Die elektronische Patientenakte (ePA) im europäischen Datenschutzrechtsvergleich

Kritik der deutschen ePA-Konzeption im Lichte der Patientenaktensysteme Österreichs, Estlands und Spaniens

Von *Christoph Krönke**

Mit der 2021 eingeführten elektronischen Patientenakte (ePA) soll die Gesundheitsversorgung in Deutschland in das digitale Zeitalter überführt werden, unter Beachtung aller datenschutzrechtlichen Vorgaben zur Wahrung größtmöglicher „Patientensouveränität". Im Vergleich mit ausgewählten Patientenaktensystemen anderer europäischer Staaten zeigt sich allerdings, dass der deutsche Gesetzgeber substanzielle datenschutzrechtliche Gestaltungsspielräume ungenutzt gelassen hat – und mithin auch wesentliche Vorteile aus der Hand gegeben hat, die mit der ePA für eine qualitativ hochwertige und allgemein verfügbare Gesundheitsversorgung hätten einhergehen können.

I. Die ePA – „Kernelement" digital unterstützter Gesundheitsversorgung in Deutschland oder „Computerspielerei"?

Seit dem 1. Juli 2021 ist es soweit: Den Ärzten und anderen Leistungserbringern in Deutschland sollte es nun möglich sein, auf Gesundheitsdaten in elektronischen Patientenakten (ePA) zuzugreifen, die den 73 Millionen gesetzlich[1] Versicherten hierzulande von Gesetzes wegen seit Anfang 2021 zur Verfügung gestellt werden müssen (§ 342 Abs. 1 SGB V). Der Gesetzgeber hatte die ePA in der Begründung zu dem Patientendaten-Schutz-Gesetz (PDSG) vom 14. Oktober 2020,[2] mit der die Regelungen über die ePA in das SGB V eingeführt wurden, nachgerade euphorisch als das „Kernelement" der digital unterstützten medizinischen und pflegeri-

* Der Beitrag wurde in dieser Form auch in der Neuen Zeitschrift für Sozialrecht (NZS), Heft 24/2021, S. 949–957 veröffentlicht und gibt wesentliche rechtliche Erkenntnisse einer Studie wieder, die der Verfasser gemeinsam mit Vanessa Aichstill, LL.M. (WU) für die Stiftung Münch angefertigt hat. Die genannte Studie wurde unter dem Titel „Die elektronische Patientenakte und das europäische Datenschutzrecht" selbständig im Verlag medhochzwei veröffentlicht. Alle zitierten URLs wurden zuletzt am 30. September 2022 abgerufen.

[1] Für die privaten Krankenversicherungen besteht keine entsprechende Verpflichtung. Sie bleiben im Folgenden daher ausgeblendet.

[2] Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur vom 14. Oktober 2020, BGBl. I 2020, S. 2115 ff.

schen Versorgung angekündigt.[3] Ob der Gesetzgeber bei der Ausgestaltung der ePA allerdings tatsächlich aus dem Vollen geschöpft hat, wird aus gesundheitswissenschaftlichen Fachkreisen bezweifelt. In seinem Gutachten „Digitalisierung für Gesundheit" aus 2021 gelangt etwa der Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen zu der eher ernüchternden Einschätzung, dass die „Chancen, die eine ePA den Versicherten bietet", unter den vom Gesetzgeber unter dem Eindruck datenschutzrechtlicher Vorgaben geschaffenen Bedingungen „wesentlich schwieriger zu realisieren" seien, und auch aus der Perspektive der Leistungserbringer blieben „einige wichtige Chancen der ePA ungenutzt".[4] Insbesondere würden „unnötige Doppeluntersuchungen, Doppelvorhaltungen von Informationen sowie vielfältige Fehlermöglichkeiten an Schnittstellen […] nicht minimiert" – mithin also wesentliche Vorzüge aus der Hand gegeben, die eine ePA mit sich bringen könnte. Vor diesem Hintergrund überrascht es kaum, dass der erhebliche Aufwand, den die Einführung der ePA allen Beteiligten abverlangt, von wichtigen Akteuren im Gesundheitswesen als nicht lohnend empfunden wird. So hat beispielsweise die Kassenärztliche Vereinigung Baden-Württemberg in einer Formulierungshilfe die ePA als aufgezwungenes „Computerspiel" abgetan, für das den Ärzten schlichtweg die Zeit fehle.[5] In Anbetracht dieser Kritik stellt sich die Frage: Hat der deutsche Gesetzgeber hier ohne triftige Gründe wichtige Chancen vertan?

Dass ein effektives elektronisches Patientenaktensystem grundsätzlich einen überragend wichtigen Beitrag zu einer qualitativ hochwertigen und allgemein verfügbaren Gesundheitsversorgung leisten kann, dürfte außer Frage stehen. Ebenso fest steht, dass Deutschland auf diesem Feld keineswegs zu den Pionieren zählt. Dem deutschen Gesundheitswesen wurde mit Blick auf die Digitalisierung im Allgemeinen[6] und die Implementierung elektronischer Gesundheitsakten im Besonderen[7] nicht nur im internationalen, sondern auch im europäischen Vergleich regelmäßig signifikanter Nachholbedarf bescheinigt, zumal „der Diskurs über Digital Health in Deutschland stark von haftungs- und datenschutzrechtlichen Fragestellungen dominiert sei" und die „eigentlichen Chancen für die medizinische Versorgung durch die Digitalisierung" demgegenüber „eher in den Hintergrund gedrängt" würden.[8] Eindrucksvoll bestätigt wird dieser Befund durch die jüngsten Anordnungen, mit denen der Bundesbeauftragte für den Datenschutz und die Informationssicherheit,

[3] BT-Drucks. 19/18793, S. 3.

[4] Dazu und zum Folgenden *SVR*, Digitalisierung für Gesundheit, 2021, S. 86.

[5] Siehe dazu die Schnellinfo der KVBW vom 25. Juni 2021, der die Formulierungshilfe unter der Überschrift „Arztzeit oder Computerspiele" beigefügt war.

[6] Im „Digital-Health-Index", der 2018 im Rahmen der „#SmartHealthSystems"-Studie der Bertelsmann Stiftung (Hrsg.) von *Thiel et al.* erstellt wurde, lag Deutschland gar abgeschlagen auf dem vorletzten 16. Platz, siehe https://www.bertelsmann-stiftung.de/de/publikationen/publikation/did/smarthealthsystems/.

[7] *V. Amelung et al.*, Die elektronische Patientenakte – Fundament einer effektiven und effizienten Gesundheitsversorgung, 2017, S. 93 ff.

[8] *Bertelsmann-Stiftung* (Fn. 6).

Ulrich Kelber, die Krankenkassen in Bezug auf die ePA belegt hat.[9] Dass gerade das Datenschutzrecht einer effektiv ausgestalteten elektronischen Patientenakte entgegenstehen soll, erscheint freilich einigermaßen bemerkenswert, denn in Europa gilt bereits seit geraumer Zeit und spätestens seit Inkrafttreten der Datenschutzgrundverordnung (DSGVO) ein harmonisiertes Datenschutzrecht. Und ein Blick in die europäische Nachbarschaft zeigt rasch, dass auch unter Geltung der DSGVO hochwirksame Patientenaktensysteme betrieben werden können. So beweist etwa *Österreich*, dessen Rechtsordnung der deutschen traditionell sehr nahesteht, mit seiner Elektronischen Gesundheitsakte (ELGA), wie ein solches System aussehen kann. Des Weiteren hat auch *Estland*, das selbst international regelmäßig als E-Health-Spitzenreiter gehandelt wird, in sein Health Information System (HIS) ein breit angelegtes Patientenaktensystem integriert. Und auch *Spanien*, das der Bundesrepublik Deutschland größenmäßig und mit Blick auf seine föderale Struktur näherkommt als kleinere, digitalaffine Staaten, hat mit der historia clínica (HC) eine allgemeine elektronische Patientenakte implementiert.

Vor diesem Hintergrund soll im Folgenden gezeigt werden, dass im Vergleich mit den Systemen der genannten europäischen Nachbarn – dazu sogleich im Überblick unter Punkt II. – in der Tat erhebliche datenschutzrechtliche Spielräume für alternative Gestaltungen der deutschen ePA bestehen. Konkret betrifft dies vor allem die *Einrichtung* und *Befüllung* der Patientenakte (III.) sowie den *Zugriff* darauf, d. h. die *Berechtigungen* der Leistungserbringer (IV.) und die *Steuerungsmöglichkeiten* der Patienten (V.). Der deutsche Gesetzgeber sollte diese Spielräume nutzen, um die ePA progressiver auszugestalten (VI.).

