und der Vertraulichkeit gemäß Abs. 1 lit. f) (dazu »4.2.2.5). Da diese Grundsätze bei jeder Datenverarbeitung erfüllt werden müssen, sind sie folglich ebenso im Kontext der Berechtigungen zum

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

100 Art. 9 Abs. 3 DSGVO setzt fest, dass „[d]ie in Absatz 1 genannten personenbezogenen Daten […] zu den in Absatz 2 Buchstabe h genannten Zwecken verarbeitet werden [dürfen], wenn diese Daten von **Fachpersonal** oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen dem **Berufsgeheimnis** unterliegt, oder wenn die Verarbeitung durch **eine andere Person** erfolgt, die ebenfalls nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer **Geheimhaltungspflicht** unterliegt.“

Zugriff auf die ePA im Rahmen eines Opt-out-Modells maßgeblich, etwa beim Abruf und beim Einsehen etc. der Gesundheitsdaten.[101]

4.2.2.1 Transparenz

Im Hinblick auf den Datenschutzgrundsatz der **Transparenz** (Art. 5 Abs. 1 lit. a) DSGVO), der neben der Bereitstellung von Informationen ebenso verlangt, dass die Verarbeitungen aufgrund von Zugriffsberechtigungen in transparenter Weise erfolgen, sodass die betroffenen Personen die Zugriffe antizipieren und nachvollziehen können, erscheint auf den ersten Blick vor allem die Gestaltungsoption **mit gesonderter Freischaltung** der Zugriffsberechtigung in Bezug auf die Leseberechtigung für maximale Transparenz zu sorgen. In diesem Falle müssten die Patientinnen und Patienten bereits vor dem Abruf und Lesen ihrer ePA-Daten eine gesonderte Freischaltung für die anderen Akteure (z.B. Leistungserbringer) tätigen. Dies würde einer prospektiv verstandenen Transparenz in größtmöglichem Umfang Rechnung tragen. Ob diese Freischaltung sodann für jeden einzelnen anderen Zugriffsberechtigten oder für bestimmte Berechtigungsgruppen abgegeben werden müsste, hängt davon ab, ob eine gänzlich gesonderte Freischaltung (vgl. »4.1.1.2) oder ein differenziertes Berechtigungssystem (vgl.»4.1.1.3) gewählt wird.

Ein gesondertes Freischaltungserfordernis würde allerdings nicht nur, wie bereits unter Punkt »4.1.1 angedeutet, in ein Spannungsverhältnis zur Gestaltungsoption einer automatischen Anlage und Befüllung ohne Registrierungserfordernis treten – die Leistungserbringer könnten bzw. müssten die ePA dann zwar ohne Zutun des Patienten beschreiben, könnten bzw. dürften aber keine Daten aus der ePA auslesen. Eine Freischaltung der Leseberechtigung würde außerdem und vor allem dem **Zweck der ePA widerstreben**, eine möglichst vollständig informierte und hochwertige Gesundheitsversorgung zu gewährleisten. Denn die Realisierung dieses Zwecks wird durch jeden weiteren prozeduralen Schritt, der dem Patienten oder Dritten bei der Verarbeitung der ePA-Daten abverlangt wird (hier: Erteilung der Leseberechtigung), zusätzlich erschwert.

Sofern sich, wie sogleich zu überlegen ist, den informationellen Anforderungen des Transparenzgebots auch im Falle einer **automatischen Erteilung der Zugriffsberechtigungen** genügen lässt und dem Patienten überdies im Ausgleich umfangreiche Steuerungsmöglichkeiten in Bezug auf die abrufbaren Inhalte der ePA eingeräumt werden (siehe dazu eingehend Punkt »5.), verdient diese Ausgestaltungsoption mit Blick auf die Zwecksetzungen der ePA prinzipiell den Vorrang. Um trotz automatischer Zugriffsberechtigungen dem Transparenzgebot gerecht zu werden, besteht für den Gesetzgeber zunächst die Möglichkeit, eine Ausgestaltungsform zu wählen, die eine qualifizierte Beziehung zwischen dem Zugriffsberechtigten und dem Patienten verlangt und dabei sicherstellt, dass der Patient unmittelbar „vor Augen“ hat, dass hier ein Dritter über den Zugriff auf seine ePA verfügt. Eine allzu lose Beziehung zwischen Zugriffsberechtigtem und Patienten, wie etwa die bloße Kenntnis der Versichertennummer, wäre nicht ausreichend, um dem Transparenzgrundsatz zu genügen. Erst durch ein **physisches oder wenigstens virtuelles Zusammentreffen** im Rahmen eines Behandlungskontakts, d.h. wenn sich die betroffene Person in Grundzügen ein Bild über die zugriffsberechtigte Person machen kann, kann dem Grundsatz der Transparenz hinreichend Rechnung getragen werden.

101 Vgl. *P. Schantz*, in: H. A. Wolff/S. Brink (Hrsg.), BeckOK Datenschutzrecht, Stand 1.11.2021, Art. 5 DSGVO Rn. 2.

Des Weiteren darf im Falle automatischer Zugriffsberechtigungen nicht davon ausgegangen werden, dass der durchschnittliche Patient mit der Verarbeitung seiner Daten rechnet. Daher muss er im Vorfeld, also bereits mit der Einrichtung seiner ePA, in „verständlicher, klarer und einfacher Sprache“ ausreichende **Informationen** über den Umstand erhalten, wer unter welchen Voraussetzungen und in welchem sachlichen und zeitlichen Umfang automatisch Zugriff auf seine ePA erhält. Da im Kontext der Gesundheitsversorgung allerdings nicht eindeutig im Vorhinein feststellbar ist, wer zukünftig eine Berechtigung zum Zugriff auf die ePA und mithin z.B. die Gesundheitsdaten abruft und liest, um dem Individuum eine qualitativ hochwertige Gesundheitsversorgung zu ermöglichen, dürfen bezüglich der Konkretisierung der Informationen freilich nicht übermäßig strenge Maßstäbe gefordert werden. Insgesamt erweist sich daher die automatische Erteilung von Zugriffsberechtigungen auch ohne gesonderte Freischaltung als mit dem Transparenzgebot vereinbare Gestaltungsoption.

Transparenzbedingte Vorgaben bestehen ferner in Bezug auf die Gestaltungsoption der vorgefassten **Gruppenzugriffsberechtigungen**, sei deren Vorgabe flexibel oder starr. Durch im Vorhinein festgesetzte Berechtigungsgruppen würden die betroffenen Patienten einen groben Überblick erhalten über die Reichweite der jeweiligen Zugriffsberechtigungen mit Blick auf die Zeit (z.B. angemessenes Zeitintervall von ein bis zwei Jahren), die Verarbeitungsarten (z.B. Lesen, Speichern) und die Datenfelder (z.B. ob auch besonders sensible Daten verarbeitet werden dürften). Anders als im Rahmen von umfassenden Zugriffsberechtigungen bestünde für die Patienten eine erhöhte Nachvollziehbarkeit hinsichtlich der jeweiligen Reichweite der Zugriffsberechtigungen. Im Falle einer **flexiblen** Gruppenzugriffsberechtigung könnten die betroffenen Personen dabei zudem im Nachhinein selbstständige Veränderungen vornehmen, was wiederum für mehr Transparenz sowie eine erhöhte Patientensouveränität sorgen dürfte. Es sprechen daher im Lichte des Datenschutzgrundsatzes der Transparenz gute Gründe dafür, **flexible Gruppenzugriffsberechtigungen** einzuführen.

4.2.2.2 Zweckfestlegung und -bindung

Neben dem Transparenzgebot haben die Verarbeitungen der personenbezogenen Daten im Rahmen der dargelegten Gestaltungsoptionen auch dem Datenschutzgrundsatz der **Zweckfestlegung und -bindung** (Art. 5 Abs. 1 lit. b) DSGVO) zu entsprechen. Die personenbezogenen Gesundheitsdaten dürfen demnach nur „für festgelegte, eindeutige und legitime Zwecke erhoben werden und […] nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden“.

Um im Rahmen der Zugriffsberechtigungen die Verarbeitungen der Gesundheitsdaten prinzipiell nur für den jeweiligen Versorgungs- und Behandlungszweck zu gestatten, scheinen vor allem **Berechtigungsgruppen** ein adäquates Mittel zu sein. Durch im Vorhinein (starr oder flexibel) festgesetzte Einstellungen könnte auch technisch wirksam festgelegt werden, wer für welche Dauer auf welche Datengruppe Zugriff hätte. Dies würde nicht nur dem Datenschutzgrundsatz der Zweckbindung, sondern ebenso dem Grundsatz der Datenminimierung (dazu sogleich unter Punkt »4.2.2.3) Rechnung tragen. Denn während beispielsweise der Allgemeinmediziner im Rahmen der Behandlung typischerweise einen umfassenden Zugriff auf sämtliche in der ePA gespeicherten Daten benötigt, ist die Apothekerin regelmäßig keineswegs auf einen solchen Zugriff angewiesen.

Obwohl im Rahmen von umfassenden Zugriffsberechtigungen eine – zwar nicht technische, aber rechtliche – Einschränkung dahingehend bestehen würde, dass die Verarbeitung von Gesundheitsdaten für die konkrete Verwendung (z.B. die ärztliche Behandlung) erforderlich ist, hätte dennoch prinzipiell jede an sich zugriffsberechtigte Person auf **sämtliche** in der ePA gespeicherten Gesundheitsdaten die Möglichkeit zum Zugriff und mithin zur Verarbeitung. Infolge dieser Gestaltung würde der Grundsatz der Zweckbindung (und, wie sogleich unter Punkt »4.2.2.3 darzustellen ist, auch der Grundsatz der Datenminimierung) unseres Erachtens entgegen den Vorgaben aus Art. 24 und Art. 25 DSGVO nicht durch hinreichende technisch-organisatorische Maßnahmen abgesichert. Der Gesetzgeber sollte daher auch vor diesem Hintergrund auf **Gruppenzugriffsberechtigungen** setzen. Den bisweilen nicht voraussehbaren Bedürfnissen einer angemessenen medizinischen Versorgung in atypischen Einzelfällen kann dabei Rechnung getragen werden, indem die Vorgaben dispositiv, also **flexibel,** erfolgen und der Patient den Umfang der Gruppenberechtigungen im Allgemeinen oder im Einzelfall eigenständig erweitern oder beschränken kann.

4.2.2.3 Datenminimierung und Speicherbegrenzung

4.2.2.3.1 Gruppenzugriffsberechtigungen

Wie angedeutet, streiten auch die Grundsätze der Datenminimierung (Art. 5 Abs. 1 lit. c) DSGVO) und der Speicherbegrenzung (Art. 5 Abs. 1 lit. e) DSGVO) aus vergleichbaren Gründen für die Einführung von **Gruppenzugriffsberechtigungen**. Sie dürften vor allem wegen des **Erforderlichkeitsgrundsatzes** geboten sein. Der Erforderlichkeitsgrundsatz besagt im vorliegenden Kontext, dass ein Informationsabruf nur zulässig ist, wenn und soweit dies zur Erreichung der konkreten Verarbeitungszwecke (konkreter Behandlungs- und Versorgungszweck) erforderlich ist und kein milderes, gleich effektives Mittel ersichtlich ist.[102] Insoweit kann eine Rolle spielen, in welcher Funktion der Verarbeiter auf die Informationen zugreift (z.B. als Arzt oder als Apotheker), und zu welchem konkreten Zweck (z.B. im Kontext einer Behandlung wegen Schwindelbeschwerden) er dies tut. Indem eine (starre oder flexible) Gruppenzugriffsberechtigung, typisierend anknüpfend an die Funktion des Verarbeiters, den Kreis technisch möglicher Verarbeitungen von vornherein einschränkt, werden nicht erforderliche Verarbeitungen in höherem Maße vermieden, als dies unter einer sachlich unbeschränkten Zugriffsberechtigung möglich wäre. Das Instrument der Gruppenzugriffsberechtigung ist somit jedenfalls ein gegenüber einer umfassenden Zugriffsberechtigung **milderes Mittel**.

