REDEKER | SELLNER | DAHS

Vereinbarkeit der Regelungen zur elektronischen Patientenakte (ePA) nach dem Patienten-Datenschutz-Gesetz (PDSG) mit europäischem Datenschutzrecht

Rechtsgutachten im Auftrag des health innovation hub

Erstattet durch:

Rechtsanwalt Dr. Cornelius Böllhoff
Rechtsanwalt Dr. Gero Ziegenhorn
Rechtsanwältin Dr. Stefanie Schulz-Große
Rechtsanwältin Dr. Samira Helena Thiery

Berlin, im November 2020

INHALTSVERZEICHNIS

A.
Zusammenfassung der Ergebnisse

Zur Granularität der Zugriffsmöglichkeiten, die Versicherte erteilen können:

1. Die Vorschriften des SGB V, die den Zugriff der Leistungserbringer auf die in der elektronischen Patientenakte (ePA) gespeicherten Daten gemäß § 341 Abs. 2 SGB V auf eine Einwilligung des Versicherten stützen, stehen im Einklang mit der DS-GVO. Das gilt für alle vorgesehenen Ausgestaltungen auf unterschiedlichen Umsetzungsstufen gem. § 342 Abs. 2 Nr. 1 lit. c und § 342 Abs. 2 Nr. 2 lit. b SGB V. Insbesondere fordert die DS-GVO nicht, dass die Versicherten ihre Einwilligungen auf Dokumentenebene („feingranular“) erteilen können.

2. Ein Verstoß gegen die Datenschutzgrundsätze der Zweckbindung, Datenminimierung, Erforderlichkeit und Vertraulichkeit liegt auch auf der ersten Umsetzungsstufe der ePA in 2021 nicht vor. Dementsprechend ist auch kein Verstoß gegen Art. 25 DS-GVO gegeben.

3. Die Sicherheit der Daten ist durch die Erteilung der Einwilligung in den Zugriff auf die ePA nicht beeinträchtigt. Die Erteilung der Zugriffsmöglichkeit betrifft allein Fragen der Freiwilligkeit der Einwilligung. Diese liegt hier vor. Deren Wirksamkeit beurteilt sich ausschließlich nach der DS-GVO und nicht nach der „Patientensouveränität“, die als politischer Begriff keinen rechtlichen Maßstab begründet.

4. Die ePA verlangt von den Betroffenen auch in der ersten Umsetzungsstufe keine Einwilligung in ein „Alles-oder-nichts“. Die Zugriffserteilung erfolgt nach dem Willen der Versicherten für alle oder nur für einzelne Leistungserbringer und kann individuell zeitlich begrenzt werden. Über diese Rechte werden die Patienten jeweils vor Erteilung der Einwilligung in die konkrete Datenverarbeitung informiert.

5. Ferner liegt in der unterschiedlichen Ausgestaltung des Berechtigungsmanagements von Frontend-Nutzern und Frontend-Nichtnutzern auf der zweiten Umsetzungsstufe kein Verstoß gegen Art. 3 Abs. 1 GG. Durch das mittelgranulare Berechtigungsmanagement auf der zweiten Umsetzungsstufe für Frontend-Nichtnutzer besteht zudem kein dem PDSG immanenter Wertungswiderspruch zu dem grundsätzlichen Anspruch einer barrierefrei versichertengeführten ePA.

Zu den Authentifizierungsanforderungen:

6. § 336 Abs. 2 Nr. 2 SGB V verstößt nicht gegen höherrangiges Recht. Weder aus der eIDAS-VO noch aus der DS-GVO ergibt sich eine Verpflichtung des Gesetzgebers, Ausführungen entsprechend den Definitionen der eIDAS-VO zum Sicherheitsniveau in das Gesetz aufzunehmen. Die Aufnahme der Formulierung eines „hohen Sicherheitsstandards“ in § 336 Abs. 2 Nr. 2 SGB V für die hiernach einzusetzenden Authentifizierungsverfahren stellt keinen Verstoß gegen höherrangiges Recht dar und ist seit Inkrafttreten des Gesetzes geltendes und anzuwendendes Recht.