II. Überblick: Die Patientenaktensysteme in Deutschland, Österreich, Estland und Spanien

Bereits im Ausgangspunkt zeigen sich erste konzeptionelle Unterschiede zwischen den Patientenaktensystemen in Deutschland, Österreich, Estland und Spanien, die auf mögliche Umgestaltungsoptionen verweisen.

1. Die deutsche ePA (§§ 341 ff. SGB V)

Der gesetzlichen Definition in § 341 Abs. 1 SGB V folgend, ist die deutsche ePA eine versichertengeführte elektronische Akte, die den Versicherten von den Kranken-

[9] Vgl. dazu BfDI, Musterbescheid zur elektronischen Patientenakte (ePA), 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. Die Krankenkassen haben angekündigt, dagegen vorzugehen, vgl. https://www.handelsblatt.com/inside/digital_health/elektronische-patientenakte-kassen-richten-sich-gegen-datenschutzbeauftragten/27602886.html?ticket=ST-112019-qnEO1H9cqycpcZ4jdSN6-ap4.

kassen[10] auf Antrag zur Verfügung gestellt wird. Dabei gestaltet sich die Nutzung freiwillig. Auf Verlangen der einzelnen Versicherten werden die nach der gesetzlichen Ausgestaltung der ePA abbildbaren medizinischen Informationen (z. B. zu Befunden, Diagnosen, Therapiemaßnahmen, Früherkennungsuntersuchungen und Behandlungsberichten) für eine einrichtungs-, fach- und sektorenübergreifende Nutzung barrierefrei elektronisch bereitgestellt, um eine effektive Gesundheitsversorgung zu ermöglichen, insbesondere eine gezielte Unterstützung von Anamnese und Befunderhebung.[11]

2. Die österreichische ELGA (§§ 13 ff. GTelG 2012)

Die österreichische ELGA ist nach der gesetzlichen Definition in § 2 Z 6 GTelG „ein Informationssystem, das allen berechtigten ELGA-Gesundheitsanbietern und ELGA-Teilnehmern ELGA-Gesundheitsdaten in elektronischer Form orts- und zeitunabhängig zur Verfügung stellt". Die Erstellung dieses sehr dezentral, auf eine Speicherung der Daten bei den Leistungserbringern angelegten Informationssystems und der Zugriff darauf beruht im Unterschied zur deutschen ePA auf einem Opt-out-Konzept. Das bedeutet, dass grundsätzlich alle Versicherten in Österreich Teilnehmer der ELGA sind und bleiben, bis sie ihren Widerspruch gegen die Teilnahme erklären. Die Abmeldequote fällt nach wie vor sehr gering aus.[12]

3. Das estnische HIS (§§ 59 ff. TTKS)

Bei dem estnischen Health Information System (HIS) handelt es sich um eine nationale zentrale Datenbank mit allen Gesundheitsdaten von Patienten, welche allen professionellen Gesundheitsdiensteanbieter in Estland zur Verfügung gestellt wird (§ 59 TTKS[13]). Das HIS ist ein – ebenfalls auf einem Opt-out-Konzept basierendes – umfassendes e-Health-System, in welchem nicht nur Gesundheitsdaten (wie z. B. Medikationsverschreibungen) verarbeitet werden, sondern auch Videokonsultationen und Ferndiagnosen (Arzt-zu-Patient und Arzt-zu-Arzt) routinemäßig ermöglicht und sämtliche Terminbuchungen und Kommunikationsvorgänge online ausgeführt

[10] Der praktisch gewiss sehr bedeutsame Bereich der Privatversicherungen soll im Folgenden der Einfachheit wegen ausgeblendet werden. An dieser Stelle mag der Hinweis genügen, dass für Privatversicherungen gemäß § 362 SGB V sämtliche datenschutzrechtlichen Vorgaben gelten, wenn von diesen eGKs für Anwendungen nach § 334 Abs. 1 S. 2 SGB V verwendet werden.

[11] Vgl. dazu die Gesetzesbegründung, BT-Drucks. 19/18793, S. 112.

[12] Vgl. etwa *OEKONSULT gmbh*, ELGA-Studie, vom Januar 2014, S. 4 ff., verfügbar unter https://www.elga.gv.at/fileadmin/user_upload/Dokumente_PDF_MP4/Infomaterialien/ELGA_2014_01_Oekonsult.pdf.

[13] Health Services Organisation Act (Tervishoiuteenuste korraldamise seadus) vom 9. Mai 2001.

werden.[14] Das System ist dabei in die vergleichsweise umfassenden E-Government-Services Estlands integriert.

4. Die spanische HC (Art. 14 ff. Ley 41/2002)

Die historia clínica ist nach gesetzlicher Definition ein Instrument zur angemessenen Unterstützung der Gesundheitsdiensteanbieter bei der Diagnose und Behandlung der Patienten, die – wie die Bezeichnung nahelegt – einen Zugang zur Krankengeschichte des Patienten ermöglicht (Art. 16 Abs. 1 Ley 41/2002). Das System ist dabei lediglich im Ausgangspunkt zentral, insbesondere durch die Formulierung von gesetzlichen Rahmenvorgaben, in der näheren Ausgestaltung dagegen weitgehend dezentral ausgestaltet. Es handelt sich – wiederum im Unterschied zur deutschen ePA – nicht um eine zentrale, patientengeführte elektronische Datei, sondern um ein System zur koordinierten Verwaltung der dezentral abgelegten Gesundheitsdaten der Patienten. Die HC basiert – wie das österreichische und das estnische System – auf einem Opt-out-Konzept.

III. Einrichtung und Befüllung der Patientenakten

Dieser Überblick deutet bereits an, dass ein erster wesentlicher Unterschied zwischen den Systemen schon in der Frage zutage tritt, ob die Patientenakten nur nach aktiver Einwilligung des Patienten oder gleichsam automatisch eingerichtet und befüllt werden. Dies hat erhebliche datenschutzrechtliche Relevanz. Die Verarbeitung personenbezogener Gesundheitsdaten ist aus datenschutzrechtlicher Sicht besonders delikat: Als Informationen „höchstpersönlicher Natur“ mit (kontextbedingt) besonders hohem Schadens- und Diskriminierungspotenzial[15] und zudem sehr ausgeprägter Identifikationskraft unterliegt ihre Verarbeitung strikteren Vorgaben als die Verarbeitung regulärer personenbezogener Daten. Bereits mit der Einrichtung und dem Befüllen der elektronischen Patientenakte greifen mit Blick auf das „Ob“ der Verarbeitung die (gegenüber Art. 6 DSGVO strengeren) Anforderungen des Art. 9 DSGVO, die nach einer qualifizierten Verarbeitungsgrundlage verlangen. Für die Modalitäten der Einrichtung und Nutzung der elektronischen Patientenakten – also das „Wie“ der Einrichtung und Befüllung – sind außerdem die grundlegenden Verarbeitungsgrundsätze in Art. 5 DSGVO maßstäblich, unter Berücksichtigung der Schwere der mit der Verarbeitung von Gesundheitsdaten[16] verbundenen Risiken für die Betroffenen.

---

[14] *R. Thiel et al.*, #SmartHealthSystems Digitalisierungsstrategien im internationalen Vergleich, 2018, S. 102.

[15] Vgl. statt vieler etwa *E. Frenzel*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG Kommentar, 3. Aufl. 2021, Art. 9 DSGVO Rn. 6 ff.

[16] Vgl. zur Bedeutung der Art der Daten für die Bestimmung des Verarbeitungsrisikos allgemein etwa *Martini* (Fn. 15), Art. 24 DSGVO Rn. 32b.