Nun könnte man einwenden, dass eine gruppenweise Beschränkung der Zugriffsberechtigung zumindest in atypisch gelagerten Fällen den Zwecken der ePA zuwiderlaufen könnte – etwa, wenn eine im Zugriff beschränkte Apothekerin ausnahmsweise Einsicht in die ärztliche Diagnose benötigt, um den Patienten bei der Verwendung eines Medikaments zu beraten. Es könnten somit Zweifel daran bestehen, dass eine Gruppenzugriffsberechtigung tatsächlich **gleichermaßen effektiv** ist wie eine umfassende Zugriffsberechtigung. Diesem Einwand könnte der Gesetzgeber jedenfalls aber begegnen, indem er die Gruppenzugriffsberechtigungen **flexibel** ausgestaltet, und die Patienten im Einzelfall Abweichungen von den voreingestellten Gruppenzugriffsberechtigungen vornehmen könnten. Bis zu welchem Grad solche Veränderungen flexibel vorgenommen werden könnten, stünde

102 Vgl. etwa *M. Albers/R. Veit*, in: H. A. Wolff/S. Brink (Hrsg.), BeckOK Datenschutzrecht, Stand 1.11.2021, Art. 6 DSGVO Rn. 16.

dem Gesetzgeber prinzipiell frei. Anders als starr voreingestellte Gruppenzugriffsberechtigungen würde die nachträgliche Änderung z.B. der Gruppenzugehörigkeit eine gesonderte Freischaltung durch die betroffenen Personen erfordern.[103]

Dem Anliegen der Datenminimierung würde somit einerseits durch die im Sinne des Art. 25 Abs. 2 DSGVO datenschutzfreundlichen Voreinstellungen[104] entsprochen – von ihnen geht prinzipiell eine gewisse Lenkungsfunktion aus, denn die wenigsten betroffenen Personen werden die initialisierten, aber abänderbaren Zugriffsberechtigungen verändern.[105] Dennoch und andererseits bestünde für die Patienten im Sinne einer auch in atypischen Fällen effektiven Ausgestaltung der ePA zusätzlich die Möglichkeit, selbstbestimmt Veränderungen an dem vorgegebenen Zuschnitt vorzunehmen. Dies scheint vor allem in jenen Behandlungssituationen vonnöten zu sein, in denen der Gruppenzugriffsberechtigte aufgrund seiner standardmäßigen Zugriffsberechtigung auf bestimmte für die Behandlung möglicherweise notwendigen Gesundheitsdaten keinen Zugriff hätte.

Flexible Gruppenzugriffsberechtigungen mit anfangs bestehenden datenschutzfreundlichen Voreinstellungen stellen daher ein milderes, gleich effektives Mittel gegenüber der unbeschränkten Zugriffsberechtigung dar. Im Vergleich zu starren Berechtigungen dürften sie dabei im Übrigen die angemessenere Variante sein, da sie auch in atypischen Fällen erlauben, den Zwecken der ePA flexibel Rechnung zu tragen, und zudem keine allzu paternalistische Vorstellung von Patientensouveränität transportieren.[106]

4.2.2.3.2 Zeitliche Beschränkung der Zugriffsberechtigungen

Neben der personenbezogenen Einschränkung der Zugriffsberechtigungen scheint auch die **Dauer der Zugriffsberechtigungen** als eigenes Gestaltungselement in Ansehung der Speicherbegrenzung[107] von Relevanz zu sein. Dass sämtliche (automatisch oder manuell) erteilten Zugriffsberechtigungen ohne zeitliche Beschränkungen für den jeweiligen konkreten Verarbeitungszweck, d.h. vor allem zu Behandlungszwecken, erforderlich sind, dürfte zu verneinen sein. So benötigt etwa ein Apotheker für die standardmäßige Ausgabe von Medikamenten gewiss keinen zeitlich unbegrenzten Zugriff auf die Medikationsdaten, um etwaige Wechselwirkungen mit dem neu verschriebenen Medikament abzugleichen. Diese Überlegung spricht schon auf den ersten Blick für die Einführung von **automatisch voreingestellte**n zeitlichen Begrenzungen durch den Gesetzgeber.

103 Sofern die betroffene Person vorab über die wesentlichen Eckpunkte der Datenverarbeitung informiert wird („in informierter Weise") und sie zusätzlich eine echte Wahlmöglichkeit auch im Sinne eines Opt-out hätte („freiwillig"), kann von einer „eindeutigen bestätigenden Handlung" im Sinne des Art. 4 Nr. 11 DSGVO gesprochen werden. Da dies in casu erfüllt wäre, ist bei einer nachträglich getroffenen Erweiterung (bzw. Verkürzung) der Zugriffsberechtigung von einer Einwilligung auszugehen, legitimiert durch Art. 9 Abs. 2 lit. a) DSGVO.

104 Vgl. nur *M. Martini*, in: B. Paal/D. A. Pauly (Hrsg.), DSGVO/BDSG, 3. Aufl. 2021, Art. 25 Rn. 2.

105 Vgl. *Artikel 29-Datenschutzgruppe*, Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke, 01189/09/DE WP 163, 2009, S. 8; *M. Hansen*, in: S. Smitis/G. Hornung/I. Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 25 Rn. 41; *M. Martini*, in: B. Paal/D. A. Pauly (Hrsg.), DSGVO/BDSG, 3. Aufl. 2021, Art. 25 Rn. 46.

106 Für die Zulässigkeit starrer Zugriffsberechtigungen dagegen *C. Dochow*, MedR 2021, S. 13 (15).

107 Der Datenschutzgrundsatz der Speicherbegrenzung (Art. 5 Abs. 1 lit. e) DSGVO) stellt im Wesentlichen eine Konkretisierung der Datensparsamkeit in zeitlicher Hinsicht dar und gilt somit als Ausdruck des Erforderlichkeitsgrundsatzes. Vgl. diesbezüglich *J. Albrecht/F. Jotzo*, Das neue Datenschutzrecht der EU, 2017, Rn. 6. Zudem geht aus ErwGr 39 DSGVO hervor, dass die „Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt" zu bleiben hat.

In der Folge stellt sich dann die Frage, von welcher Dauer die zeitliche Begrenzung sein sollte und ob die Voreinstellung zwingend oder dispositiv sein sollte. Für eine **dispositive** Ausgestaltung der zeitlichen Begrenzungen streiten vor allem das Recht auf informationelle Selbstbestimmung im positiven Sinne sowie der Zweck der ePA, auch in atypischen Fällen erforderlichenfalls längere Zugriffsberechtigungen erteilen zu können. Der Gesetzgeber sollte es daher ermöglichen, dass der Patient voreingestellte zeitliche Begrenzungen der Zugriffsberechtigungen selbstständig modifizieren kann. Mit Blick auf die konkrete Dauer lässt sich dem Datenschutzrecht freilich keine bezifferbare Vorgabe entnehmen. Anhaltspunkt sollte die Überlegung sein, wie lange der betreffende Akteur für die ihm obliegenden Verarbeitungen typischerweise Zugriff benötigt. Vor diesem Hintergrund erscheint uns etwa eine Voreinstellung von 18 Monaten beispielsweise für Ärztinnen und Ärzte gut vertretbar zu sein.

4.2.2.3.3 Prozedurale Anforderungen

Schließlich müssen ungeachtet der gewählten Gestaltungsoption auch prozedurale Vorkehrungen getroffen werden, um die 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 Angehörige des **Fachpersonals** entscheiden können (vgl. in diesem Sinne Art. 9 Abs. 3 DSGVO). Sofern eine andere Person eine Verarbeitung ob ihrer Zugriffsberechtigung vornimmt, hat diese aber jedenfalls einer „Geheimhaltungspflicht“[108] zu unterliegen.

4.2.2.4 Richtigkeit

Im Hinblick auf den Datenschutzgrundsatz der Richtigkeit (Art. 5 Abs. 1 lit. d) DSGVO) erscheinen im Kontext der Zugriffsberechtigungen und der Verarbeitungsarten insbesondere die Aktualisierung und Vervollständigung der abgerufenen Informationen relevant. Auch wenn bei der Überprüfung der Richtigkeit von Bestandsdaten ein geringerer Maßstab als bei der Erhebung von Gesundheitsdaten angesetzt wird, ist zu erörtern, ob die Zugriffsberechtigten (z.B. Ärzte) etwaigen Pflichten zur Aktualisierung unterliegen, wenn sie beispielsweise im Rahmen des Abrufs und Lesens von einem Befund auf unrichtige oder veraltete Informationen stoßen. Hervorzuheben ist dabei, dass sich die **sachliche Richtigkeit** nur auf **Tatsachenangaben** (z.B. Körpergewicht sowie -größe der Patienten) und mithin nicht auf Werturteile (z.B. Diagnose von einem anderen Arzt) beziehen kann.[109] Dennoch kann es zu einer Berichtigung kommen, sofern ein Beweis verfügbar ist bzw. die Gesundheitsdaten als Tatsachenbestandteile etwa für eine Diagnose herangezogen werden.[110]

Gemäß Art. 5 Abs. 2 DSGVO ist allerdings grundsätzlich der **Verantwortliche** (Art. 4 Nr. 7 DSGVO), d.h. gemäß § 341 Abs. 4 SGB V die jeweilige **Krankenkasse**[111], „für die

108 Vgl. ebenso die Vorgaben zu den Geheimhaltungspflichten in Art. 90 DSGVO.

109 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.

110 Vgl. *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.

111 Siehe ebenso z. B. *J. Eichenhofer*, NVwZ 2021, 1090 (1092 f.).

Einhaltung“ des Datenschutzgrundsatzes der Richtigkeit „verantwortlich und muss dessen Einhaltung nachweisen können“. Hierbei scheint auf den ersten Blick problematisch, dass prinzipiell gemäß Art. 9 Abs. 2 lit. h) i.V.m. Abs. 3 DSGVO lediglich Fachpersonal und – auch ausweislich des § 352 SGB V – keine Krankenkasse auf die ePA-Gesundheitsdaten zugreifen darf. Allerdings ist in diesem Kontext Art. 5 Abs. 1 lit. d) 2. Halbsatz DSGVO relevant, der keine eigenhändige Kontrolle und/oder Korrektur verlangt, sondern lediglich vorgibt, dass „alle angemessenen Maßnahmen zu treffen“ sind. Es dürfte daher genügen, wenn die Krankenkassen 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 der jeweils aktuellste Befund sich in der ePA befindet und einsehbar ist. Mit Blick auf die sachlich-inhaltliche Richtigkeit dürfen die Krankenkassen freilich auch auf die Kompetenz des Fachpersonals vertrauen, das zum Zugriff auf die Informationen berechtigt ist (vgl. Art. 9 Abs. 3 DSGVO).