7. Welche technischen und organisatorischen Maßnahmen zur Sicherheit der Datenverarbeitung getroffen und welche Garantien in die Verarbeitung selbst aufgenommen werden müssen, muss der Verantwortliche gemäß Art. 32 Abs. 1 und 2 bzw. Art. 25 Abs. 1 DS-GVO selbst ermitteln. Ggf. ist dies im Rahmen einer umfassenden Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO durchzuführen. In jedem Fall ergeben sich hieraus keine konkreten Maßnahmenvorgaben, sondern vielmehr eine Vorgehensweise, die der Verantwortliche einhalten muss, um selbst notwendige Maßnahmen zu ermitteln. Die DS-GVO verpflichtet ihn (nur) hierzu sowie die so ermittelten Maßnahmen dann auch zu treffen. Konkrete technische und organisatorische Maßnahmen oder konkrete Arten solcher Maßnahmen sind insofern nicht vorgeschrieben. Der Verantwortliche ist (nur) gehalten, praktisch realisierbare Maßnahmen umzusetzen, die ein angemessenes Schutzniveau garantieren.

B. Sachverhalt

Der Deutsche Bundestag hat am 03.07.2020 das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz – „PDSG“) beschlossen, das am 20.10.2020 in Kraft getreten ist.[1] Fokus dieser Gesetzgebung ist die elektronische Patientenakte („ePA“), die bereits nach bisheriger Rechtslage in § 291a Abs. 3 Nr. 4 und Absatz 5c Satz 4 bis 6 SGB V a.F. vorgesehen war.[2] Die ePA soll weiterentwickelt und hinsichtlich ihrer Inhalte, ihrer Nutzung, der Verarbeitungsbefugnisse und der Zugriffskonzeption in einen neuen rechtlichen Rahmen gestellt werden.

Im Gesetzgebungsverfahren wurde durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) sowie einige Datenschutz-Aufsichtsbehörden der Länder bereits Kritik formuliert. Vor einer näheren Beschreibung dieser Kritikpunkte, die sowohl hinsichtlich der Art und Weise des Vorgehens der Aufsichtsbehörden als auch hinsichtlich ihres Inhalts näher zu beleuchten sind, sollen im Folgenden die Vorschriften zur ePA im PDSG und insbesondere die Möglichkeiten des Zugriffs hierauf näher dargelegt werden (nachfolgend Abschnitt I.). Dem folgt ein kurzer Überblick über die Regelung von Authentifizierungsanforderungen (nachfolgend Abschnitt II.) und zur datenschutzrechtlichen Verantwortlichkeit sowie den konkret Betroffenen (nachfolgend Abschnitt III.).

Die von den Datenschutz-Aufsichtsbehörden geäußerte Kritik wird sodann in Abschnitt IV. dargestellt.

I. Vorschriften zur elektronischen Patientenakte (ePA) in der Fassung des PDSG

Die ePA ist eine wesentliche Anwendung der Telematikinfrastruktur („TI“). Hierbei handelt es sich um eine digitale Informations-, Kommunikations- und Sicherheitsinfrastruktur, die der sicheren, schnellen, sektorenübergreifenden und, soweit erforderlich, barrierefreien Kommunikation von Leistungserbringern, Kostenträgern, Versicherten und weiteren Akteuren des Gesundheitswesens dient. Für eine bessere digitale Kommunikation zwischen Leistungserbringern und Patienten, zur Erleichterung der Abläufe im Behandlungsalltag sowie zur qualitativen Verbesserung der medizinischen Versorgung wurde mit dem PDSG im SGB V ein eigener Titel zur ePA geschaffen

---

1 Gesetz vom 14.10.2020 (BGBl. I Nr. 46, S. 2115).

2 § 291a Abs. 3 Nr. 4 SGB V in der bis zum Inkrafttreten des PDSG geltenden Fassung (SGB V a.F.).

(Zweiter Titel, §§ 341 ff. SGB V in der seit Inkrafttreten des PDSG geltenden Fassung, im Folgenden: SGB V).