1. Deutschland: Striktes Einwilligungskonzept nach Maßgabe des Leitprinzips der „Patientensouveränität“

Die Einrichtung und die Nutzung der deutschen ePA erfolgt auf freiwilliger Basis (§ 341 Abs. 1 S. 2 SGB V). Wie bereits ausgeführt, handelt es sich bei der ePA – im Unterschied etwa zu arztgeführten Fallakten – um eine versichertengeführte elektronische Akte. Sie ist dabei unter das Banner größtmöglicher „Patientensouveränität“[17] gestellt und folgt einem strikten Opt-in-System. So findet insbesondere keine automatische Einspeisung von Informationen in die ePA statt. Die ePA basiert vielmehr von vornherein auf *Einwilligungen* in die Einrichtung, Befüllung und Weiterverarbeitung nach Maßgabe von Art. 6 Abs. 1 lit. a) bzw. Art. 9 Abs. 2 lit. a) DSGVO: Gemäß § 342 Abs. 1 SGB V erfolgt die Einrichtung der ePA „auf Antrag und mit Einwilligung des Versicherten“, begleitet von einer umfassenden Information durch die Krankenkasse (§ 343 SGB V). Auch im Weiteren setzt jede Befüllung der ePA aus dem Wortlaut der weitgehend parallel strukturierten §§ 347 ff. SGB V („auf Verlangen“) ersichtlich eine entsprechende Willensbetätigung der Patienten voraus,[18] jeweils auf der Grundlage einer entsprechenden obligatorischen Information in Bezug auf ihren gesetzlichen Befüllungsanspruch. Entsprechendes gilt für das Abrufen und sonstige Weiterverarbeiten der in der ePA gespeicherten Informationen (§§ 352 f. SGB V) sowie für das voraussetzungslose Löschen (§ 344 Abs. 3 SGB V) – dazu ausführlich unten in Punkt D. I.

2. Österreich, Estland und Spanien: Differenzierter Rückgriff auf gesetzliche Verarbeitungstatbestände

In Österreich, Estland und Spanien setzen die Gesetzgeber bei der Anlage und Befüllung der elektronischen Krankenakten demgegenüber – entsprechend der dort jeweils gewählten Opt-out-Konzeptionen – auf die *gesetzlichen* Verarbeitungsgrundlagen nach Art. 6 Abs. 1 lit. e) bzw. – vor allem – Art 9 Abs. 2 lit. g) bis j) DSGVO.

a) Österreich

Insbesondere in Österreich verweist der Gesetzgeber in § 13 Abs. 1 GTelG 2012 explizit auf die Bestimmungen des Art. 9 Abs. 2 lit. g) bis j) DSGVO. Bemerkenswert ist hier vor allem die deutliche und saubere Differenzierung zwischen der Anlage und Befüllung der ELGA einerseits nach Maßgabe von § 13 Abs. 1 und 3 GTelG 2012 und dem Abrufen und sonstigen Weiterverarbeiten der gespeicherten Gesundheitsdaten andererseits gemäß § 13 Abs. 2 und § 14 Abs. 2 GTelG 2012. Während das Abrufen und sonstige Weiterverarbeiten neben einwilligungsbasierten Zugriffen (§ 16 i.V.m. § 14 Abs. 2 Z 2 GTelG 2012) ausschließlich auf den Verarbeitungstatbestand des Art. 9 Abs. 2 lit. h) i.V.m. Abs. 3 DSGVO (d. h. die Verarbeitung zu Zwe-

[17] Siehe insbesondere BT-Drucks. 19/18793, S. 3, 82, 101 f., 109 f., 114, 118 und 130 f.
[18] Vgl. auch BT-Drucks. 19/18793, S. 120.

cken individueller Gesundheitsbelange, siehe § 14 Abs. 2 Z 1 GTelG 2012) bezogen wird – dazu später ausführlich unter IV. 2. –, wird die Einrichtung und Befüllung der ELGA zusätzlich auf die Verarbeitungstatbestände in Art. 9 Abs. 2 lit. g), i) und j) DSGVO gestützt, die primär *öffentliche (Gesundheits-)Interessen* im Blick haben.

Diese Differenzierung zwischen Anlegen und Befüllen einerseits und Abrufen bzw. sonstigem Weiterverarbeiten andererseits überzeugt: Die Anlage und die Befüllung der Patientenakten mit je möglichst vollständigen individuellen Gesundheitsdatenbanken schafft überhaupt erst die informationelle Basis für eine qualitativ hochwertige, allgemein zugängliche und selbstbestimmte (!) individuelle Gesundheitsversorgung, wie sie jedem elektronischen Patientenaktensystem vorschwebt. Ohne diese möglichst vollständige gesundheitsinformationelle Basis ist eine spätere wirksame Nutzung von im Rahmen konkreter Behandlungen und sonstiger Leistungserbringungen generierter Daten möglicherweise schon aus praktischen Gründen kaum möglich. Dies betrifft einerseits Verarbeitungen auf gesetzlicher Basis. Andererseits hat es der „datensouveräne" Patient im Nachhinein nicht mehr ohne Weiteres in der Hand, gesundheitsbezogene Daten, die für eine spätere Versorgung relevant werden, nachträglich auf Einwilligungsbasis einspeisen zu lassen und zu verwenden. Zu Recht benennt daher § 13 Abs. 1 GTelG 2012 die „Qualitätssteigerung diagnostischer und therapeutischer Entscheidungen sowie der Behandlung und Betreuung" (Z 1), die „Steigerung der Prozess- und Ergebnisqualität von Gesundheitsdienstleistungen" (Z 2), den „Ausbau integrierter Versorgung" (Z 3), die „Aufrechterhaltung einer qualitativ hochwertigen, ausgewogenen und allgemein zugänglichen Gesundheitsversorgung" (Z 4) sowie nicht zuletzt auch die „Stärkung der Patient/inn/en/rechte" (Z 5) als die für das Einspeichern von Gesundheitsdaten gemäß § 13 Abs. 3 GTelG 2012 relevanten „erheblichen öffentlichen Interessen" im Sinne von Art. 9 Abs. 2 lit. g) und i) GTelG 2012. Insgesamt spiegelt sich in der Wahl dieser Verarbeitungszwecke und -grundlagen der prononciert wirksamkeitsorientierte Ansatz des österreichischen Modells.

Diese Konstruktion dürfte – wie sich im Grundsatz bereits dem noch zur Datenschutzrichtlinie erarbeiteten Arbeitspapier der Artikel 29-Datenschutzgruppe zu elektronischen Patientenakten entnehmen ließ[19] – mit den Vorgaben der DSGVO grundsätzlich im Einklang stehen. Maßstäblich ist insoweit zunächst der Grundsatz der *Zweckfestlegung* (und der nachfolgenden Zweckbindung) gemäß Art. 5 Abs. 1 lt. b) DSGVO. Dieser verlangt, dass die Informationen nur „für festgelegte, eindeutige und legitime Zwecke erhoben werden" und „nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden" dürfen. Die Bedeutung dieses Grundsatzes wird durch seine Verankerung in Art. 8 Abs. 2 S. 1 GR-Charta unterstrichen. Eine Speicherung personenbezogener Daten „auf Vorrat zu unbestimmten und noch nicht bestimmbaren Zwecken" ist somit nicht nur nach deut-

[19] Vgl. Artikel 29-Datenschutzgruppe, Arbeitspapier zur Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA) – WP 131, 2007, S. 14.

schem Verfassungsrecht,[20] sondern auch unionsrechtlich[21] seit je her unzulässig – auch dann, wenn es – wie hier – um Verarbeitungen in Erfüllung einer öffentlichen Aufgabe geht.[22] Eine unzulässige „Vorratsgesundheitsdatenspeicherung" wird man in dem österreichischen Konzept gleichwohl nicht sehen können. Die Speicherung der in § 14 Abs. 3 GTelG 2012 aufgeführten Informationen dient in erster Linie dazu, ordnungsgemäße und qualitativ hochwertige, zum Zeitpunkt der Erhebung gewiss noch nicht im Einzelnen feststehende künftige Behandlungen und sonstige Maßnahmen nach § 14 Abs. 2 i.V.m. § 13 Abs. 2 GTelG 2012 überhaupt erst zu ermöglichen oder zumindest informationell zu unterstützen. Die spätere Verarbeitung erfolgt auf der Basis von Art. 9 Abs. 2 lit. h) DSGVO (individuelle Gesundheitsversorgung) bzw. einer Einwilligung des Patienten (dazu unten bei IV. sowie V.). Diese Zweckfestlegung in § 13 Abs. 1 und 3 GTelG 2012 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.[23] Dabei sollten insbesondere auch die spezifischen praktischen Bedürfnisse im medizinischen Bereich 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.