4.2.2.5 Integrität und Vertraulichkeit

Schließlich können sich aus dem in Art. 5 Abs. 1 lit. f) DSGVO verankerten **Grundsatz der Integrität und Vertraulichkeit** Vorgaben für die Gestaltung der Zugriffsberechtigungen ergeben. Damit den Vorgaben dieses Grundsatzes Rechnung getragen wird, müssen neben einer adäquaten technisch-organisatorischen Gesamtarchitektur des jeweiligen Systems – wie bereits unter Punkt »3.2.2.5 dargelegt – wiederum adäquate Instrumente zur **Identifikation** und **Authentifizierung**[112] der eingebundenen Akteure etabliert werden. Es gilt daher sicherzustellen, dass zum einen sämtliche Akteure (z.B. Leistungserbringer) absolut zweifelsfrei identifiziert werden[113] und zum anderen nur jene einen Zugriff auf die ePA haben, die hierzu eine Berechtigung haben und in der Regel an der Gesundheitsbehandlung der betroffenen Person beteiligt sind.[114] Zudem muss gewährleistet werden, dass unbefugte Personen (z.B. in der Arztpraxis) auch keinen Zugang „zu den Geräten haben, mit denen [die Gesundheitsdaten der betroffenen Personen] verarbeitet werden.“[115] Überdies hat – wie bereits in Punkt »3. dargelegt – eine **Protokollierung** darüber stattzufinden, wann welcher Akteur auf welche Daten und in welcher Weise auf die Gesundheitsdaten in der ePA Zugriff genommen hat.[116]

Im Hinblick auf die wesentlichen denkbaren Gestaltungsoptionen bedarf insbesondere die **automatische Zugriffsberechtigung**, bei der keine gesonderte Freischaltung hinsichtlich der Leseberechtigung durch den Patienten erfolgt, einer näheren Betrachtung. Aus datenschutzrechtlicher Perspektive könnte man daran zweifeln, ob der damit verbundene Verzicht auf eine „Vorabkontrolle“ der Zugriffsberechtigten durch den Betroffenen mit

112 Siehe die begriffliche Unterscheidung bereits oben unter Punkt »3.1.1

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

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

115 Siehe *P. Schantz*, in: H. A. Wolff/S. Brink (Hrsg.), BeckOK Datenschutzrecht, Stand 1.11.2021, Art. 5 DSGVO Rn. 36.

116 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).

den in Art. 9 Abs. 2 lit. h) i.V.m. Abs. 3 DSGVO geforderten „Bedingungen und Garantien“ und Art. 5 Abs. 1 lit. f) DSGVO vereinbar ist. Richtigerweise wird man ein zwingendes gesondertes Freischaltungserfordernis allerdings auch nicht aus dem Grundsatz der Vertraulichkeit und Integrität ableiten können. Zum einen ist bereits höchst fraglich, ob eine eigenverantwortliche Vorabkontrolle durch den Patienten selbst überhaupt geeignet ist, um die Vertraulichkeit und Integrität der Verarbeitungen zu erhöhen. Zum anderen existieren unseres Erachtens hinreichende und effektivere objektive Sicherungsinstrumente, um Missbrauchsrisiken zu vermeiden und somit einen „Schutz vor unbefugter oder unrechtmäßiger Verarbeitung“ im Kontext der Zugriffsberechtigungen zu gewährleisten.

Solange lediglich registrierte bzw. authentifizierte zugriffsberechtigte Akteure einen Zugriff auf die ePA erhalten und überdies ein hinreichender Kontakt zu dem betreffenden Patienten besteht – insbesondere in Form einer physischen Anwesenheit oder zumindest eines nachweisbaren virtuellen Kontakts –, dürfte der Vertraulichkeit und Integrität der Verarbeitungen hinreichend Rechnung getragen sein. Umgekehrt würde eine gesonderte Freischaltung in praxi vielmehr dazu führen, dass Patientinnen und Patienten, abhängig von der Hürde des Freischaltungserfordernisses[117], unbesehen zahlreiche Leistungserbringer – womöglich „auf Vorrat“ – freischalten; das Freischaltungserfordernis würde damit gleichsam leerlaufen und zur bloßen Förmelei. Alternativ könnte die Einführung eines gesonderten Freischaltungserfordernisses, wie bereits dargelegt, auch dazu führen, dass etwa nicht technikaffine Personen oder jene, die die Zeit hierfür nicht aufbringen möchten, schlichtweg keine Freischaltung erteilen und die Effektivität der ePA-Nutzung insgesamt in Frage gestellt würde.

Als dem Datenschutzgrundsatz der Integrität und Vertraulichkeit zuträglich erweisen sich überdies starre bzw. flexible **Gruppenzugriffsberechtigungen**, da sie aufgrund der auf Basis von Typisierungen vorgegebenen technischen 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. Mit Rücksicht auf die primäre Zwecksetzung der ePA, eine möglichst hochwertige und informierte Gesundheitsversorgung zu gewährleisten, dürfte dabei jeweils eine **dispositive** Beschränkung vorzugswürdig sein, da dies in atypischen Fällen eine gegebenenfalls erforderliche sachliche Erweiterung bzw. zeitliche Verlängerung der Zugriffsberechtigungen gestattet.

4.2.3 Ergänzende grundrechtliche Vorgaben

Neben den Datenschutzgrundsätzen können im Rahmen der Interpretation dessen, was geeignete „Bedingungen und Garantien“ der Verarbeitung der personenbezogenen Daten gemäß Art. 9 Abs. 2 lit. h) i.V.m. Abs. 3 DSGVO sind, auch von den Grundrechten der Grundrechtecharta und des Grundgesetzes, namentlich vom **Recht auf informationelle Selbstbestimmung**, Grenzen und Impulse für die Ausgestaltung der Zugriffsberechtigungen ausgehen. Dabei sind an dieser Stelle weniger die Grenzen relevant – diese gehen typischerweise bereits in den Datenschutzgrundsätzen auf –, sondern vielmehr – umgekehrt – die für eine effektive Nutzung der ePA streitenden **ermöglichenden Impulse** (siehe dazu bereits eingehend Punkt »3.2.3).

117 Siehe dazu bereits unter Punkt »4.1.1.2.

Da die Etablierung einer weitgehend vollständigen gesundheitsinformationellen Basis (und deren Nutzung) auch den einzelnen Patienten in die Lage versetzt, in Ausübung seiner Patientensouveränität eine möglichst informierte, selbstbestimmte Entscheidung über den weiteren Umgang mit der eigenen Gesundheit zu treffen, sprechen die positiv verstandenen Patientenrechte unseres Erachtens für ein Modell der **automatischen Zugriffsberechtigung** ohne gesondertes Freischaltungserfordernis. Gleiches dürfte mit Blick auf eine **dispositive** Gestaltung von etwaigenfalls vorgesehenen gesetzlichen Beschränkungen gelten, die mit **Gruppenzugriffsberechtigungen** und zeitlichen Einschränkungen der **Zugriffsdauer** einhergehen. Auch insofern dürfte das Selbstbestimmungsrecht der Patientinnen und Patienten im Zweifel für eine Gestaltung sprechen, die ihnen eine Abweichung von den gesetzlichen (datenschutzfreundlichen) Voreinstellungen ermöglichen.

4.2.4 Sonstige Vorgaben

4.2.4.1 Informationspflichten (Art. 12 ff. DSGVO)

Nach den übrigen allgemeinen datenschutzrechtlichen Regeln treffen den Verantwortlichen in Bezug auf sämtliche Gestaltungen der Zugriffsberechtigungen gewisse Informationspflichten, sodass die betroffenen Personen in ausreichend verständlicher und präziser Weise über die möglichen Zugriffe auf ihre Gesundheitsdaten informiert werden. Sofern der Gesetzgeber – in rechtmäßiger und sinnvoller Weise – **automatische Zugriffsberechtigungen** vorsieht, bei denen kein Freischaltungserfordernis besteht, gibt es zweifelsohne einen erhöhten Informationsbedarf seitens der Patienten. Diese sollten im Rahmen einer solchen Gestaltung vorab in „verständlicher, klarer und einfacher Sprache“ umfassend über die Modi der möglichen Verarbeitungsarten im Rahmen der Zugriffsberechtigungen informiert werden.

4.2.4.2 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Dass den datenschutzfreundlichen Voreinstellungen gemäß Art. 25. Abs. 2 DSGVO eine erhebliche Bedeutung im Rahmen der Gestaltung der Zugriffsberechtigungen zukommt, insbesondere im Kontext der **Gruppenzugriffsberechtigungen** und **zeitlichen Beschränkungen**, wurde bereits unter Punkt »4.2.2.3 aufgezeigt. Insofern wird an dieser Stelle auf obige Ausführungen verwiesen.

4.2.4.3 Datensicherheit (Art. 32 DSGVO)

Aus Art. 32 DSGVO ergeben sich ferner konkrete Vorgaben für die „Sicherheit der Verarbeitung“. Dabei gilt es zumal zur Gewährleistung der Vertraulichkeit der Systeme und Dienste sicherzustellen, dass nur jene Personen auf die Gesundheitsdaten in der ePA zugreifen können, die eine entsprechende Berechtigung haben. Damit geht einher, dass ein geringeres Risiko eines Zugriffs von Unberechtigten auf Daten in der ePA besteht.[118] Als besonders zielführend erscheinen dabei wiederum entsprechende Zugriffskontrollsysteme im Kontext der **Gruppenzugriffsberechtigungen** und **zeitlichen Beschränkungen**,

118 *S. Jandt*, in: J. Kühling/B. Buchner (Hrsg.), DS-GVO BDSG, 3. Aufl. 2020, Art. 32 Rn. 23.

da diese zumindest typisierend darauf abzielen, dass nur „materiell“ zugriffsberechtigte Personen auf die für sie vorgesehenen Datenfelder und für die erforderliche Dauer eine „förmliche“ Berechtigung zum Zugriff haben.

4.2.4.4 Widerspruchsrechte (Art. 21 DSGVO)

Schließlich ist zu berücksichtigen, dass – wie bereits unter Punkt »3.2.4.3 dargelegt wurde – gerade im Rahmen von Opt-out-Gestaltungen effektive Widerspruchsrechte der Betroffenen vorgesehen werden müssen. Dies betrifft auch und vor allem den **Entzug** von Zugriffsberechtigungen und dessen konkrete Ausgestaltung. Das Widerspruchsrecht dient unmittelbar dem Recht auf informationelle Selbstbestimmung; seine Ausübung muss für die betroffenen Personen niedrigschwellig und unbürokratisch möglich sein.[119] Die Betroffenen müssen außerdem ausdrücklich auf diese Möglichkeit hingewiesen werden (vgl. Art. 21 Abs. 4 DSGVO). Je mehr Opt-out-Elemente für die ePA vorgesehen sind (d.h. je eher die Verarbeitungen „automatisch“ erfolgen, ohne gesonderte Zustimmung oder Einwilligung), desto höher sind die Anforderungen an eine effektive Widerspruchsmöglichkeit. Besonderes Augenmerk dürfte insofern auf den hier präferierten **automatischen Zugriffsberechtigungen** liegen.

Bedeutsam für die datenschutzrechtliche Bewertung sämtlicher Typen von Zugriffsberechtigungen erscheint vor allem die Gestaltung der **Modalitäten** des Entzugs der Zugriffsberechtigung durch den Patienten. Die Hoch- bzw. Niedrigschwelligkeit der Entzugsmöglichkeit dürfte sich freilich nicht pauschal für sämtliche Patientinnen und Patienten bestimmen lassen. So wird für technikaffine Personen der Entzug via ePA-App die denkbar einfachste Möglichkeit darstellen – und der (physische) Weg zum Leistungserbringer, zur Ombudsstelle o.Ä. eher eine Beschwerlichkeit. Für technisch weniger versierte Personen könnte dagegen der analoge Zugang zu Entziehungsmöglichkeiten den einfachsten Weg bilden. Entscheidend erscheint daher, dass der Gesetzgeber für den Entzug eine **multimodale** Gestaltungsoption wählt, also 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 unkompliziert zur Verfügung steht.

4.3 Zusammenfassung

In Bezug auf die Frage, wer neben dem Patienten im Allgemeinen und im Konkreten Zugriff auf die ePA haben soll, steht der Gesetzgeber im Wesentlichen vor **vier Gestaltungsentscheidungen**. Zum einen hat er 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 vor der Frage, welchen **sachlichen Umfang** die Zugriffsberechtigungen haben sollten. So könnte er insbesondere umfassende Zugriffsberechtigungen oder typisiert beschränkte,

119 Siehe bereits oben unter Punkt »3.2.4.3.

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 über eine etwaige (wiederum starr oder flexibel festsetzbare) Beschränkung der **Dauer** der Zugriffsberechtigungen entscheiden und überdies die Modalitäten des **Entzugs** der Zugriffsberechtigungen regeln.