1. Nutzung und Inhalte der ePA

Gemäß § 341 Abs. 1 SGB V ist die ePA eine versichertengeführte elektronische Akte, die den Versicherten auf Antrag zur Verfügung gestellt wird und deren Nutzung für jeden einzelnen Versicherten freiwillig ist. In § 341 Abs. 2 SGB V heißt es weiter:

> „Mit ihr [der ePA, Anm. d. Verf.] sollen den Versicherten auf Verlangen Informationen, insbesondere zu Befunden, Diagnosen, durchgeführten und geplanten Therapiemaßnahmen sowie zu Behandlungsberichten, für eine einrichtungs-, fach- und sektorenübergreifende Nutzung für Zwecke der Gesundheitsversorgung, insbesondere zur gezielten Unterstützung von Anamnese und Befunderhebung, barrierefrei elektronisch bereitgestellt werden“.

§ 341 Abs. 2 SGB V regelt enumerativ die Daten, die in die ePA eingestellt werden dürfen. Diese sind unter anderem:

- medizinische Informationen über den Versicherten, insbesondere Daten zu Befunden, Diagnosen, durchgeführten und geplanten Therapiemaßnahmen, Früherkennungsuntersuchungen, Behandlungsberichten und sonstige untersuchungs- und behandlungsbezogene medizinische Informationen (Nr. 1), sowie

- Gesundheitsdaten, die durch den Versicherten zur Verfügung gestellt werden (Nr. 6).

In der Gesetzesbegründung zu § 341 Abs. 2 SGB V heißt es:

> „Ziel ist es zum einen, die in die Behandlung der Versicherten einbezogenen Leistungserbringer im Bedarfsfall bestmöglich über Vorerkrankungen und vorliegende Befunddaten der Versicherten zu informieren. Im Rahmen der Anamnese und Befunderhebung hat der Behandelnde die für die geplante Behandlung wesentlichen Umstände, insbesondere auch Vorbefunde, in Erfahrung zu bringen. Das geschieht zurzeit durch Befragung des

> Versicherten oder seiner Angehörigen und Anforderung fachärztlicher Befunde mit Einverständnis des Patienten. Die elektronische Patientenakte ermöglicht es den Leistungserbringern, basierend auf Anamnese und Befunderhebung und je nach z. B. Komplexität und Dringlichkeit des medizinischen Problems, gezielt ergänzende Vorinformationen einzusehen und unterstützt die Leistungserbringer dadurch bei der Auswahl der für die Versicherten geeigneten medizinischen Behandlung.
>
> Zum anderen sollen auch die Versicherten besser über ihre Gesundheitsdaten informiert werden und dadurch ihre medizinische Behandlung besser begleiten können.
>
> Die elektronische Patientenakte ist eine versichertengeführte Akte. Das heißt, dass der Versicherte bestimmt, welche Dokumente bzw. Datensätze im Einzelnen in der elektronischen Patientenakte gespeichert oder gelöscht werden und wer diese Daten mit Einwilligung des Versicherten in der elektronischen Patientenakte auslesen und in lokalen Datenverwaltungssystemen zur weiteren Verwendung speichern oder auch unmittelbar in der elektronischen Patientenakte verarbeiten darf".

Das Gesetz intendiert somit eine sehr weitgehende und über das unionrechtlich gebotene Mindestmaß hinausgehende Selbstbestimmung der Versicherten über ihre Daten. Weder die Nutzung der ePA noch die Erteilung eines Zugriffs auf darin gespeicherte Daten dürfen von den Versicherten verlangt werden. Insofern ist in § 335 SGB V ein Diskriminierungsverbot normiert, nach dessen Abs. 3 Versicherte nicht bevorzugt oder benachteiligt werden dürfen, weil sie die ePA nutzen oder nicht nutzen und den Leistungserbringern Zugriff auf den Akteninhalt gewähren oder verweigern. Der behandelnde Leistungserbringer darf sich nicht allein auf die Vollständigkeit der ePA verlassen. Ihn trifft vielmehr nach wie vor die Pflicht, die für die geplante Behandlung wesentlichen Umstände, insbesondere auch Vorbefunde, in Erfahrung zu bringen. Ferner haben Patienten nach wie vor die Möglichkeit, dem jeweiligen Leistungserbringer Dokumente zu Vorbefunden und Diagnosen analog, in Papierform zur Verfügung zu stellen.