Auch die stets zu verlangende *Erforderlichkeit* der Datenspeicherung durfte der österreichische Gesetzgeber zumindest in Bezug auf reguläre Gesundheitsdaten (z. B. Befunde oder Medikationsdaten) prinzipiell unterstellen. In Anbetracht der typischerweise bestehenden Prognoseunsicherheiten hinsichtlich deren Relevanz für künftige Behandlungen muss der Datenschutzgesetzgeber im Grundsatz über entsprechende Prognosespielräume verfügen. Von diesen Spielräumen hat das GTelG 2012 durchaus differenziert Gebrauch gemacht, zumal § 13 Abs. 4 GTelG 2012 vor diesem Hintergrund für sensiblere Bilddaten eine Einzelfallprüfung durch den jeweiligen Gesundheitsdiensteanbieter verlangt.

Keine andere Bewertung ergibt sich aus dem *Gebot datenschutzfreundlicher Voreinstellungen* – sei es in unmittelbarer Anwendung des Art. 25 Abs. 2 DSGVO, sei es unter Rückgriff auf die in jener Bestimmung konkretisierten datenschutzrechtlichen Grundsätze. Die Anlage und Befüllung der ELGA nach Maßgabe des Opt-out-Modells österreichischer Provenienz lässt sich, wie gezeigt, auf der Basis des geltenden

[20] Vgl. dazu BVerfGE 125, 260 (317).

[21] Vgl. nur EuGH, Urteil Digital Rights Ireland, C-293/12 und C-594/12, EU:C:2014:238.

[22] A.A. und großzügiger offenbar *H. Wolff*, D. Grundprinzipien und Zulässigkeit der Datenverarbeitung, in: Neues Datenschutzrecht, 2017, Rn. 404.

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

Datenschutzrechts, insbesondere der gesetzlichen Verarbeitungstatbestände und der allgemeinen Datenschutzgrundsätze, rekonstruieren. Ein über jene Vorgaben hinausweisender „Vorrang von Einwilligungslösungen" oder ein pauschaler „Vorrang des Opt-in" lässt sich dem geltenden Datenschutzrecht richtigerweise nicht entnehmen.

b) Estland

Die zumindest im Grundsatz ähnlichen Opt-out-Konzeptionen der Systeme in Estland und Spanien stützen sich auf vergleichbare Zwecke bei der Anlage und Befüllung der Patientenakten. Im estnischen Gesetz über die Organisation der Health Services verweist vor allem die Eingangsdefinition des HIS in § 59[1] TTKS auf die Qualität von Gesundheitsdienstleistungen, die Patientenrechte sowie den Schutz der öffentlichen Gesundheit. Das Abrufen und sonstige Zugriffsbefugnisse sind – wie im österreichischen Recht, wenn auch ohne explizite Hinweise auf die Verarbeitungstatbestände der DSGVO – getrennt davon in § 593 TTKS geregelt.

c) Spanien

Die spanischen Regelungen über die HC definieren deren Ziele und die damit eingehenden öffentlichen Interessen zunächst in Art. 15 Ley 41/2002. Die Einbringung sämtlicher Informationen, die „für die wahrheitsgemäße und aktuelle Kenntnis des Gesundheitszustandes des Patienten als wesentlich erachtet werden" (Abs. 1), dient gemäß Abs. 2 der „Ermöglichung und Unterstützung der Gesundheitsversorgung" („facilitar la asistencia sanitaria"). Art. 16 Ley 41/2002 wiederholt diese Zwecksetzung und bezeichnet die HC als ein Instrument, das „grundsätzlich dazu dient, eine angemessene Versorgung des Patienten zu gewährleisten" („destinado fundamentalmente a garantizar una asistencia adecuada al paciente").

3. Wertender Vergleich

Vor allem die genauere Analyse der österreichischen Konzeption zeigt indes, dass die Patientensouveränität einerseits und die Wirksamkeit eines elektronischen Patientenaktensystems andererseits keineswegs gegeneinander ausgespielt werden dürfen. Der vermeintlich patientenautonomieaverse Rückgriff auf gesetzliche Verarbeitungstatbestände (und nicht die Einwilligung) zur Anlage und Befüllung von Patientenakten kann sich demnach mittel- und langfristig als Absicherung und Stärkung gerade auch der Patientenautonomie erweisen. Denn nur wer auf eine vollständige gesundheitsinformationelle Basis zurückgreifen kann, ist im Rahmen späterer Maßnahmen der Gesundheitsversorgung überhaupt in der Lage, eine möglichst informierte, selbstbestimmte Entscheidung über den weiteren Umgang mit der eigenen Gesundheit zu treffen. § 13 Abs. 1 Z 5 GTelG 2012 benennt daher nicht umsonst die „Stärkung der Patient/inn/en/rechte" als eines jener erheblichen öffentlichen Interessen, die für die Speicherung der im Einzelnen näher bezeichneten Gesundheits-

daten auf gesetzlicher Basis streiten. Umgekehrt wurde bei der rechtlichen Einordnung deutlich, dass das Selbstbestimmungsrecht der Patienten im Rahmen von Opt-out-Lösungen hinreichend respektiert und – wie es in Art. 9 Abs. 2 lit. g) bis j) DSGVO heißt – mit „angemessenen und spezifischen Maßnahmen" bedacht werden muss, damit die anfänglich defizitäre aktive Patientenbeteiligung an der Anlage und Befüllung elektronischer Patientenakten durch spätere Beteiligungs- und Sicherungselemente kompensiert werden kann. Die Belange der Patientensouveränität und der Wirksamkeit des Patientenaktensystems müssen und sollten vor diesem Hintergrund keineswegs als gegenläufige Prinzipien begriffen werden. In Anbetracht der dargelegten Vorzüge eines autonomiesichernd ausgestalteten Opt-out-Modells sowohl für die Wirksamkeit eines Patientenaktensystems als auch für die Stärkung der Patientenautonomie drängt sich der Schluss auf, dass die Implementierung eines solchen Modells den Bedürfnissen eines modernen Gesundheitssystems besser Rechnung trägt als ein striktes Opt-in-Modell, wie es nun in Deutschland vorgesehen ist.[24]

IV. Berechtigung einzelner Leistungserbringer zum Zugriff auf die Patientenakte

Die Berechtigung für den einzelnen Leistungserbringer zum Abruf von Informationen, die in einer elektronischen Patientenakte abgespeichert sind, setzt zunächst – wie schon die Einrichtung und Befüllung der Akte – einen Erlaubnistatbestand nach Art. 9 Abs. 2 DSGVO voraus. Als Verarbeitungsgrundlage kommt einerseits wiederum Art. 9 Abs. 2 lit. a) DSGVO (explizite Einwilligung) in Betracht, andererseits aber auch einwilligungsunabhängige gesetzliche Verarbeitungstatbestände. Für den Informationsabruf erscheint vor allem Art. 9 Abs. 2 lit. h) i.V.m. Abs. 3 DSGVO relevant (Belange der individuellen Gesundheit, insbesondere medizinische Diagnostik, Versorgung und Behandlung). Für sämtliche Verarbeitungstatbestände gilt auch an dieser Stelle, dass sie dem Erforderlichkeitsgrundsatz genügen müssen, d. h. ein Informationsabruf ist nur zulässig, wenn und soweit dies zur Erreichung der konkreten Verarbeitungszwecke erforderlich und kein milderes, gleich effektives Mittel greifbar ist;[25] eine wichtige Rolle spielt insoweit insbesondere die Frage, in welcher Funktion (z. B. als Arzt) und zu welchem konkreten Zweck (z. B. im Kontext einer Behandlung wegen Schwindelbeschwerden) ein Zugriffsberechtigter auf Informationen in der Patientenakte zugreifen möchte. Insgesamt kommt der Einwilligung dabei trotz des gesteigerten Risikos der Verarbeitung großer Mengen an Gesundheitsdaten kein Vorzug gegenüber den gesetzlichen Verarbeitungsgrundlagen zu, diese stehen auch mit Blick auf den Abruf von Gesundheitsdaten prinzipiell gleichberechtigt nebeneinander.[26]

[24] Vgl. im Ergebnis ebenso und zu Recht *SVR Gesundheit* (Fn. 4), S. 85 ff.

[25] Vgl. allgemein etwa *M. Albers/Veit*, in: Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht Kommentar, Art. 6 DSGVO Rn. 16.

[26] Vgl. grundsätzlich *Frenzel* (Fn. 15), Art. 6 DSGVO Rn. 10.