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, also 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** 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 beschriebenen Gestaltungsoptionen muss der Gesetzgeber somit spezifische Bedingungen und Garantien vorsehen, die dem jeweiligen Charakter der gewählten Option bezüglich der Zugriffsberechtigung hinreichend Rechnung tragen. 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** konnte zunächst herausgearbeitet werden, dass diese Grundsätze deutlich für die Einführung von **Gruppenzugriffsberechtigungen** sprechen. Durch diese kann entsprechend dem Verarbeitungszweck in typisierender Weise eine Eingrenzung der Zugriffsberechtigungen vorgenommen und prinzipiell nur jenen Personen eine technische Berechtigung zum Zugriff gewährt werden, die diesen regelmäßig auch materiell-rechtlich zusteht, weil sie die betreffenden Informationen typischerweise etwa für konkrete Behandlungs- bzw. Versorgungszwecke benötigen. Bei umfassend ausgestalteten Zugriffsberechtigungen wären demgegenüber keine standardmäßig beschränkten Zugriffsberechtigungen vorgesehen – auch nicht für Akteure, die typischerweise keinen umfassenden Zugriff benötigen. Das Recht auf informationelle Selbstbestimmung im positiven Sinne dürfte dabei für eine flexible, also **dispositive** gesetzliche Voreinstellung der Gruppenzugriffsberechtigungen sprechen, die von den betroffenen Personen selbstbestimmt abgeändert, d.h. erweitert oder auch eingeschränkt 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 ebenfalls prozedurale Vorkehrungen getroffen werden, um die Zweckmäßigkeit und Erforderlichkeit der Zugriffe zu gewährleisten. Welche konkreten Gesundheitsdaten im Rahmen des aktuellen Behandlungs- bzw. Versorgungskonnexes beispielsweise für den Abruf erforderlich sind, dürften vor allem Angehörige des **Fachpersonals** treffen können.

Der Grundsatz der **Richtigkeit** der Verarbeitungen gemäß Art. 5 Abs. 1 lit. d) DSGVO ist ebenfalls für sämtliche Gestaltungsoptionen relevant. Er verlangt zwar keine eigenhändige Kontrolle und/oder Korrektur von ePA-Informationen, gibt den verantwortlichen Krankenkassen 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 der jeweils aktuellste Befund sich in der ePA befindet und einsehbar ist. Mit Blick auf die sachlich-inhaltliche Richtigkeit dürfen die Krankenkassen freilich auch auf die Kompetenz des Fachpersonals vertrauen, das zum Zugriff auf die Informationen berechtigt ist.

Der Grundsatz der **Vertraulichkeit und Integrität** entfaltet Vorgaben zum einen für die Einrichtung **automatischer Zugriffsberechtigungen**, steht diesen aber 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 – 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 technischen 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 Gestaltungsoptionen – also die **Gruppenzugriffsberechtigungen** sowie die **zeitliche Beschränkung** der Zugriffsmöglichkeiten – sollte mit Rücksicht auf das **Selbstbestimmungsrecht** der Patientinnen und Patienten eine **dispositive**, also flexible gesetzliche Voreinstellung vorgesehen werden. Eine zwingende, starre Vorgabe würde über das Ziel hinausschießen.

Von den übrigen datenschutzrechtlichen Regelungen erscheint vor allem das Erfordernis einer **Widerspruchsmöglichkeit** 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, also 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 unkompliziert zur Verfügung steht.

5 Einzelne abrufbare Inhalte der ePA

Während das vorherige Kapitel über die Berechtigung zum Zugriff auf die ePA insbesondere die Frage behandelt, wer in persönlicher Hinsicht auf die ePA zugreifen dürfen und können soll, sind die nachstehenden Ausführungen 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 haben, dass einzelne Daten(-sätze) – im negativen Sinne – gelöscht werden bzw. gar nicht oder nur teilweise für die anderen Zugriffsberechtigten einsehbar sind. Im Folgenden werden insofern zunächst wiederum die wesentlichen denkbaren Gestaltungsoptionen (»5.1) aufgezeigt und anschließend wird eine datenschutzrechtliche Bewertung (»5.2) vorgenommen.

5.1 Wesentliche denkbare Gestaltungsoptionen

Bei der Regelung der Steuerungsmöglichkeiten der Patienten bezüglich der abrufbaren Inhalte in ihrer ePA hat der Gesetzgeber zunächst zu bestimmen, wie der **technische Zugang** der Patientinnen und Patienten zur Steuerung der Inhalte ausgestaltet sein soll (»5.1.1). In weiterer Folge bedarf es der näheren Erörterung, in welchem **Umfang** die betroffenen Personen die in die ePA eingespeisten Inhalte steuern können sollen; hierbei kann prinzipiell zwischen feingranularen einerseits sowie mittelgranularen Steuerungsmöglichkeiten andererseits unterschieden werden (»5.1.2). Ferner bedürfen die **Modalitäten der Entfernung** von Inhalten durch die betroffenen Personen einer näheren Betrachtung (»5.1.3). Des Weiteren stellt sich in diesem Zusammenhang die Frage, ob lediglich den betroffenen Personen selbst diese **Steuerungsberechtigung** über die einzelnen abrufbaren Inhalte zukommen soll, oder ob ebenso andere Zugriffsberechtigte diese innehaben sollten (»5.1.4). Abschließend wird auf mögliche Gestaltungselemente zur **informationellen Unterstützung** der Patientinnen und Patienten bei der Steuerung der ePA-Inhalte eingegangen, insbesondere auf Hinweise und Kontrollfunktionen für die betroffenen Personen (»5.1.5).

5.1.1 Technischer Zugang der Patienten zur Steuerung der Inhalte

Als mögliche technische Zugangswege der Patienten zur ePA kommen, wie bereits unter Punkt »4. angedeutet, insbesondere der Zugang über ein eigenes Endgerät bzw. eine

Website in Betracht (»5.1.1.1), ferner ein Zugang vor Ort beim Leistungserbringer (»5.1.1.2) sowie – etwa in den Räumlichkeiten der Ombudsstellen, der Krankenkassen etc. – über Serviceterminals (»5.1.1.3). Dabei ist erneut zu reflektieren, dass sich die Hoch- bzw. Niedrigschwelligkeit hinsichtlich der Zugangswege zur Steuerung der (einzelnen) Inhalte durch die betroffenen Personen nicht pauschal für sämtliche Patienten bestimmen lässt. Denn während der potenzielle Zugangsweg über ein Endgerät bzw. eine Website für technikaffine Personen voraussichtlich den denkbar einfachsten darstellt, könnte sich dieser für weniger technisch versierte Personen (z.B. Personen höheren Alters) eher als eine Beschwerlichkeit erweisen. Für letztere könnte dagegen ein analoger Zugangsweg den einfachsten bilden, etwa der (physische) Weg zum Leistungserbringer. Es kann daher an dieser Stelle nochmals herausgestellt werden, dass der deutsche Gesetzgeber im Kontext der Zugangsmodalitäten für die Patientinnen und Patienten vor allem eine **multimodale Gestaltungsoption** in Betracht ziehen sollte.

5.1.1.1 Eigene Endgeräte und webbasierte Lösungen

Sowohl über ein eigenes Endgerät (z.B. ein Mobiltelefon oder ein Tablet mit entsprechender ePA-App) als auch über eine Website könnte für die betroffenen Personen die Möglichkeit eingerichtet werden, die einzelnen Inhalte in ihrer ePA zu steuern.[120] Ohne große Hürden sowie prinzipiell in Echtzeit könnten die Betroffenen auf diese Weise kurzerhand (einzelne) Daten aus ihrer ePA entfernen. Für die Authentifizierung der betroffenen Personen müsste dabei ein geeignetes technisches Verfahren etabliert werden, das einen entsprechend hohen Sicherheitsstandard gewährleistet.[121] Perspektivisch dürfte sich dafür die gemäß § 291 Abs. 8 SGB V „[s]pätestens ab dem 1. Januar 2023“ durch die Krankenkassen zur Verfügung zu stellende „digitale Identität für das Gesundheitswesen“ als Sicherungsmechanismus anbieten.

Fallbeispiel: Damit Anna Umstellungen in ihrer ePA vornehmen kann – etwa die Entfernung der Informationen zu dem Blutbild, das in B erstellt wurde –, benötigt sie einen technischen Zugang zur Steuerung der Inhalte. In Betracht kämen beispielsweise ihr Smartphone mit entsprechender ePA-App bzw. eine speziell eingerichtete ePA-Website. Da Anna eine gewisse technische Affinität aufweist, könnte sie niedrigschwellig auf ihre ePA zugreifen.

5.1.1.2 Leistungserbringer

Ferner könnten die betroffenen Personen auch bei einem Leistungserbringer vor Ort die Inhalte ihrer ePA steuern. Für diesen Zugangsweg müsste der Gesetzgeber ebenfalls einen hohen Sicherheitsstandard hinsichtlich der Authentizität gewährleisten, etwa durch Einführen der eGK in ein Lesegerät und Eingabe einer PIN bzw. eines Passworts. Zudem könnte perspektivisch auch insoweit die „digitale Identität für das Gesundheitswesen“ im Sinne des § 291 Abs. 8 SGB V verwendet werden.

120 Besitzer eines geeigneten Endgeräts werden auch als „Frontend-Nutzer“ bzw. Nutzer ohne geeignete Endgeräte als „Nicht-Frontend-Nutzer“ bezeichnet. Vgl. diesbezüglich bereits *C. Krönke/V. Aichstill,* in: Stiftung Münch (Hrsg.), Die elektronische Patientenakte und das europäische Datenschutzrecht, 2021, S. 24.

121 Vgl. etwa im gegenwärtigen Opt-in-Modell § 336 Abs. 2 Nr. 2 SGB V.

Fallbeispiel: Annas Großvater ist nicht gleichermaßen technisch versiert wie Anna selbst. Wenn er – wie er dies regelmäßig tut – alte ePA-Daten löschen möchte, sucht er meist seinen langjährigen Hausarzt in B auf und nimmt die Löschungen vor Ort vor.

5.1.1.3 Serviceterminals

Zudem bestünde für den Gesetzgeber die Möglichkeit, vorzusehen, dass den Patientinnen und Patienten über Serviceterminals[122] ein Zugang zur Steuerung der ePA-Inhalte eröffnet wird. Diese Terminals könnten entweder bei Leistungserbringern vor Ort oder in den Räumlichkeiten der Krankenkassen platziert werden. Auch hier wäre ein entsprechend effektiver Authentifizierungsmechanismus vorzusehen.

Fallbeispiel: Gelegentlich löscht Annas Großvater seine alten ePA-Daten auch über das Serviceterminal in der Außenstelle seiner Krankenkasse.

5.1.2 Granularität der Steuerung der Inhalte

Des Weiteren müsste der Gesetzgeber darüber entscheiden, ob die betroffenen Personen im Kontext der Einführung der ePA als Opt-out-Modell die einzelnen Inhalte auf ihrer ePA feingranular (»5.1.2.1) oder lediglich mittel- bis grobgranular (»5.1.2.2) steuern können sollen.

5.1.2.1 Feingranulare Steuerung

Im Rahmen einer feingranularen Steuerung könnten die betroffenen Personen unter anderem **spezifische** Dokumente sowie Datensätze[123] steuern, insbesondere löschen oder ausblenden (im Folgenden auch: **dokumentenscharfe** Steuerung). Zudem könnte eine Spielart der feingranularen Steuerungsmöglichkeit eingeführt werden, die es den Betroffenen ermöglicht, zusätzlich zu dieser dokumentenscharfen Steuerung von einzelnen Dokumenten und Datensätzen auch eine Steuerung bestimmter Dokumenten- bzw. Datensatzgruppen (im Folgenden: **gruppenspezifische** Steuerung) vorzunehmen. Mithin bestünde für die Patienten etwa die Möglichkeit, dass sie eine Gruppe von Dokumenten anhand einer inhaltlichen Qualifizierung (z.B. Entlassbriefe, OP-Berichte oder Medikationsangaben) oder anhand bestimmter Erstellungs- oder Änderungsdaten auswählen und löschen bzw. (für alle oder bestimmte Zugriffsberechtigte) ausblenden.[124] Eine solche

122 Im Rahmen des gegenwärtigen Opt-in-Modells war die Errichtung von Serviceterminals („eKiosk“) ebenso geplant, allerdings als möglicher Weg zur Erteilung der Einwilligung. Erwähnenswert erscheint, dass die Idee der Serviceterminals jedoch aus Kostengründen verworfen wurde. Siehe diesbezüglich *C. Dochow*, MedR 2021, 13 (19).

123 Miteinander verknüpfte Daten werden im Folgenden als Datensätze bezeichnet.

124 Vgl. zu näheren Informationen hinsichtlich möglicher Gruppen von Dokumenten oder Datensätzen die Erwägungen des Gesetzgebers in BT-Drs. 19/8793, S. 115.

gruppenspezifische Steuerung könnte die Handhabung der ePA-Daten bequemer und damit zugleich niedrigschwelliger gestalten.