Flankiert wird dieser Grundsatz der Selbstbestimmung von einem Einwilligungsgebot: § 344 Abs. 1 SGB V sieht vor, dass die Krankenkassen nur dann eine ePA einrichten und die dafür erforderlichen administrativen personenbezogenen Daten verarbeiten dürfen, wenn der jeweilige Versicherte wirksam einwilligt. Hat sich der Versicherte für eine ePA entschieden, hat er gegenüber dem behandelnden Leistungserbringer regelmäßig einen Anspruch darauf, dass Daten, soweit diese im Rahmen der vertragsärztlichen Versorgung bei der Behandlung des Versicherten elektronisch verarbeitet werden, in der ePA gespeichert werden (§§ 346 – 349 SGB V).

Spiegelbildlich ist der Versicherte gemäß § 337 Abs. 2 SGB V berechtigt, in der ePA gespeicherte Daten eigenständig zu löschen. Alternativ müssen Daten in der ePA auf Verlangen des Versicherten jedenfalls durch die zugriffsberechtigten Leistungserbringer gelöscht werden. Ferner kann der Versicherte gemäß § 344 Abs. 3 SGB V gegenüber seiner Krankenkasse jederzeit die vollständige Löschung seiner ePA verlangen.

2. Zugriff auf Daten durch Leistungserbringer

Die potentiell Zugriffsberechtigten sind in einem Katalog in § 352 SGB V enumerativ aufgeführt. Dabei handelt es sich insbesondere um Ärzte, Zahnärzte, Psychotherapeuten, Gesundheits-, Kranken- und Altenpfleger, die zur Versorgung der Versicherten in die Behandlung eingebunden sind, sowie Apotheker, Hebammen und Physiotherapeuten. Außerdem sind Personen potentiell zugriffsberechtigt, die als berufsmäßige Gehilfen oder zur Vorbereitung auf den Beruf tätig sind oder deren Zugriff im Rahmen der von ihnen zulässigerweise zu erledigenden Tätigkeiten erforderlich ist und unter Aufsicht des jeweiligen Leistungserbringers erfolgt.

§ 339 Abs. 1 i.V.m. § 353 SGB V regelt, dass potentiell zugriffsberechtigte Leistungserbringer und andere zugriffsberechtigte Personen auf die Gesundheitsdaten der Versicherten nur zugreifen dürfen, soweit der Versicherte auch hierzu – mittels einer eindeutigen bestätigenden Handlung durch technische Zugriffsfreigabe – seine vorherige Einwilligung erteilt hat.

Es sind mithin zwei Arten von Einwilligungen vorgesehen – einerseits Einwilligungen in die Einrichtung und die dafür erforderliche Verarbeitung administrativer personenbezogener Daten durch die Krankenkassen (siehe oben 1.) und andererseits Einwilligungen in den Zugriff auf die in der ePA gespeicherten Gesundheitsdaten durch die jeweiligen Leistungserbringer (sowie ggf. deren berufsmäßige Gehilfen und dgl.).