Besondere Bedeutung dürfte im Kontext eines Berechtigungssystems (entweder unmittelbar gemäß Art. 25 Abs. 2 DSGVO oder als Ausfluss des allgemeinen Prinzips der Datenminimierung) dem Datenschutz durch Voreinstellung zukommen. Das Prinzip verpflichtet den Verantwortlichen, seine Voreinstellungen bereits so einzusetzen, dass die Datenverarbeitung nur für den jeweiligen Verarbeitungszweck erfolgt und nicht erforderliche Daten auch nicht verarbeitet werden.[27] Durch eine solche Anwendung werden Nutzer geschützt, die die datenschutzrechtlichen Implikationen nicht erfassen können oder sich nicht darüber Gedanken machen und somit eine eigene datenschutzfreundliche Einstellung nicht vornehmen. Das Ziel hierbei ist – um dies noch einmal zu betonen – kein genereller Opt-in-Zwang, sondern die Ermöglichung einer autonom getroffenen Entscheidung durch die Vermeidung von datenschutzfeindlichen Voreinstellungen.[28] Freilich verbirgt sich hinter dieser Vorschrift eine gewisse Lenkungsfunktion, denn die wenigsten Nutzer ändern die initialisierten, aber abänderbaren Konfigurationen.[29] Dabei muss die Zugänglichkeit der personenbezogenen Daten ebenso auf das erforderliche Maß zur Zweckerreichung beschränkt sein, auch für den Datenverarbeiter selbst.[30]

1. Deutschland und Österreich: Starre Gruppenzuordnungen auf unterschiedlicher Rechtsgrundlage

In Deutschland und Österreich ergeben sich aus den gesetzlichen Regelungen jeweils differenzierte *Berechtigungsgruppen.* So unterscheiden die *deutschen* Bestimmungen zwischen den Akteuren mit (1) umfassender, (2) beschränkter – auf Lesen, Speichern und Verwenden bestimmter Datenfelder (immerhin einschließlich medizinischer Informationen wie Befunde, Diagnosen, Therapiemaßnahmen etc.) – und (3) versorgungsunabhängiger Berechtigung sowie (4) Akteuren ohne Zugriffsberechtigung, siehe § 352 i.V.m. § 341 Abs. 2 SGB V. Diese Differenzierung trägt letztlich den datenschutzrechtlichen Grundsätzen der Erforderlichkeit und der Datenminimierung Rechnung: Umfassenden Zugriff auf sämtliche gespeicherten Informationen haben grundsätzlich allein diejenigen Akteure, die diesen ihrer Funktion nach typischerweise auch benötigen, namentlich Ärzte, Zahnärzte und Psychotherapeuten sowie deren berufsmäßigen Gehilfen und Personal zur Vorbereitung auf den Beruf; einschränkendes Merkmal ist freilich im konkreten Fall stets die Erforderlichkeit des Zugriffs für die jeweilige Behandlung. Von vornherein keinen umfassenden Zugriff billigt der Gesetzgeber demgegenüber etwa einem Apotheker aus der Berechtigungsgruppe 3 zu, der beispielsweise keinen Zugriff auf Daten aus einer elektronischen

[27] *Martini* (Fn. 15), Art. 25 DSGVO Rn. 2.

[28] *Martini* (Fn. 15), Art. 25 DSGVO Rn. 13 f.

[29] Vgl. Art. 29-Datenschutzgruppe, Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke – WP 163, 2009, S.8; *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht DS-GVO mit BDSG, 2019, Art. 25 DSGVO Rn. 41; *Martini* (Fn. 15), Art. 25 DSGVO Rn. 46.

[30] *Martini* (Fn. 15), Art. 25 DSGVO Rn. 52.

Zusatzanwendung i. S. v. § 345 Abs. 1 SGB V haben kann (z. B. aus einer Health-App).

Die *österreichischen* Regelungen sind in ähnlicher Weise nach Berechtigungsgruppen ausdifferenziert, sehen dabei zum Teil aber noch weitergehende Einschränkungen vor. So erhalten lediglich Ärzte, Einrichtungen der Pflege und Mitarbeiter der ELGA-Ombudsstelle sowie deren gesetzliche und bevollmächtigte Vertreter eine generelle Zugriffsberechtigung, wohingegen Zahnärzte nur auf medizinische Dokumente und Medikationsdaten und Apotheken ohnehin nur auf Medikationsdaten zugreifen können. Eine spezifische Zugriffsberechtigung besteht darüber hinaus noch für Gesundheitsdiensteanbieter der Primärversorgung und impfende Anbieter. Eine besondere Rolle spielen wiederum die Erforderlichkeit sowie der Verarbeitungskonnex des konkreten Informationsabrufs.

Ein wesentlicher Unterschied zwischen dem deutschen und dem österreichischen Modell bildet – wie schon mit Blick auf die Befüllung der Patientenakten – die maßgebliche *Rechtsgrundlage* individueller Zugriffe. Das strikte *deutsche* Einwilligungskonzept erfordert hier zusätzlich zu der schriftlichen Einwilligung zur Anlage und Einrichtung der ePA (1. Opt-in-Stufe) eine erneute Einwilligung in Bezug auf den behandelnden und grundsätzlich zugriffsberechtigten Gesundheitsdiensteanbieter, wenn dieser Informationen abrufen dürfen soll (2. Opt-in-Stufe). Sollte die Standardeinstellung der Dauer der Zugriffsberechtigung von einer Woche nicht geändert worden sein, wird jeweils nach Ablauf der Zeit eine erneute Einwilligung notwendig. Auch bei der Involvierung weiterer Leistungserbringungen in die bereits bestehende Behandlung müssen ggfs. multiple Einwilligungen eingeholt werden (3. Opt-in-Stufe), von der Freigabe zu Forschungszwecken ganz zu schweigen (4. Opt-in-Stufe). Ein solches kaskadenartiges Opt-in-Modell dürfte mehr zur Ermüdung denn zur Ermutigung des Patienten führen, Leistungserbringern Zugriff auf seine Patientenakte zu gewähren.[31]

In *Österreich* wird demgegenüber auf einen gesetzlichen, einwilligungsunabhängigen Verarbeitungstatbestand zurückgegriffen. Anders als bei der Befüllung der ELGA wird der Abruf von Informationen zwar nicht auf die Tatbestände des Art. 9 Abs. 2 lit. g) oder j) DSGVO gestützt, wohl aber auf die Basis für eine individuelle Gesundheitsversorgung nach Art. 9 Abs. 2 lit. h) i.V.m. Abs. 3 DSGVO (siehe § 14 Abs. 2 Z 1 GTelG). Anhaltspunkte für eine Unvereinbarkeit mit deren Vorgaben, insbesondere die Anforderungen des Art. 9 Abs. 3 DSGVO, sind nicht ersichtlich. Der Zugriff eines Gesundheitsdiensteanbieters kann konsequenterweise gesperrt werden.

[31] Dazu auch *SVR Gesundheit* (Fn. 4), *S. 8*6.

2. Estland und Spanien: Gesetzliche Zugriffsberechtigung ohne relevante Gruppenbeschränkungen

Die Systeme in Estland und Spanien weisen im Unterschied zu den deutschen und österreichischen Konzepten keine gesetzlich definierten Gruppen mit unterschiedlichen Berechtigungen auf. In *Estland* hat gemäß § 59[3] Abs. 2 TKKS grundsätzlich jeder „health care provider", d. h. gemäß § 4 TKKS alle als „health care providers" geltenden „health care professionals" (§ 3 Abs. 1 TKKS: „doctors", „dentists", „nurses" und „midwives") und „legal entities providing health services", zum Zwecke der Erbringung von (vertraglichen) Gesundheitsdienstleistungen Zugriff auf die Daten eines Patienten.

Ähnliches gilt für das *spanische* System. In Art. 16 Abs. 1 S. 2 Ley 41/2002 ist vorgesehen, dass die „medizinischen Fachkräfte des Zentrums, die den Patienten diagnostizieren oder behandeln, […] Zugang zu den Krankenakten des Patienten als grundlegendes Instrument für die ordnungsgemäße Versorgung" haben. Daneben finden sich lediglich Restriktionen für Verwaltungs- und Managementpersonal und Gesundheitspersonal mit „Inspektions-, Evaluierungs-, Akkreditierungs- und Planungsfunktionen" (Art. 16 Abs. 4 und 5 Ley 41/2002), also Personen, die mit den einzelnen Patienten in keinem unmittelbaren gesundheitsbezogenen Kontext zu tun haben.