Fallbeispiel: Mittels der Steuerungsmöglichkeiten in ihrer ePA-App kann Anna einerseits „dokumentenscharf" einen einzelnen Befund (z. B. das Blutbild aus B) ausblenden. Andererseits könnte sie auch gruppenspezifisch sämtliche Daten zu Blutuntersuchungen aus der ePA gesammelt entfernen.

5.1.2.2 Mittel- bis grobgranulare Steuerung

Während Patienten im Rahmen der feingranularen Steuerung auch die kleinsten Datenobjekte ansteuern könnten, würde ihnen im Rahmen einer mittel- bis grobgranularen Steuerung – je nach konkreter Ausgestaltung – hingegen **nur** eine **gruppenspezifische** Ansteuerung von Dokumenten sowie Datensätzen ermöglicht. Mit Blick auf die sinnvollerweise fixierbaren Gruppen von Dokumenten bzw. Datensätzen käme beispielsweise eine Zusammenfassung anhand der Dokumentart (Befunde, Diagnosen etc.) oder anhand der Sensibilität der Informationen (d.h. sensible bzw. nicht sensible Daten) in Betracht.

Fallbeispiel: Im Rahmen einer nur mittel- bis grobgranularen Steuerung könnte Anna nicht „dokumentenscharf" auch einzelne Befunde (z. B. das Blutbild aus B) entfernen. Sie könnte lediglich gruppenspezifisch eine bestimmte Gruppe von Dokumenten oder Datensätzen ausblenden – etwa alle Daten zu Blutuntersuchungen oder alle Diagnosen.

5.1.3 Modalitäten der Entfernung von Inhalten

Gestaltungsbedürftig sind für jedes ePA-System überdies und vor allem auch die Modalitäten der Entfernung von Inhalten. Datenschutzrechtliche Relevanz haben sie insbesondere wegen des bereits angesprochenen, im Rahmen eines Opt-out-Modells zwingenden Erfordernisses einer Widerspruchsmöglichkeit für die betroffenen Personen. Im Vorgriff auf die datenschutzrechtliche Bewertung lässt sich dabei zumindest im Groben festhalten, dass die rechtlichen Anforderungen an eine effektive Widerspruchsmöglichkeit umso höher sein dürften, je mehr die Verarbeitungen von ePA-Daten „automatisch" erfolgen, also ohne gesonderte Zustimmung oder Einwilligung der Patienten. Mit Blick auf die Modalitäten der Entfernung von Inhalten stehen dem deutschen Gesetzgeber im Wesentlichen die folgenden beiden Gestaltungsoptionen offen: Zum einen könnte er eine Löschung (»5.1.3.1) und/oder zum anderen lediglich eine Ausblendung (»5.1.3.2) von Inhalten in der ePA für die betroffenen Personen vorsehen.

5.1.3.1 Löschung

Sofern der deutsche Gesetzgeber eine Löschung von ePA-Daten durch die Patientinnen und Patienten gestattet, stünde den betroffenen Personen die Entscheidung offen, ihre (einzelnen) ePA-Daten **gänzlich** zu löschen. Die betreffenden Informationen wären somit

unwiederbringlich aus der ePA entfernt und müssten gegebenenfalls neu eingepflegt werden.

Fallbeispiel: Wenn Anna die Informationen aus B zu ihrem Blutbild löscht, werden diese Daten vollständig aus ihrer ePA entfernt. Wenn ihr Hausarzt in A später darauf zugreifen wollte, könnte auch Anna selbst ihm keinen Zugriff mehr darauf verschaffen. Die Informationen müssten dann gegebenenfalls aus dem Krankenhaus in B beschafft werden, sofern sie dort überhaupt noch vorhanden sind.

5.1.3.2 Ausblendung

Alternativ oder daneben könnte der Gesetzgeber überdies die Möglichkeit vorsehen, dass der Patient ePA-Daten lediglich ausblenden kann. Hierbei könnte in weiterer Folge differenziert werden zwischen einer **völligen** Ausblendung für (andere) Zugriffsberechtigte (»5.1.3.2.1) einerseits und einer **beschränkten** Einsehbarkeit ausgeblendeter Daten für (andere) Zugriffsberechtigte (»5.1.3.2.2) andererseits.

5.1.3.2.1 Völlige Ausblendung für andere Zugriffsberechtigte

Infolge einer völligen Ausblendung der ePA-Daten wären diese für andere Zugriffsberechtigte **gänzlich verborgen**, wenn auch nicht vollständig gelöscht. Der Patient selbst hätte weiterhin die Möglichkeit, in die für andere Zugriffsberechtigte ausgeblendeten ePA-Daten Einsicht zu nehmen und diese gegebenenfalls auch wieder sichtbar zu machen.

Fallbeispiel: Wenn Annas Befunde aus B vollständig ausgeblendet sind, sieht ihr Hausarzt in A nicht, dass sie überhaupt jemals in B behandelt wurde. Auch im Notfall hätte er keinen Zugriff auf die in B generierten Befunde.

5.1.3.2.2 Beschränkte Einsehbarkeit von ausgeblendeten Daten für andere Zugriffsberechtigte

Während im Falle einer völligen Ausblendung für andere Zugriffsberechtigte lediglich die betroffenen Personen Einsicht in ihre ePA-Daten nehmen können, bestünde für den Gesetzgeber des Weiteren die Möglichkeit, eine beschränkte Einsehbarkeit von ausblendeten Daten für andere Zugriffsberechtigte vorzusehen. Denkbare Ausgestaltungsmodi hierfür wären zum einen „Verschattungen“ (»5.1.3.2.2.1) sowie zum anderen ein „Notfallmodus“ (»5.1.3.2.2.2).

5.1.3.2.2.1 Verschattungen

Die Ausblendung von ePA-Daten könnte eine Verschattung zur Folge haben, d.h. für andere Zugriffsberechtigte wäre zwar sichtbar, *dass* ein bestimmtes Dokument oder ein bestimmter Datensatz oder mehrere bestimmte Dokumente oder Datensätze in der ePA abgelegt sind, nicht dagegen dessen bzw. deren *Inhalte*. Auf diese Weise hätten Zugriffs-

berechtigte zwar keinen Zugriff auf die betreffenden Vollinformationen, wohl aber könnten sie auf bestimmte, vom Gesetzgeber gegebenenfalls näher festzulegende **Metadaten** (Behandlungsort, Datum etc.) zugreifen. So könnte beispielsweise ein behandelnder Arzt in Ansehung nicht näher bezeichneter ePA-Daten seinen Patienten im Rahmen der Behandlung auf die „verschatteten" Informationen ansprechen und ihn auf die mögliche Relevanz etwaiger „Datenlücken" ansprechen. Der Patient könnte dann im Einzelfall entscheiden, ob er die Information offenlegen möchte.

Fallbeispiel: Wenn die Befunde aus B lediglich verschattet sind, könnte Annas Hausarzt in A zumindest sehen, *dass* bestimmte Informationen in Annas ePA vorhanden sind, auf deren *Inhalte* er aber keinen Zugriff hat. Im Gespräch mit Anna könnte der Arzt erfragen, um welche Art von Informationen es sich handelt, und sie aufklären, welche Informationen für ihre laufende Behandlung von Relevanz sein könnten.

5.1.3.2.2.2 „Notfallmodus"

Zusätzlich oder alternativ könnte der Gesetzgeber auch einen „Notfallmodus" einführen, der es bestimmten anderen Zugriffsberechtigten im Notfall (z.B. Bewusstlosigkeit des Patienten infolge eines schweren Verkehrsunfalls) ermöglichen würde, ausnahmsweise auch ausgeblendete ePA-Daten einzusehen. Der Zugriff im „Notfallmodus" könnte dabei mit einer zwingenden **Begründungs- und Protokollierungsfunktion** einhergehen, um sicherzustellen, dass der Zugriff im „Notfallmodus" lediglich die Ausnahme zur Regel darstellt und nachträglich auch effektiv überprüfbar ist.

Fallbeispiel: Wenn Annas Befunde aus B ausgeblendet sind, könnte beispielsweise eine nach einer erneuten Schwindelattacke herbeigerufene Ärztin ausnahmsweise auf die Befunde zugreifen und bestimmte Ursachen für die Attacke von vornherein ausschließen.

5.1.4 Steuerungsberechtigung

Aus gesetzgeberischer Sicht gestaltungsbedürftig ist außerdem die Steuerungsberechtigung, also die Frage, wer die Berechtigung zur Steuerung der (einzelnen) ePA-Inhalte innehaben soll. Hierbei wäre für den deutschen Gesetzgeber denkbar, dass entweder den Patientinnen und Patienten bzw. ihren Vertretern die **exklusive** Steuerungsberechtigung (»5.1.4.1) zukommt oder zusätzlich auch bestimmte andere Zugriffsberechtigte eine Berechtigung zur Steuerung von Inhalten (»5.1.4.2) besitzen.

5.1.4.1 Exklusive Steuerungsberechtigung der Patienten bzw. ihrer Vertreter

Im Falle einer exklusiven Berechtigung der betroffenen Personen zur Steuerung der (einzelnen) ePA-Daten hätten sie die **alleinige Berechtigung**, (einzelne) ePA-Daten zu steuern, d.h. insbesondere zu entfernen – sei es durch Löschung oder durch Ausblendung.

5.1.4.2 Steuerungsberechtigung auch anderer Zugriffsberechtigter

Alternativ könnte der deutsche Gesetzgeber ebenso in Erwägung ziehen, dass neben den Patienten auch bestimmte andere Zugriffsberechtigte gewisse ePA-Daten steuern können. So könnte beispielsweise Ärztinnen und Ärzten die Möglichkeit eingeräumt werden, einzelne von ihnen selbst in die ePA eingebrachte Daten bzw. Datensätze zu **ändern**, zu **löschen** oder **auszublenden**. Auf diese Weise könnten Änderungen, Löschungen sowie Ausblendungen ohne nähere Kenntnis der Patienten vorgenommen werden und bestünden für den/die betreffenden Leistungserbringer unter Umständen mehr Einsichtsmöglichkeiten in die ePA-Daten als für die betroffene Person selbst.[125]

Fallbeispiel: Hätte auch Annas Hausarzt eine Berechtigung zur Steuerung der ePA jenseits seiner regulären Schreib- und Leseberechtigung, könnte er beispielsweise seine Diagnose bezüglich Annas Angststörung im Rahmen einer späteren Behandlung revidieren und gänzlich löschen, sodass diese Information nicht mehr in Annas ePA vorhanden wäre.

5.1.5 Informationelle Unterstützung der Patienten: Hinweise und Kontrollfunktionen

Zudem könnte der Gesetzgeber Funktionen vorgeben, um den Patienten im Zusammenhang mit der Ausübung seiner Steuerungsberechtigung informationell zu unterstützen. Vor allem beim Umgang mit einzelnen Inhalten könnten **Hinweispflichten** sinnvoll sein (»5.1.5.1). Zudem könnte sich eine in der ePA eingerichtete **„Preview-Funktion“** (»5.1.5.2) als adäquate Kontrolle für die betroffenen Personen erweisen.

5.1.5.1 Hinweise bei der Ansteuerung einzelner Inhalte

Speziell im Kontext von **besonders weitreichenden Steuerungsentscheidungen**, wie etwa bei der vollständigen Löschung von ePA-Daten, kommt der informationellen Unterstützung der betroffenen Personen eine wesentliche Bedeutung zu. Die Zielvorstellung hierbei ist, dass den Betroffenen die Auswirkungen der beabsichtigten Ansteuerung vor Augen geführt werden. Durch die Einführung einer gesetzlich vorgesehenen **Warnhinweispflicht im Einzelfall** könnte den betroffenen Personen ein gewisser „Übereilungsschutz“ geboten werden.

Fallbeispiel: Wenn Anna sich selbst dazu entschließt, die Diagnose der Angststörung aus ihrer ePA zu löschen, erscheint beim Click auf das „Löschen“-Feld ein Pop-up-Fenster mit einem Text, in dem Anna vor der endgültigen Löschung gewarnt und auf die Möglichkeit hingewiesen wird, die betreffende Information „nur“ auszublenden.