Zusätzlich zum Erfordernis einer Einwilligung des Versicherten dürfen gem. den in § 352 SGB V enthaltenen Vorgaben die dort aufgeführten Leistungserbringer, denen gegenüber eingewilligt wurde, nur auf die in der ePA gespeicherten Daten zugreifen, soweit dies für die Versorgung der Versicherten *erforderlich* ist. Werden Dokumente in der ePA mithin für die Aufgabenerfüllung des jeweiligen Leistungserbringers nicht benötigt, ist es ihm untersagt, darauf zuzugreifen (auch wenn der Patient ihm dies durch Erteilung seiner Einwilligung gestattet hat). Gemäß § 339 Abs. 3 SGB wird zum Zwecke des Nachweises eines möglichen Missbrauchs elektronisch protokolliert, wer auf die Daten zugegriffen hat und auf welche Daten zugegriffen wurde. Der Zugriff durch den Leistungserbringer oder eine andere zugriffsberechtigte Person erfordert gemäß § 339 Abs. 3 SGB V den Einsatz der elektronischen Gesundheitskarte durch den Versicherten. Weiterhin erfordert der Zugriff der Leistungserbringer oder einer anderen zugriffsberechtigten Person einen ihrer Berufszugehörigkeit entsprechenden elektronischen Heilberufsausweis in Verbindung mit einer Komponente zur Authentifizierung von Leistungserbringerinstitutionen. Abweichend hiervon kann der Leistungserbringer gemäß § 339 Abs. 4 SGB V nur auf die Daten zugreifen, wenn der Versicherte in diesen Zugriff über eine Benutzeroberfläche eines geeigneten Endgeräts eingewilligt hat [dazu sogleich unter a)].

Die Art und Weise der Nutzung und insbesondere der Zugriffsberechtigungserteilung durch den Versicherten divergiert zunächst in Abhängigkeit von der Umsetzungsstufe der ePA, da aus technischen Gründen mit Einführung der ePA zum 1. Januar 2021 noch nicht sämtliche Funktionen zur Verfügung stehen werden, die es zukünftig geben wird. Die Funktionen werden vielmehr sukzessive erweitert. Auf allen Umsetzungsstufen werden den Versicherten jedoch jeweils bestimmte Beschränkungsmöglichkeiten eröffnet.

Weiterhin unterscheidet das Gesetz mit Blick auf die Zugriffsberechtigungserteilung zwischen Versicherten, die über die Benutzeroberfläche eines geeigneten Endgeräts über eine App auf die ePA zugreifen (sog. Frontend-Nutzer) und Versicherten, die keine Benutzeroberfläche eines geeigneten Endgeräts nutzen können oder wollen (sog. Frontend-Nichtnutzer).

Im Einzelnen gestaltet sich dies wie folgt:

a) Berechtigungsmanagement auf der ersten Umsetzungsstufe
(1. Januar 2021 bis 31. Dezember 2021)

Auf der ersten Umsetzungsstufe gelten mit Blick auf die Zugriffsberechtigungserteilung für Frontend-Nutzer und -Nichtnutzer dieselben Bedingungen.

Gemäß § 342 Abs. 2 Nr. 1 lit. c SGB V muss die ePA auf der ersten Umsetzungsstufe gewährleisten, dass die Frontend-Nutzer mittels ihres Endgeräts und die Frontend-Nichtnutzer mittels einer dezentralen Infrastruktur der Leistungserbringer eine Einwilligung in den Zugriff durch zugriffsberechtigte Leistungserbringer auf Daten in der ePA insgesamt abgeben können. Außerdem müssen sie in den Zugriff entweder ausschließlich auf Daten nach § 341 Abs. 2 Nr. 1 SGB V (medizinische Informationen über den Versicherten) oder auf Daten nach § 341 Abs. 2 Nr. 6 (Gesundheitsdaten, die durch den Versicherten zur Verfügung gestellt werden) einwilligen können. Bei der dezentralen Infrastruktur der Leistungserbringer handelt es sich um den Konnektor und das Kartenlesegerät, das die Versicherten mithilfe ihrer elektronischen Gesundheitskarte und PIN-Eingabe nutzen können.

Gemäß § 342 Abs. 2 Nr. 1 lit. e SGB V ist – wiederum für Frontend-Nutzer und - Nichtnutzer – durch eine entsprechende technische Voreinstellung die Dauer der Zugriffsberechtigung für den Leistungserbringer standardmäßig auf eine Woche beschränkt. Der Versicherte kann aber im Einzelfall gemäß § 342 Abs. 2 Nr. 1 lit. f SGB V eine andere Einstellung vornehmen und die Dauer der Zugriffsberechtigung zwischen einem Tag bis höchstens 18 Monaten festlegen.

b) Berechtigungsmanagement auf der zweiten Umsetzungsstufe
(1. Januar 2022 bis 31. Dezember 2022)

Abweichend von der ersten Umsetzungsstufe können auf der zweiten Umsetzungsstufe, die am 1. Januar 2022 beginnt, sowohl Frontend-Nutzer als auch Frontend-Nichtnutzer gemäß § 342 Abs. 2 Nr. 2 lit. f SGB V die Dauer der Zugriffsberechtigung frei festlegen. Die Berechtigung muss mindestens einen Tag andauern und kann auch unbefristet sein.