Was die Rechtsgrundlage für die Ausübung einer Zugriffsberechtigung betrifft, enthalten die estnischen und spanischen Regelungen zwar keine dem österreichischen Recht vergleichbare explizite Angabe. Es wird indes deutlich, dass auch sie die Verarbeitung auf den gesetzlichen, einwilligungsunabhängigen Tatbestand des Art. 9 Abs. 2 lit. h) i.V.m. Abs. 3 DSGVO stützen.

3. Wertender Vergleich

Ein Vergleich der unterschiedlichen Modelle macht zunächst – ganz ähnlich wie die Überlegungen zur Einrichtung der elektronischen Patientenakten unter Punkt III. – deutlich, dass die erfolgreichen Patientenaktensysteme Österreichs, Estlands und Spaniens in zulässiger Weise von gesetzlichen Zugriffsberechtigungen auf der Basis von Art. 9 Abs. 2 lit. h) i.V.m. Abs. 3 DSGVO Gebrauch machen. Die deutsche Einwilligungskaskade erscheint im Vergleich dazu als umständliche, ineffiziente Exotenregelung, die offenkundig alle Gestaltungsentscheidungen einer sehr formal interpretierten Patientensouveränität unterordnet.

Die Bildung von Berechtigungsgruppen wirkt demgegenüber im Grundsatz durchaus sinnvoll, zumal im Rahmen eines Opt-out-Modells: Sie wird den Grundsätzen der Erforderlichkeit und der Datenminimierung gerecht und sollte daher prinzipiell beibehalten werden. Die estnischen und spanischen Regelungen erscheinen im Vergleich extrem großzügige Zugriffsberechtigungen zu vergeben. Reflektiert werden sollte indes, ob die gesetzlichen Berechtigungsgruppen – wie derzeit im deutschen und österreichischen Modell jeweils vorgesehen – tatsächlich zwingend vor-

gegeben werden sollten, oder ob sie als dispositive, datenschutzfreundliche Voreinstellung lediglich den Ausgangspunkt bilden sollten, von dem der Patient kraft seiner Einwilligungsbefugnis bewusst abweichen darf. Zwar mag eine zwingende Vorgabe auf der Basis des Art. 9 Abs. 4 DSGVO noch rechtlich vertretbar sein;[32] einer richtig, d. h. nicht übermäßig paternalistisch verstandenen Patientensouveränität dürfte sie jedenfalls nicht entsprechen.

V. Steuerungsmöglichkeiten des Patienten

Für die Steuerung der Inhalte der einzelnen Patientenakte durch den Patienten erscheinen vor allem zwei datenschutzrechtliche Maßgaben von besonderer Relevanz. In einem *positiven* Sinne sollte der einzelne Patient, schon aufgrund seiner Einwilligungsbefugnis kraft Art. 9 Abs. 2 lit. a) DSGVO, grundsätzlich die Möglichkeit haben, explizit in jede Verarbeitung seiner Gesundheitsdaten einzuwilligen. Allerdings gestattet Art. 9 Abs. 4 DSGVO es den Mitgliedstaaten, dass sie „zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist", d. h. die mitgliedstaatlichen Ausgestaltungen können die Erlaubnistatbestände des Art. 9 Abs. 2 DSGVO im Grundsatz modifizieren oder gar vollständig verdrängen, sofern und soweit dadurch das datenschutzrechtliche Schutzniveau angehoben wird.[33]

In einem *negativen* Sinne muss der Patient überdies gewisse Möglichkeiten haben, die Speicherung von Informationen ganz oder teilweise zu verhindern bzw. gespeicherte Informationen ganz oder teilweise zu sperren oder zu löschen, also Möglichkeiten zu einem vollständigen oder teilweisen Opt-out oder Blank-out, und zwar in differenzierter Weise.[34] Normative Ansatzpunkte sind einerseits der Erforderlichkeitsgrundsatz – ohne ausdifferenzierte Blank-out-Möglichkeiten lassen sich Zugriffe nicht sinnvoll auf das erforderliche Maß beschränken –, andererseits konzeptabhängige Vorgaben. Speziell für einwilligungsbasierte Systeme dürfte sich ein „Beschränkungsrecht" bereits aus dem allgemeinen Recht zum Widerruf der Einwilligung nach Art. 7 Abs. 3 DSGVO ergeben. Ein Gebot zur Differenzierung

[32] Vgl. ausdrücklich etwa *C. Dochow*, Das Patienten-Datenschutz-Gesetz (Teil 2): Die elektronische Patientenakte und erweiterte Datenverarbeitungsbefugnisse der Krankenkassen, MedR 2021, S. 13 (15).

[33] Vgl. grundsätzlich *D. Kampert*, in: Sydow (Hrsg.), Europäische Datenschutzgrundverordnung Kommentar, 2. Aufl. 2018, Art. 9 DSGVO Rn. 59 f.; *T. Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht DS-GVO mit BDSG, 2019, Art. 9 DSGVO Rn. 101.

[34] Diese Forderung besteht in der deutschen Datenschutzrechtswissenschaft bereits seit geraumer Zeit, wenn auch mit unterschiedlichen Begründungen – vgl. etwa *T. Weichert*, Die elektronische Gesundheitskarte, DuD 2004, S. 391 (400); *G. Hornung*, Die digitale Identität, 2005, S. 224 ff.; *C. Dochow*, Grundlagen und normativer Rahmen der Telematik im Gesundheitswesen, 2017, S. 1118 ff.; *J. Schütz/S. Schmitz/J. Ippach*, Die elektronische Patientenakte – Anforderungen aus Sicht des Datenschutzes, RDV 2019, S. 224 (230).

der Steuerungsmöglichkeiten ergibt sich dabei aus dem Freiwilligkeitsgrundsatz (Art. 7 Abs. 4 DSGVO), denn bei undifferenzierten Steuerungsmöglichkeiten nach dem Prinzip „Alles oder nichts" würde der Patient unter Druck gesetzt, im Interesse einer funktionierenden Patientenakte den Zugriff im Zweifel auf mehr Informationen zu gestatten, als ihm eigentlich lieb wäre. Bei Systemen, die auf einer automatischen Einrichtung und Befüllung auf gesetzlicher Grundlage basieren, wird man Opt-out- und Blank-out-Möglichkeiten als Ausgestaltungen des Widerspruchsrechts begreifen müssen. In Art. 21 DSGVO wird ein Widerspruchsrecht explizit rechtlich niedergelegt. Dieses wird als unbedingtes Recht nur bei bestimmten Verarbeitungen vorgesehen, etwa bei der Direktwerbung (Abs. 2 und 3). Nichtsdestotrotz wird man bei Opt-out-Systemen, die Gesundheitsinformationen auf der Basis des gesetzlichen Verarbeitungstatbestands nach Art. 9 Abs. 2 lit. g) DSGVO verarbeiten, als zwingend „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).

1. Deutschland

Zumindest in seiner finalen Ausbaustufe ab dem 1. 1. 2022 soll das deutsche Patientenaktensystem es dem Einzelnen gestatten, von seinem eigenen Endgerät aus feingranular den Zugriff von Leistungserbringern auf Dokumente und Datensätze bzw. Gruppen von Dokumenten und Datensätzen zu steuern (§ 342 Abs. 2 Nr. 2 lit. b) SGB V) oder mittels der dezentralen Infrastruktur eines Leistungserbringers eine Einwilligung in den Zugriff zumindest mittelgranular auf Kategorien von Dokumenten und Datensätzen erteilen können (§ 342 Abs. 2 Nr. 2 lit. c) SGB V). Auch wenn die Möglichkeit bestehen soll, einem Vertreter die Befugnis zu erteilen, die Rechte des Vertretenen im Rahmen der Führung der Patientenakte – und damit auch die feingranulare Ansteuerung über ein Endgerät – innerhalb der erteilten Befugnis wahrzunehmen (§ 343 Abs. 1 S. 3 Nr. 19 SGB V), wurde die nur mittelgranulare Steuerungsmöglichkeit über die Infrastruktur der Leistungserbringer – wie bereits in der Einführung und in Teil 1[35] angedeutet – in Deutschland teilweise für datenschutzrechtswidrig befunden.[36] Bei allen Ansteuerungen sollen die für den betreffenden Leistungserbringer ggfs. ausgeblendeten Dokumente und Datensätze gänzlich verborgen bleiben. Ein vollständiger Opt-out unter Löschung sämtlicher In-

[35] In Teil 1 der für die Stiftung Münch (Hrsg.) angefertigten Studie von *Krönke/Aichstill*, Die elektronische Patientenakte und das europäische Datenschutzrecht, 2021, S. 7.