125 Lediglich im Rahmen des estnischen Opt-out-Modells der ePA besteht die Möglichkeit, dass Gesundheitsdienstanbieter 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. die rechtsvergleichende Studie im Auftrag der Stiftung Münch von *C. Krönke/V. Aichstill*, in: Stiftung Münch (Hrsg.), Die elektronische Patientenakte und das europäische Datenschutzrecht, 2021, S. 113.

5.1.5.2 „Preview-Funktion“

Zudem könnte der Gesetzgeber vorgeben, dass die ePA über eine „Preview-Funktion“ verfügen muss. Dabei handelt es sich um eine Funktion, die dem Patienten im Rahmen einer „Vorschau“ anzeigt, was ein bestimmter anderer Zugriffsberechtigter (z.B. ein Arzt) konkret sehen würde, wenn er Einsicht in die ePA nehmen würde. Es würde sich dabei um eine effektive **Kontrollfunktion** für die betroffenen Personen handeln, um festzustellen, ob die vorgenommenen Steuerungen im Ergebnis dem entsprechen, was die Betroffenen sich vorgestellt hatten.

Fallbeispiel: Anna könnte eine Preview-Funktion nutzen, um sich anzusehen, wie ihrem Hausarzt in A die Informationen präsentiert werden, die in ihrer ePA vorhanden sind. Auf diese Weise könnte sie überprüfen, ob die von ihr gewählten Einstellungen zu dem gewünschten Resultat geführt haben – beispielsweise, ob der Hausarzt in A das ausgeblendete Blutbild aus B tatsächlich nicht mehr einsehen kann.

5.2 Datenschutzrechtliche Bewertung

5.2.1 Effektive Einsichtnahme- und Steuerungsmöglichkeiten

Für die Beurteilung der Optionen bezüglich der Steuerung der ePA-Inhalte durch die Patienten erscheinen vor allem zwei datenschutzrechtliche Maßgaben relevant. Zum einen müssen die Patientinnen und Patienten über die Möglichkeit verfügen, in einem **negativen** Sinne in differenzierter Weise einzelne Inhalte der ePA entweder gänzlich zu löschen oder für die anderen Zugriffsberechtigten auszublenden. Normative Grundlage der damit verbundenen Maxime, den Patienten **effektive Möglichkeiten** hinsichtlich der Einsichtnahme sowie zur Steuerung der (einzelnen) Inhalte an die Hand zu geben, sind nicht nur die Datenschutzgrundsätze – allen voran der **Transparenz** (Art. 5 Abs. 1 lit. a) DSGVO) –, sondern ebenso die Grundrechte, namentlich das **Recht auf informationelle Selbstbestimmung**. Auf ebendiese Belange verweisen die für die Verarbeitung von ePA-Daten im Rahmen eines Opt-out-Systems heranzuziehenden datenschutzrechtlichen Verarbeitungsgrundlagen in Art. 9 Abs. 2 lit. h) und i) sowie Abs. 3 DSGVO, wenn sie vorgeben, dass das mitgliedstaatliche Recht „Bedingungen und Garantien“ sowie „angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person“ vorsehen muss.

Als gegenläufige Belange, die eine Einschränkung jener „Effektivitätsmaxime“ rechtfertigen können, kommen vor allem die mit der Einführung der ePA als Opt-out-Modell zu Versorgungszwecken beabsichtigten Verbesserungen hinsichtlich der Qualität und Effizienz in der sektoren-, fach- sowie einrichtungsübergreifenden Gesundheitsversorgung in Betracht. Dabei muss der Gesetzgeber, wie bereits in Punkt »5.1 eingangs kurz festgehalten, die Möglichkeiten zur Einsichtnahme und Steuerung der ePA-Inhalte **umso effektiver** ausgestalten, **je mehr Opt-out-Elemente** er für die ePA-Nutzung im Übrigen vorgesehen hat, also je mehr Verarbeitungen „automatisch“ erfolgen dürfen, ohne gesonderte Zustimmung oder Einwilligung der Patienten. Jedes gesetzliche Opt-out-System gleicht mit Blick auf die einschlägigen datenschutzrechtlichen Vorgaben mithin einem „beweglichen System“.

Zum anderen müssen die Patientinnen und Patienten freilich – umgekehrt – auch über effektive Steuerungsmöglichkeiten verfügen, die es ihnen ermöglichen festzulegen, dass bestimmte Informationen für bestimmte Zugriffsberechtigte in einem **positiven** Sinne überhaupt einsehbar sind. Dies dürfte unabhängig von der in Art. 9 Abs. 4 DSGVO vorgesehenen Befugnis der Mitgliedstaaten gelten, gegenüber den in Art. 9 Abs. 2 lit. h) und i) sowie Abs. 3 DSGVO ohnehin schon vorgegebenen Einschränkungen, „zusätzliche Bedingungen, einschließlich Beschränkungen, ein[zu]führen oder aufrecht[zu]erhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist". Denn beim Gebrauchmachen von jener Befugnis wäre der deutsche Gesetzgeber gleichwohl an die **grundrechtlichen** Vorgaben des Grundgesetzes gebunden. Dazu zählt nicht nur das Recht, *vor* Datenverarbeitungen geschützt zu werden, sondern auch, wie mehrfach dargelegt, das aus der informationellen Selbstbestimmung ebenfalls fließende Recht *auf* eine bestimmte Datenverarbeitung, zumal im Kontext der ihrerseits grundrechtsrelevanten Gesundheitsversorgung.

5.2.2 Effektivität der einzelnen Gestaltungsoptionen

Es gilt daher im Folgenden zu erörtern, ob die einzelnen Gestaltungsoptionen hinsichtlich der Zugangsmodalitäten (»5.2.2.1), der Granularität (»5.2.2.2), der Entfernungsmodalitäten (»5.2.2.3) sowie der Hinweis- und Kontrollfunktionen (»5.2.2.4) als jeweils „angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person" im Sinne des Art. 9 Abs. 2 DSGVO einer „effektiven" Möglichkeit zur Einsichtnahme bzw. zur Steuerung der Inhalte durch die Patienten entsprechen.

5.2.2.1 Zugangsmodalitäten

Als mögliche Zugriffskanäle für die Steuerung der (einzelnen) Inhalte durch die betroffenen Personen bestünden – wie oben dargelegt – für den deutschen Gesetzgeber das Endgerät (Mobiltelefon, Tablet etc.) bzw. eine Website, ferner technische Einrichtungen direkt vor Ort beim Leistungserbringer sowie Serviceterminals insbesondere in Räumlichkeiten der Krankenkassen. Um den durchschnittlichen betroffenen Personen einen niedrigschwelligen Zugangsweg zu ermöglichen, damit sie von ihren Steuerungsberechtigungen überhaupt erst Gebrauch machen können, scheint als eine effektive Modalität und mithin als „angemessene und spezifische Maßnahme[n] zur Wahrung der Rechte und Freiheiten der betroffenen Person" **jedenfalls** der Zugangsweg über das **Endgerät** bzw. eine **Website** zwingend einzufordern zu sein. Dass das Endgerät bzw. eine Website als Zugangsweg jedenfalls vorzusehen sind, unterstreicht vor allem die hohe Anzahl der Smartphone-Nutzer – laut einer Erhebung[126] benutzten in Deutschland im Jahr 2021 rund 62 Millionen Personen ein Smartphone. Die Betroffenen könnten überall und jederzeit ihre ePA-Inhalte steuern und, im Lichte des Datenschutzgrundsatzes der Transparenz (Art. 5 Abs. 1 lit. a) DSGVO), ohne Weiteres nachvollziehen, wer wann auf welche Daten zugegriffen hat bzw. zugreifen könnte.

126 Die Erhebung fand durch VuMA, Bitkom Research und comScore statt und wurde im Jahr 2021 veröffentlicht, online verfügbar unter https://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/.

Dennoch gilt zu beachten, dass die ePA nicht nur ein Instrument für die durchschnittliche betroffene Person darstellt, sondern ein Instrument für alle Personen. Mithin sollte unseres Erachtens – wie bereits unter Punkt »4. im Zusammenhang mit der Entziehung der Zugriffsberechtigungen dargelegt – neben dem elektronischen Zugangsweg über ein Endgerät bzw. eine Website **zusätzlich** auch einer der beiden anderen, **„analogen" Zugangswege** eröffnet werden, d.h. ein Zugang auch direkt vor Ort beim Leistungserbringer und/oder über Serviceterminals ermöglicht werden. Vor allem für jene Personen höheren Alters und/oder mit geringer technischer Affinität sind diese zusätzlichen Zugangswege relevant. Für den Zugangsweg direkt vor Ort beim Leistungserbringer könnte dabei vor allem sprechen, dass – anders als bei einem Serviceterminal – regelmäßig eine fachkundige persönliche Unterstützung seitens des Leistungserbringers möglich wäre. Insgesamt dürfte es dem Gesetzgeber gleichwohl offenstehen, für welchen der beiden zusätzlichen Zugangswege er sich entscheidet, um den betroffenen Personen eine effektive Möglichkeit zur Einsichtnahme und in weiterer Folge zur Steuerung der einzelnen Inhalte zu geben.

5.2.2.2 Granularität der Steuerung der Inhalte

Darüber hinaus stellt sich die Frage, ob als „angemessene und spezifische Maßnahme[n] zur Wahrung der Rechte und Freiheiten" den betroffenen Personen zwingend eine feingranulare Steuerungsmöglichkeit zustehen muss. Vor allem in Ansehung des Datenschutzgrundsatzes der Transparenz (Art. 5 Abs. 1 lit. a) DSGVO) sowie des Rechts auf informationelle Selbstbestimmung (im negativen Sinne) scheint für die betroffenen Personen eine feingranulare Steuerungsmöglichkeit im Rahmen eines Opt-out-Modells der ePA allerdings unverzichtbar. Denn sofern eine automatische, einwilligungsunabhängige Anlage und Befüllung auf der ersten Stufe des Opt-out eingeführt wird, müssen den Betroffenen gleichsam als Ausgleich des damit verbundenen „Übergehens" einer *ex ante* selbstbestimmten Befüllung möglichst **weitreichende Steuerungsmöglichkeiten** *ex post* zustehen. Generell ist nämlich davon auszugehen, dass die Anforderungen an eine effektive Widerspruchsmöglichkeit umso höher sein dürften, je mehr Opt-out-Elemente für die ePA vorgesehen sind, also je mehr Verarbeitungen „automatisch" erfolgen, ohne gesonderte Zustimmung oder Einwilligung der Patienten.

Sofern der Patient nur gruppenspezifisch Dokumente und Datensätze mittel- oder grobgranular steuern kann, besteht die Gefahr, dass ihm eine „Alles oder nichts"-Entscheidung aufgenötigt wird und er entweder mehr entfernt, als ihm eigentlich lieb ist, oder umgekehrt sämtliche Zugriffe gestattet, obwohl er einzelne Dokumente oder Datensätze an sich lieber verborgen halten würde. Im Rahmen von solchen mittel- oder grobgranularen Steuerungsmöglichkeiten würden die Patienten daher unter Druck gesetzt werden, im Zweifel von ihrer Steuerungsmöglichkeit in die eine oder andere Richtung Abstand zu nehmen. Dies würde nicht zu einer selbstbestimmten Entscheidung über die Verarbeitung ihrer Gesundheitsdaten führen, wie sie das Recht auf informationelle Selbstbestimmung an sich einfordert.

Der Gesetzgeber hat daher für die betroffenen Personen zwingend eine feingranulare Steuerungsmöglichkeit einzuführen. Dabei sollte er diese feingranularen Steuerungsmöglichkeiten unseres Erachtens auch auf **sämtlichen Zugriffswegen** implementieren. Ob es mit zwingenden datenschutzrechtlichen Vorgaben vereinbar ist, dass eine feingranulare Steuerungsmöglichkeit den betroffenen Personen etwa – wie derzeit unter dem geltenden Opt-in-System in Deutschland – nur auf ihrem Endgerät zusteht, nicht dagegen bei einer Steuerung über die Systeme eines Leistungserbringers, scheint uns jedenfalls bei einer

Gestaltung der ePA als Opt-out-System durchaus zweifelhaft zu sein.[127] Der Gesetzgeber sollte daher im Zweifelsfall auf allen Zugriffswegen für feingranulare Steuerungsmöglichkeiten sorgen.