Mit Blick auf die Zugriffsberechtigungserteilung bestehen auf der zweiten Umsetzungsstufe für Frontend-Nutzer und -Nichtnutzer unterschiedliche Regelungen:

Frontend-Nutzer sollen eine Einwilligung in den Zugriff gemäß § 342 Abs. 2 Nr. 2 lit. b SGB V sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen in der ePA erteilen können (sog. feingranulares Berechtigungsmanagement). Gruppen von Dokumenten sind etwa von einem bestimmten Autor erstellte Dokumente, bestimmte Dokumentarten (wie zum Beispiel Entlassungsbriefe, OP-Berichte oder Medikationsangaben) oder Dokumente mit bestimmten Erstellungs- oder Änderungsdaten.

Frontend-Nichtnutzer haben demgegenüber zwei Optionen, die Zugriffsberechtigungserteilung durchzuführen:

- Gemäß § 342 Abs. 2 Nr. 2 lit. c SGB V haben sie einerseits die Möglichkeit, den Zugriffsberechtigten mittels der dezentralen Infrastruktur der Leistungserbringer eine Einwilligung in den Zugriff mindestens auf Kategorien von Dokumenten und Datensätzen zu erteilen. Bei diesen Kategorien handelt es sich um medizinische Fachgebietskategorien, sodass Versicherte beispielsweise bestimmen können, dass ein Orthopäde lediglich Zugriff auf orthopädische medizinische Informationen erhalten kann (sog. mittelgranulares Berechtigungsmanagement).

- Andererseits steht den Frontend-Nichtnutzern gem. § 342 Abs. 2 Nr. 2 lit. b SGB V ebenfalls das feingranulare Berechtigungsmanagement zur Verfügung, wenn sie dazu einen Vertreter ermächtigen, der über die Benutzeroberfläche eines geeigneten Endgeräts verfügt.

Frontend-Nichtnutzer haben also, wenn sie keinen Vertreter bevollmächtigen, weniger Möglichkeiten bei der Einstellung von Zugriffsberechtigungen (dem sog. Berechtigungsmanagement) als Frontend-Nutzer. Angesichts dessen verpflichtet § 338 Abs. 2 SGB V die Gesellschaft für Telematik, bis zum Ende der zweiten Umsetzungsstufe zu evaluieren, ob zusätzlich zur Vertreterregelung Bedarf für eine flächendeckende Schaffung technischer Einrichtungen durch die Krankenkassen in ihren Geschäftsstellen besteht, die das feingranulare Erteilen von Zugriffsberechtigungen auf Daten in der ePA ermöglichen. Darüber hinaus wird die Gesellschaft für Telematik in § 354 Abs. 1 Nr. 5 SGB V verpflichtet, die Voraussetzungen dafür zu schaffen, dass die Möglichkeiten der Frontend-Nichtnutzer zur Zugriffsfreigabe unter Berücksichtigung der Verhältnismäßigkeit des dafür erforderlichen Aufwandes an die Möglichkeiten der feingranularen Zugriffsfreigabe nach § 342 Abs. 2 Nr. 2 lit. b) SGB V angeglichen werden.