[36] Vgl. dazu *BfDI*, BfDI zu Folgen der Gesetzgebung des PDSG, DuD 2020, S. 640; s.a. *BfDI*, Stellungnahme zum PDSG vom 25.5. 2020, S. 12 f.; kritisch auch BRat, BT-Dr. 19/19365, S. 14 f.; BR-Drucksache 164/20, S. 17; *Bundespsychotherapeutenkammer*, Stellungnahme zum PDSG vom 19. Mai 2020; *Deutscher Caritasverband e.V.*, Stellungnahme zum PDSG vom 19. Mai 2020.

formationen schließlich ist gemäß § 344 Abs. 3 SGB V jederzeit möglich. Differenziertere Opt-out-Möglichkeiten sind in Deutschland angesichts des Einwilligungsmodells entbehrlich. Mit Blick auf die Zugriffsdauer wird der eingewilligte Zugriff im Sinne datenschutzfreundlicher Voreinstellung (Art. 25 Abs. 2 DSGVO) für eine Woche freigeschalten und kann weitergehend zwischen einen Tag und 18 Monate verkürzt bzw. verlängert werden; letztendlich soll in der Endphase sogar eine unbegrenzte Zeitspanne möglich sein. Im Leitfaden des Unternehmens gematik für die deutschen Krankenkassen wird technisch eine Zeitspanne auf bis zu 540 Tagen vorgenommen.

2. Österreich

Auch das österreichische ELGA-Portal erlaubt individuelle feingranulare Steuerungsmöglichkeiten in Form von Rechten auf ausdifferenzierte Ein- und Ausblendungen von ELGA-Gesundheitsdaten (§ 16 Abs. 2 lit. a) GTelG), auf Löschung von ELGA-Gesundheitsdaten (§ 16 Abs. 2 lit. a) GTelG) sowie das Recht einer zeitlichen Verkürzung von Zugriffsberechtigungen für ELGA-Gesundheitsdiensteanbieter (§ 16 Abs. 2 lit. b) GTelG), und zwar sowohl über ein Endgerät als auch bei der Ombudsstelle. Weitergehend kann auch ein Gesundheitsdiensteanbieter des besonderen Vertrauens mit dessen Einverständnis ernannt werden (§ 16 Abs. 2 lit. c) GTelG). Einschränkungen liegen in der österreichischen Variante besonders bei der e-Medikation durch die lediglich bestehende Ausblendemöglichkeit der gesamten Liste und beim Impfpass, der keinerlei Schaltungsmöglichkeiten zulässt. Der Impfpass ist jedoch eine eigene Anwendung, die nur im ELGA-Portal angesiedelt, jedoch kein förmlicher Bestandteil der ELGA davon ist.[37] Ferner besteht ein ausgebautes Vertretungsmodul. Die Zugriffsbeschränkungen bezüglich einzelner Informationen haben – wie in Deutschland – zur Folge, dass die Dokumente gänzlich verborgen werden.

Mit Blick auf die Opt-Out-Möglichkeiten ist das österreichische Modell sehr stark ausdifferenziert. Es gibt einerseits einen generellen Opt-out über die Benutzeroberfläche sowie über die ELGA-Ombudsstellen sowie einen situativen Opt-out beim Leistungserbringer vor Ort – so können gewissermaßen „in letzter Minute" noch einzelne Gesundheitsdiensteanbieter vom Zugriff ausgeschlossen werden. Eine weitere Besonderheit des differenzierten Opt-out in Österreich bezieht sich auf die besonderen Informationsrechte nach § 16 Abs. 2 Z 2 GTelG, wonach bei besonders sensiblen Daten, nämlich Daten betreffend HIV-Infektionen (a)), psychische Erkrankungen (b)), die in § 71a Abs. 1 GTG genannten genetischen Daten (c)) oder Schwangerschaftsabbrüche (d)), dezidiert auf die Datenaufnahme sowie das damit eingehende Recht auf einen Widerspruch informiert werden muss. Hinzuweisen ist erneut auf das Pilotprojekt eines elektronischen Impfpasses, der kein Bestandteil der ELGA ist, je-

[37] Siehe https://www.elga.gv.at/e-impfpass/e-impfpass/ sowie https://www.elga.gv.at/e-impfpass/faq-zum-e-impfpass/.

doch im ELGA-Portal eingegliedert wird. Ein Opt-out aus dieser Anwendung ist aufgrund des besonderen wichtigen öffentlichen Interesses nicht möglich – hier wird (auch) auf die COVID-19-Pandemie und die Bedeutung einer lückenlosen Dokumentation aller Impfungen für die Durchimpfungsrate der Bevölkerung verwiesen.[38] Mit Blick auf die – wie in Deutschland voreingestellte – Zugriffsdauer wird schließlich zwischen generellen Gesundheitsdiensteanbietern, Apothekern und den Gesundheitsdiensteanbietern des besonderen Vertrauens unterschieden. Ein allgemeiner Zugriff besteht für 28 Tage ab Identifikation, Apotheker erhalten hier nur zwei Stunden und der eigens gewählte Vertrauensanbieter kann bereits für ein Jahr zugreifen (§ 18 Abs. 6 und 7 GTelG).

3. Estland

In Estland existiert, ähnlich wie in Österreich, ein feingranulares Berechtigungsmanagement mit Möglichkeiten der Ein- und Ausblendungen sowie einzelner Sperrungen durch den Einzelnen über dessen Endgerät; sogar ein Gesundheitsdiensteanbieter kann zum Schutze des Lebens und der Gesundheit der Patienten einzelne Daten für bis zu sechs Monate ausblenden. Auch ein Vertretermodell ist in Estland vorgesehen. Mit Blick auf die Opt-out-Möglichkeiten kennt das estnische Modell einen generellen Opt-out sowie einen situativen Opt-out mittels Antrags beim Leistungserbringer. Auch in Estland hat ein Blank-out die vollständige Verbergung der betreffenden Daten zur Folge. Eine Voreinstellung der Zugriffsdauer besteht in Estland nicht.

4. Spanien

In Spanien gestalten zwar die einzelnen autonomen Gemeinschaften sowie die Centros de Salud Einzelheiten der Portale, jedoch sollen auch sie gemäß den Leitlinien des spanischen Gesundheitsministeriums entsprechende feingranulare Ein- und Ausblendefunktionen vorsehen.[39] In der Praxis ermöglichen die autonomen Gemeinschaften beispielsweise in der Region des Baskenlands und Madrids freilich kaum solche genauen Schaltungsmöglichkeiten. Grundsätzlich kann auch in den dezentralen spanischen Regelungen ein Vertretungssystem etabliert werden, beispielsweise in den Regelungen im Baskenland, mit ihrer kontinuierlichen Bezugnahme auf den Versicherten selbst oder die bevollmächtigte Person (Art. 12 Decreto 38/2012). Bemerkenswert ist das spanische Modell zunächst insofern, als es – soweit ersichtlich – auf einen generellen Opt-out verzichtet und der lückenlosen und umfas-

[38] Siehe https://www.elga.gv.at/e-impfpass/e-impfpass/ und https://www.elga.gv.at/e-impfpass/faq-zum-e-impfpass/.

[39] Vgl. dazu das Konzeptpapier des früheren spanischen Instituts für Gesundheitsinformationen (heute: Abteilung für Gesundheitsinformation und Evaluierung im spanischen Gesundheitsministerium) zum spanischen Electronic Health Record System, verfügbar unter https://www.mscbs.gob.es/organizacion/sns/planCalidadSNS/docs/HCDSNS_English.pdf.

senden Gesundheitsvorsorge somit einen sehr hohen Stellenwert zuspricht. Besonders hervorzuheben ist ferner auch, dass die zitierten Leitlinien des spanischen Gesundheitsministeriums die Verankerung eines Warnhinweises für Ausblendungen vorsehen und den Leistungserbringern mittels „Verschattung" angezeigt werden soll, dass in Ansehung nicht näher bezeichneter Daten eine Ausblendung vorgenommen wurde. Letzteres dürfte eine eigenständige Datenverarbeitung sein, die sich auf Art. 9 Abs. 2 lit. g) DSGVO stützen lässt. In ebendiese Richtung zielt schließlich auch ein in den Leitlinien ebenfalls vorgesehener Notfallmodus, denn durch einen einfachen Klick und Bestätigung eines Warnhinweises sollen die spanischen Gesundheitsdiensteanbieter ohne weitere Anforderungen die Ausblendungen sichtbar machen können. In Ansehung der Zugriffsdauer wird in Spanien eine „angemessene Zeit" vorgegeben, mindestens 5 Jahre ab Entlassung (Art. 17 Abs. 1 Ley 41/2002).