5.2.2.3 Entfernungsmodalitäten

Mit Blick auf die Modalitäten der Entfernung von ePA-Inhalten durch die Patientinnen und Patienten muss einerseits entschieden werden, ob der deutsche Gesetzgeber die Löschung oder nur eine Ausblendung für die Patienten gestatten darf bzw. muss (»5.2.2.3.1). Andererseits ist zu prüfen, ob der Gesetzgeber daran gehindert wäre, eine „Verschattung" und/oder einen „Notfallmodus" (»5.2.2.3.2) zu implementieren.

5.2.2.3.1 Löschung oder nur Ausblendung?

Für die Gestaltungsoption (auch) der **Löschung** spricht aus kurzfristiger Sicht zunächst das Recht auf informationelle Selbstbestimmung im negativen Sinne. Somit könnten die betroffenen Personen über ihren Zugangsweg, d.h. jedenfalls über ihr Endgerät/Website, nahezu in Echtzeit einzelne Inhalte vollständig und ohne verbleibende „Datenspuren" aus ihrer ePA löschen und mithin punktuell aus der ePA „hinausoptieren". Dieses Ergebnis dürfte auch prinzipiell dem Anliegen des **Löschungsrechts** gemäß Art. 17 Abs. 1 DSGVO entsprechen, das den Patienten im Falle eines Widerspruchs[128] gegen die Datenverarbeitungen grundsätzlich zusteht.

Indes steht das Löschungsrecht aus Art. 17 Abs. 1 lit. c) DSGVO ersichtlich unter dem **Vorbehalt**, dass „keine vorrangigen berechtigten Gründe für die Verarbeitung" vorliegen.[129] In diesem Sinne streitet das Recht auf informationelle Selbstbestimmung im positiven Sinne aus langfristiger Sicht und im Lichte der Versorgungszwecke für die Gewährleistung einer möglichst lückenlosen gesundheitsinformationellen Basis auf der ePA, die durch vollständige Datenlöschungen durchaus substanziell in Frage gestellt werden kann. Vor diesem Hintergrund erscheint es uns datenschutzrechtlich zumindest vertretbar, eine vollständige Löschung einzelner ePA-Daten nicht zu ermöglichen. Damit würde sich der Gesetzgeber auch nicht in Widerspruch zur Möglichkeit eines „Gesamt-Opt-outs" stellen, denn aus der Perspektive der Gesundheitsversorgung erscheint eine für einen Leistungs-

127 Vgl. zur Frage der Datenschutzkonformität des derzeit in Deutschland vorgesehenen Konzepts 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 Bundestages. 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.

128 Wie bereits in Punkt »4. eingehend dargelegt: Sollte sich der Gesetzgeber für die Einführung eines Opt-out-Modells bezüglich der Befüllung der ePA entscheiden, trifft ihn in der Konsequenz die Pflicht, ein Widerspruchsrecht für die betroffenen Personen vorzusehen. Obzwar ein solches Widerspruchsrecht in Art. 21 DSGVO explizit nur bei bestimmten Verarbeitungen zwingend vorgesehen ist, wird man bei Opt-out-Systemen, die Gesundheitsinformationen auf der Basis eines gesetzlichen Verarbeitungstatbestands nach Art. 9 Abs. 2 lit. g), h) und/oder i) DSGVO verarbeiten, nichtsdestotrotz als zwingende „angemessene und spezifische Maßnahme[n] zur Wahrung der Grundrechte und Interessen der betroffenen Person" jedenfalls eine im Grundsatz unbedingte Widerspruchsmöglichkeit einfordern müssen, die nur ausnahmsweise bei gegebenen zwingenden schutzwürdigen Gründen i.S.v. Art. 21 Abs. 1 DSGVO überwunden werden kann (z. B. in Notfällen).

129 *C. Worms*, in: H. A. Wolff/S. Brink (Hrsg.), BeckOK Datenschutzrecht, Stand 1.11.2021, Art. 17 DSGVO Rn. 37.

erbringer (z.B. den Arzt) unerkannt lückenhafte ePA deutlich gefährlicher als eine vollständig gelöschte ePA. Während der behandelnde Arzt im letzteren Fall weiß, dass er sich lediglich auf die ihm konventionell vorliegenden Informationen (Befunde, Diagnosen etc.) verlassen darf, könnte er im erstgenannten Fall irrigerweise davon ausgehen, dass die ePA vollständig ist – obwohl möglicherweise essenzielle Informationen gelöscht wurden.

Diese Überlegungen gebieten es, dass der Gesetzgeber in Bezug auf die Löschung von ePA-Daten zumindest einen gewissen **Übereilungsschutz** gewährleistet. Ob dieser Schutz im Ausschluss einer punktuellen Löschung von ePA-Daten besteht oder über entsprechende Warnhinweise erfolgt (siehe dazu unten Punkt »5.2.2.4), liegt im freien Ermessen des Gesetzgebers.

5.2.2.3.2 „Verschattung“ oder „Notfallmodus“

Sieht der Gesetzgeber anstelle oder zusätzlich zu der Löschung von Gesundheitsdaten die Möglichkeit der Ausblendung von ePA-Daten vor, stellt sich zudem die Frage, ob er dabei eine völlige Ausblendung vorsehen müsste oder den anderen Zugriffsberechtigten eingeschränkte Einsichtnahmemöglichkeiten gewähren dürfte, in Gestalt von Verschattungen bzw. eines „Notfallmodus“. Anders als bei der völligen Ausblendung, also der gänzlichen Verborgenheit der Gesundheitsdaten für die anderen Zugriffsberechtigten, würden im Kontext der Verschattung die anderen Zugriffsberechtigten zwar nicht die dahinterstehende „Vollinformation“ einsehen können, jedoch bestimmte Metadaten der Gesundheitsinformationen. Wie bereits dargelegt, geht der „Notfallmodus“ noch einen Schritt weiter, da er (bestimmten) Zugriffsberechtigten im Notfall die Einsicht in die ePA ermöglichen würde, wenn auch technisch begleitet durch effektive Begründungs- und Protokollierungsfunktionen.

Aus datenschutzrechtlicher Sicht stellt die Offenlegung sowohl von Verschattungsdaten als auch von Vollinformationen im „Notfallmodus“ jeweils eine reguläre Datenverarbeitung dar, die auf eine Verarbeitungsgrundlage gestützt werden und sich an den Datenschutzgrundsätzen messen lassen muss. Mit Blick auf das „Ob“ der Verarbeitung dürften die Verschattung und der „Notfallmodus“ durch **Art. 9 Abs. 2 lit. h) i.V.m. Abs. 3 DSGVO** legitimierbar sein. Aufgrund einer Verschattung erhalten Leistungserbringer zwar keinen Einblick in die dahinterstehende „Vollinformation“ der ePA-Daten; allerdings könnten sie im Interesse einer lückenlosen Gesundheitsversorgung der Patienten durch Nachfrage zumindest eine Vorstellung von der Art der dahinterstehenden Vollinformationen erhalten und die Versorgung des Patienten entsprechend darauf einstellen. Auch der „Notfallmodus“ würde im Sinne des Art. 9 Abs. 2 lit. h) DSGVO dafür sorgen, dass bestimmten Zugriffsberechtigten (z.B. einem Notarzt) versorgungsrelevante Informationen offengelegt würden.

Mit Blick auf die Verarbeitungsmodalitäten nach Maßgabe der Datenschutzgrundsätze und -grundrechte – also für das „Wie“ der Verarbeitung – dürfte das Recht auf informationelle Selbstbestimmung sowie das aus Art. 2 Abs. 2 Satz 1 GG folgende Recht auf „gesundheitliche Selbstbestimmung“ grundsätzlich für die Möglichkeit der **Verschattung** sprechen. Dadurch würde der Patient überhaupt erst in die Lage versetzt, auf Nachfrage eines Leistungserbringers (z.B. seines Arztes) über die Versorgungsrelevanz ausgeblendeter Informationen zu reflektieren und sich unter dem Eindruck ärztlicher Beratung gegebenenfalls zur Offenlegung der Informationen im Interesse einer angemessenen Versorgung zu entscheiden. Zweifelsfrei würde dies der Idee einer fach-, sektoren- und ein-

richtungsübergreifenden Gesundheitsversorgung entsprechen und mithin im Interesse der effektiven Nutzung der ePA zu Versorgungszwecken liegen. Allerdings ist der mit der Offenlegung bestimmter Metadaten gegenüber bestimmten Zugriffsberechtigten ein gegenüber der Übermittlung der Vollinformationen ungleich weniger intensiver Eingriff in die informationelle Selbstbestimmung der Patienten, der vom Gesetzgeber in Anbetracht der beschriebenen gegenläufigen Belange prinzipiell zurückgestellt werden dürfte.

Auch die Einführung eines **„Notfallmodus“** erscheint angesichts der datenschutzrechtlichen Vorgaben für das „Wie“ der Verarbeitung zulässig. Sofern der Gesetzgeber hinreichende technische und organisatorische Vorkehrungen (d.h. effektive Begründungs- und Protokollierungsfunktionen) trifft, mit denen sichergestellt wird, dass die in möglichst genau zu bestimmenden, hinreichend gewichtigen Notfällen befugten Zugriffsberechtigten tatsächlich nur im erforderlichen Maße auf ePA-Informationen zugreifen – siehe dazu den Grundsatz der Datenminimierung, Art. 5 Abs. 1 lit. c) DSGVO, sowie den Grundsatz der Vertraulichkeit und Integrität, Art. 5 Abs. 1 lit. f) DSGVO –, dürfte das gewichtige Interesse an einer angemessenen Versorgung des betreffenden Patienten im Notfall die Achtung der Patientenentscheidung bezüglich der Ausblendung bestimmter ePA-Informationen ausnahmsweise überwiegen.

Aus alledem folgt, dass der deutsche Gesetzgeber bei der Einführung der ePA als Opt-out-Modell zu Versorgungszwecken letztlich nicht daran gehindert ist, als „angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person“ sowohl die Verschattung ausgeblendeter Informationen als auch den „Notfallmodus“ zu implementieren.

5.2.2.4 Hinweis- und Kontrollfunktionen

Darüber hinaus bedürfen etwaige Hinweis- sowie Kontrollfunktionen im Rahmen der Steuerungsmöglichkeiten durch die betroffenen Personen einer näheren datenschutzrechtlichen Betrachtung. Fraglich erscheint insofern, ob der Gesetzgeber „als angemessene und spezifische Maßnahme[n] zur Wahrung der Rechte und Freiheiten der betroffenen Person“ zwingend eine solche informationelle Unterstützung für die Patienten vorzusehen hat.

Vor allem im Kontext von **weitreichenden Steuerungsentscheidungen**, die dazu führen können, dass für gesundheitsbezogene Entscheidungen der Patienten in der Zukunft keine hinreichende informationelle Basis besteht, ist der Gesetzgeber verpflichtet, **Warnhinweispflichten** vorzusehen. Dies betrifft insbesondere die vollständige **Löschung** punktueller ePA-Daten. Solche Warnhinweispflichten erscheinen als Übereilungsschutz verfassungsrechtlich nicht nur gerechtfertigt, sondern auch geboten, als Form einer „sanft paternalistischen“ Einwirkung auf die prinzipiell selbstbestimmte Entscheidung des Patienten über den Verbleib der eigenen Gesundheitsdaten. Der Patient könnte sich ohne Weiteres über diese Einwirkung hinwegsetzen, auf seinem Endgerät beispielsweise durch einen einfachen Klick auf ein „Ignorieren“ des Warnhinweises. Auch wenn die betroffenen Personen gleichwohl in ihren Steuerungsmöglichkeiten geringfügig eingeschränkt werden, scheint im Rahmen einer wertenden Betrachtung mit Blick auf die Belange der Versorgungszwecke der langfristige Schutz der persönlichkeits- und gesundheitsbezogenen Selbstbestimmungsrechte der Patientinnen und Patienten dadurch ungemein und zwingend gesteigert zu werden.