5. Wertender Vergleich

Im Vergleich zeigt sich zunächst, dass eine feingranulare Steuerungsmöglichkeit ganz offensichtlich zum datenschutzrechtlichen „State of the Art" gehört. Dass diese Feinsteuerungsmöglichkeit in Deutschland lediglich über ein eigenes Endgerät eröffnet sein soll und nicht über ein Service-Terminal o. ä., erscheint auch angesichts der Modelle in Estland und Spanien unbedenklich, zumal sämtliche Konzepte ein Vertretermodul vorsehen und es Personen mit geringer technischer Affinität möglich sein wird, zumindest vertretungsweise feingranulare Zugriffsrechte auszuüben.

Auch auf einen Opt-out verzichtet keines der Vergleichsmodelle, auch wenn sich im Einzelnen deutliche Unterschiede ergeben. Das deutsche Modell erscheint hier wenig vergleichstauglich, da es als einziges System auf einem Einwilligungskonzept basiert. Als sehr ausgewogen erweist sich insbesondere das österreichische Modell mit seinem ausdifferenzierten Opt-out, der vor allem für die Einspeicherung von ganz besonders sensiblen Gesundheitsdaten ausnahmsweise auf eine explizite Willensbetätigung des Patienten hinwirkt. Nicht ganz unproblematisch erscheint insofern das spanische Modell, das keine generelle Opt-out-Möglichkeit kennt und an dieser Stelle kaum als Vorbild taugen dürfte.

Anders scheint uns der Weg zu bewerten zu sein, den das spanische Konzept in Bezug auf die Modalitäten des Blank-out gegangen ist. Für eine Gesundheitsversorgung ohne „Datenlücken" dürfte eine Verschattung ausgeblendeter Daten besonders wichtig sein. Ansonsten besteht ggfs. keine uneingeschränkte Möglichkeit für den Versorger, eine umfassende Diagnose auf Basis der Daten zu treffen.[40] Eine Verschattung würde es ermöglichen, dass der Leistungserbringer diese bei Bedarf im Behandlungsgespräch thematisieren könnte, etwa bei der Neuverordnung eines Medikamentes zur Überprüfung von potenziellen Wechselwirkungen. Auch der Notfallmodus erscheint uns erwägenswert, jedenfalls mit entsprechenden Absicherungen wie etwa einer besonderen Begründungs- und Protokollierungspflicht.

[40] *SVR Gesundheit* (Fn. 4), S. 89 ff.

Mit Blick auf die Zugriffsdauer erscheint ein Datenschutz durch Voreinstellungen angebracht. Die Vorgaben in Deutschland und Österreich dürften insoweit grundsätzlich den Vorzug vor den Modellen Estlands und Spaniens verdienen, die keine vergleichbaren Voreinstellungen kennen.

VI. Fazit

Im Vergleich mit den Ausgestaltungen der Patientenaktensysteme in Österreich, Estland und Spanien und unter dem Eindruck von deren datenschutzrechtlicher Einordnung und Bewertung drängen sich Regelungsoptionen auf, die das deutsche Patientenaktensystem dem Ziel einer effizienten und effektiven, gleichzeitig aber auch informationssicheren Gesundheitsversorgung deutlich näherbringen könnten. Dies betrifft zumal die Einrichtung und Befüllung der Patientenakten sowie das Zugriffsmanagement. Belässt es der Gesetzgeber bei der gegenwärtigen Ausgestaltung, droht die ePA nicht nur zu einer für alle Beteiligten aufwändigen „Computerspielerei" zu werden. Vielmehr könnten auch die enormen Chancen, die eine ePA gerade für die zum Leitprinzip des deutschen Konzepts erhobene Patientensouveränität mit sich bringen könnte, im Einwilligungsdickicht des SGB V verloren gehen.

Der Ausblick auf die deutsche ePA fällt gleichwohl positiv aus. 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 ERezeptes 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 (optout). 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." Wie der Gesetzgeber den Opt-out umsetzt, ist damit zwar noch nicht entschieden. Wesentliche Gestaltungsoptionen zeigen sich indes – wie der vorliegende Beitrag gezeigt hat – bei einem Blick in das europäische Ausland.

Literatur

Albers, Marion: Art. 6 DSGVO, in: Wolff, Heinrich A./Brink, Stefan (Hrsg.), Beck'scher Online-Kommentar Datenschutzrecht, 41. Ed. (Stand 1. 11. 2021) 2021, München 2021.

Amelung, Volker E./*Binder*, Sebastian/*Bertram*, Nick/*Chase*, Daniela P./*Urbanski*, Dominika: Die elektronische Patientenakte – Fundament einer effektiven und effizienten Gesundheitsversorgung, in: Stiftung Münch (Hrsg.), Heidelberg 2017.

Artikel 29-Datenschutzgruppe (Hrsg.): Arbeitspapier zur Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA) – WP 131, Brüssel 2007.

Dochow, Carsten: Das Patienten-Datenschutz-Gesetz (Teil 2): Die elektronische Patientenakte und erweiterte Datenverarbeitungsbefugnisse der Krankenkassen, MedR 2021, S. 13 ff.

Dochow, Carsten: Grundlagen und normativer Rahmen der Telematik im Gesundheitswesen, Baden-Baden 2017.

Frenzel, Eike M.: Art. 6 DSGVO, in: Paal, Boris P./Pauly, Daniel A. (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz (DSGVO/BDSG), 3. Aufl. 2021, München 2021.

Frenzel, Eike M.: Art. 9 DSGVO, in: Paal, Boris P./Pauly, Daniel A. (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz (DSGVO/BDSG), 3. Aufl. 2021, München 2021.

Hansen, Marit: Art. 25 DSGVO, in: Simitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hrsg.), Datenschutzrecht. DSGVO mit BDSG, 2019, Baden-Baden 2019.

Herbst, Tobias: Art. 5 DSGVO, in: Kühling, Jürgen/Buchner, Benedikt (Hrsg.), Datenschutz-Grundverordnung, BDSG. Kommentar, 3. Aufl. 2020, München 2020.

Hornung, Gerrit: Die digitale Identität, Baden-Baden 2005.

Kampert, David: Art. 9 DSGVO, in: Sydow, Gernot (Hrsg.), Europäische Datenschutzgrundverordnung Handkommentar, 2. Aufl. 2018, Baden-Baden u. a. 2018.

Martini, Mario: Art. 24 DSGVO, in: Paal, Boris P./Pauly, Daniel A. (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz (DSGVO/BSG), 3. Aufl. 2021, München 2021.

Martini, Mario: Art. 25 DSGVO, in: Paal, Boris P./Pauly, Daniel A. (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz (DSGVO/BDSG), 3. Aufl. 2021, München 2021.

OEKONSULT gmbh (Hrsg.): Wie halten es die ÖsterreicherInnen mit ELGA?, ELGA-Studie, Baden 2014.

Petri, Thomas: Art. 9 DSGVO, in: Simitis; Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hrsg.), Datenschutzrecht. DSGVO mit BDSG, 2019, Baden-Baden 2019.

Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen (SVR Gesundheit) (Hrsg.): Digitalisierung für Gesundheit. Ziele und Rahmenbedingungen eines dynamisch lernenden Gesundheitssystems, Bonn 2021, verfügbar unter https://www.svr-gesundheit.de/fileadmin/Gutachten/Gutachten_2021/SVR_Gutachten_2021.pdf.

Schütz, Joachim/*Schmitz*, Sonja/*Ippach*, Jan: Die elektronische Patientenakte – Anforderungen aus Sicht des Datenschutzes, RDV 2019, S. 224 ff.

Thiel, Rainer/*Deimel*, Lucas/*Schmidtmann*, Daniel/*Piesche*, Klaus/*Hüsing*, Tobias/*Rennoch*, Jonas/*Stroetmann*, Veli/*Stroetmann*, Karl/*Kostera*, Thomas: #SmartHealthSystems. Digitalisierungsstrategien im internationalen Vergleich, in: Bertelsmann Stiftung (Hrsg.), Gütersloh 2018.

Weichert, Thilo: Die elektronische Gesundheitskarte, DuD 2004, S. 391 ff.