Anders als die Warnhinweispflicht erweist sich die angedachte **„Preview-Funktion“** als eine für die betroffenen Personen lediglich **optionale Unterstützungsfunktion**, die keinen zwingenden verfassungs- oder datenschutzrechtlichen Vorgaben entspricht. Dem deutschen Gesetzgeber steht es damit prinzipiell offen, ob er zusätzlich zu punktuellen Warnhinweispflichten bei weitreichenden Steuerungsentscheidungen (v.a. bei der Löschung) eine allgemeine Preview-Funktion einführen möchte.

5.2.3 Steuerungsberechtigung anderer Zugriffsberechtigter

Es bleibt aus datenschutzrechtlicher Sicht zu prüfen, ob der Gesetzgeber lediglich den betroffenen Personen eine Steuerungsberechtigung zuordnen darf oder ob ebenso auch andere Zugriffsberechtigte (z.B. Ärzte in Bezug auf von ihnen eingespielte Informationen) über Steuerungsmöglichkeiten verfügen dürfen. Sowohl die Änderung als auch die Löschung von Gesundheitsinformationen auf der ePA stellt eine eigenständige, **rechtfertigungsbedürftige Datenverarbeitung** dar. Mithin gilt erneut zwischen den Vorgaben in Bezug auf das „Ob“ und solchen für das „Wie“ der Datenverarbeitung zu differenzieren.

Sowohl die Änderung als auch die Löschung von Gesundheitsdaten dürfte im Wesentlichen einer Befüllung gleichkommen – man denke vor allem an die Korrektur oder Entfernung einer unrichtigen Vermutungsdiagnose durch den behandelnden Arzt. Eine Löschung zum Schutz der informationellen Selbstbestimmung der betroffenen Patienten, wie sie insbesondere Art. 17 DSGVO im Blick hat, werden zugriffsberechtigte Leistungserbringer von sich aus kaum vornehmen wollen. Vor diesem Hintergrund bestünde für den deutschen Gesetzgeber hinsichtlich des **„Ob“** wiederum die Wahl zwischen den Ausnahmetatbeständen des Art. 9 Abs. 2 lit. h) i.V.m. Abs. 3 oder lit. i) DSGVO. Gerade im Falle der Korrektur unrichtiger Diagnosen oder Verschreibungen wird man dahinter durchaus den Zweck erkennen können, Fehler bei der künftigen Versorgung des betreffenden Patienten infolge einer unrichtigen Datengrundlage vermeiden zu wollen.

Vor allem im Lichte des Rechts auf informationelle Selbstbestimmung sowie der Datenschutzgrundsätze der Transparenz (Art. 5 Abs. 1 lit. a) DSGVO) und der Integrität (Art. 5 Abs. 1 lit. f) DSGVO) erscheint es allerdings problematisch, wenn andere Zugriffsberechtigte zumal Löschungen und/oder Änderungen und/oder Ausblendungen von Gesundheitsdaten auf der ePA vornehmen können. So erscheint es unter dem Gesichtspunkt der **Integrität** der Gesundheitsdatenbestände des Patienten selbstverständlich, dass in erster Linie er selbst darüber entscheidet, ob bestimmte Daten aus der ePA entfernt werden, und dass prinzipiell ein Recht auf Konservierung des Datenbestandes besteht. Bei gänzlichen Löschungen oder Ausblendungen wäre für die betroffenen Personen zudem nicht mehr nachvollziehbar, welche Gesundheitsdaten tatsächlich einmal in ihrer ePA vorhanden waren und ob ihre ePA noch eine weitgehend vollständige gesundheitsinformationelle Basis bietet.

Als gegenüber der vollständigen Löschung oder Ausblendung milderes Mittel zur Vermeidung von Fehlern bei der künftigen Versorgung des betreffenden Patienten infolge unrichtiger Datengrundlage 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 – ohne allerdings die „historischen“ Daten vollständig zu entfernen. Dieser Gestaltungsoption dürfte mit Blick auf den **Erforderlichkeitsgrundsatz** (siehe auch Art. 9 Abs. 2 lit. h) und i) DSGVO: „die

Verarbeitung ist […] erforderlich“) gegenüber einem Löschungs- oder Ausblendungsrecht für Dritte zwingend der Vorzug zu geben sein, wenn der Gesetzgeber dem Interesse an einer materiell richtigen Datengrundlage in besonderer Weise Rechnung tragen möchte.

5.3 Zusammenfassung

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 Patientinnen und 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 „angemessene[n] und spezifische[n] Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person“ verlangen. Dabei sind auch die Datenschutzgrundsätze, allen voran das Transparenzgebot (Art. 5 Abs. 1 lit. a) DSGVO), sowie das Recht auf informationelle Selbstbestimmung maßstäblich.

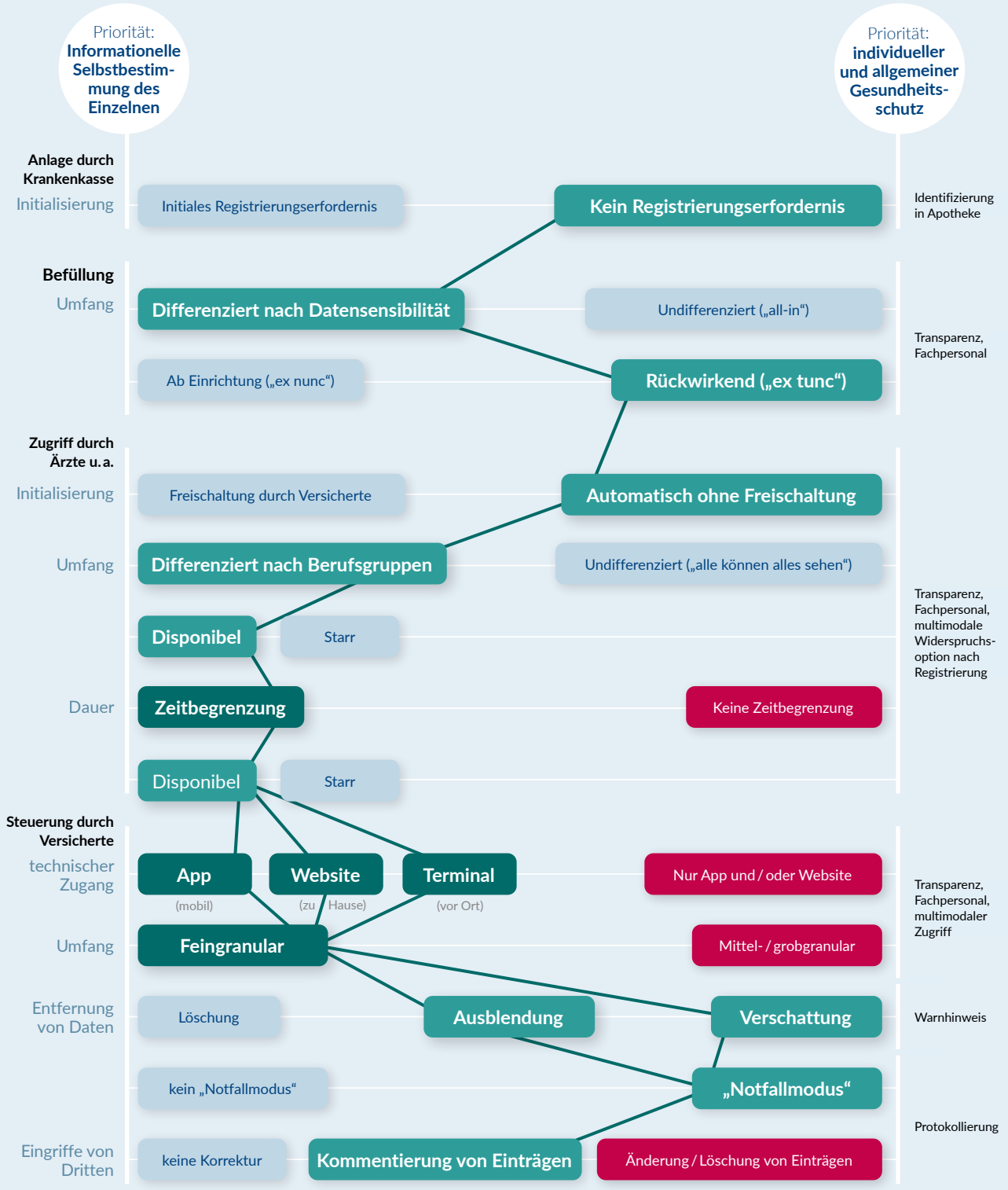
Bei der Regelung der Steuerungsmöglichkeiten der Patienten bezüglich der abrufbaren Inhalte in ihrer ePA hat der Gesetzgeber im Wesentlichen **fünf Gestaltungsentscheidungen** zu treffen. Er hat zunächst den **technischen Zugang** der Patientinnen und Patienten zur Steuerung der Inhalte auszugestalten. Außerdem muss er den **Umfang** der Steuerungsmöglichkeiten festlegen (mit feingranularen oder mittel- bis grobgranularen Steuerungsmöglichkeiten). Ferner hat er die **Modalitäten der Entfernung** von Inhalten vorzugeben (mit der Möglichkeit zur Löschung und/oder der vollständigen oder beschränkten Ausblendung der entfernten Daten). Er könnte sich überdies entschließen, nicht nur den Patienten selbst, sondern auch anderen Zugriffsberechtigten eine **Steuerungsberechtigung** zuzuordnen. Und schließlich hat der Gesetzgeber über Gestaltungselemente zur **informationellen Unterstützung** der Patienten bei der Steuerung der ePA-Inhalte nachzudenken, insbesondere über Hinweise und Kontrollfunktionen für die betroffenen Personen.

Um den durchschnittlichen Betroffenen einen niedrigschwelligen **Zugangsweg** zu ermöglichen, scheint als „angemessene und spezifische Maßnahme[n] zur Wahrung der Rechte und Freiheiten der betroffenen Person“ jedenfalls der Zugangsweg über das **Endgerät** bzw. eine **Website** zwingend einzufordern zu sein. Daneben sollte der Gesetzgeber **zusätzlich** einen **„analogen“ Zugangsweg** eröffnen, also 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 er im Rahmen einer insgesamt als Opt-out-Modell ausgestalteten ePA die feingranularen Steuerungsmöglichkeiten auf **sämtlichen Zugriffswegen** implementieren.

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 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 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

Abwägungsprozess für ePA-Opt-out



Abwägungsgründe: ■ zwingend ■ empfohlen ■ optional ■ ausgeschlossen

Quelle: Bertelsmann Stiftung 2022, eigene Darstellung

STIFTUNG MÜNCH | BertelsmannStiftung

Interessen der Patienten hat er aber auch die Möglichkeit, eine Verschattung ausgeblendeter Informationen sowie einen „Notfallmodus“ für bestimmte Zugriffsberechtigte einzuführen.

Im Kontext von **weitreichenden Steuerungsentscheidungen**, die dazu führen können, dass für gesundheitsbezogene Entscheidungen der Patientinnen und Patienten in der Zukunft keine hinreichende informationelle Basis besteht, ist der Gesetzgeber verpflichtet, **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 zum Zwecke der Vermeidung von Fehlern bei der künftigen Versorgung des betreffenden Patienten infolge einer unrichtigen Datengrundlage ist datenschutzrechtlich unzulässig. 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.

Impressum

Herausgeber:
Bertelsmann Stiftung
Carl-Bertelsmann-Str. 256
33311 Gütersloh
www.bertelsmann-stiftung.de

Verantwortlich:
Uwe Schwenk
Director des Programms Gesundheit

Lektorat: Heike Herrberg, Bielefeld

Gestaltung: Dietlind Ehlers

Bildnachweis
© tadamichi – stock.adobe.com

Adresse | Kontakt

Bertelsmann Stiftung
Carl-Bertelsmann-Straße 256
33311 Gütersloh
Telefon +49 5241 81-0

Dr. Stefan Etgeton
Senior Expert
Programm Gesundheit
Telefon +49 30 275788-316
stefan.etgeton@bertelsmann-stiftung.de

www.bertelsmann-stiftung.de

BertelsmannStiftung