3. Informationspflichten gegenüber den Versicherten

Krankenkassen und Leistungserbringer müssen nach dem PDSG jeweils gewisse Informationspflichten gegenüber den Versicherten erfüllen. Diese unterscheiden sich wiederum nach der Umsetzungsstufe und danach, ob es sich bei den Versicherten um Frontend-Nutzer oder Frontend-Nichtnutzer handelt.

a) Krankenkassen

Umfassende Informationspflichten sieht § 343 SGB V vor. Nach dessen Abs. 1 haben die Krankenkassen den Versicherten, bevor sie ihnen eine ePA anbieten, umfassendes, geeignetes Informationsmaterial über die ePA in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache und barrierefrei zur Verfügung zu stellen. Er muss über alle relevanten Umstände der Datenverarbeitung für die Einrichtung der ePA, die Übermittlung von Daten in die ePA und die Verarbeitung von Daten in der ePA durch Leistungserbringer einschließlich der damit verbundenen Datenverarbeitungsvorgänge in den verschiedenen Bestandteilen der Telematikinfrastruktur und über die für die Datenverarbeitung datenschutzrechtlich Verantwortlichen informiert werden. Es ist insbesondere zu informieren über:

- die Freiwilligkeit der ePA und das Recht auf jederzeitige teilweise oder vollständige Löschung (Nr. 3),
- das Erfordernis der vorherigen Einwilligung in die Datenverarbeitung in der ePA gegenüber Krankenkassen, Anbietern und Leistungserbringern sowie die Möglichkeit des Widerrufs der Einwilligung (Nr. 4),
- die Voraussetzungen für den Zugriff von Leistungserbringern auf Daten in der ePA und die Verarbeitung dieser Daten durch die Leistungserbringer (Nr. 10),
- die Möglichkeit, bei der Datenverarbeitung nach Nr. 10 beim Leistungserbringer durch technische Zugriffsfreigabe in die konkrete Datenverarbeitung einzuwilligen (Nr. 11),
- die fehlende Möglichkeit, vor dem 1. Januar 2022 die Einwilligung sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA nach § 342 Abs. 2 Nr. 2 lit. b SGB V zu beschränken (Nr. 12),

- die fehlende Möglichkeit, die Einwilligung mittels der dezentralen Infrastruktur der Leistungserbringer auf spezifische Dokumente und Datensätze zu beschränken (Nr. 13),

- die Möglichkeit, ab dem 1. Januar 2022 über die Benutzeroberfläche eines geeigneten Endgeräts einem Vertreter die Befugnis zu erteilen, die Rechte des Versicherten im Rahmen der Führung seiner ePA innerhalb der erteilten Vertretungsbefugnis wahrzunehmen (Nr. 19).

Über diese allgemeinen Informationspflichten hinaus sieht § 342 Abs. 2 Nr. 1 lit. g SGB V vor, dass die Frontend-Nutzer bis einschließlich 31. Dezember 2021 *jeweils bei ihrem Zugriff* auf die ePA vor der Speicherung eigener Dokumente auf die fehlende Möglichkeit hingewiesen werden müssen, die Einwilligung zum Zugriff durch zugriffsberechtigte Leistungserbringer sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen zu beschränken. § 342 Abs. 2 Nr. 1 lit. h SGB V schreibt darüber hinaus vor, dass die Frontend-Nutzer bis einschließlich 31. Dezember 2021 *vor Erteilung einer Einwilligung* in den Zugriff durch zugriffsberechtigte Leistungserbringer auf die fehlende Möglichkeit hingewiesen werden, die Zugriffsberechtigung sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der elektronischen Patientenakte zu beschränken.

b) Leistungserbringer

Die Leistungserbringer treffen gemäß § 353 Abs. 2 Nr. 2 SGB V Informationspflichten gegenüber jedem Frontend-Nichtnutzer. Vor dessen Einwilligung in einen konkreten Datenzugriff ist der Leistungserbringer verpflichtet, ihn über die fehlende Möglichkeit der Beschränkung der Zugriffsrechte nach § 342 Abs. 2 Nr. 2 lit. b SGB V und die Bedeutung der Zugriffsberechtigung auf Kategorien von Dokumenten und Datensätzen nach § 342 Abs. 2 Nr. 2 lit. c SGB V zu informieren.

II. Regelung von Authentifizierungsanforderungen

Mit dem PDSG wurden auch allgemeine Vorschriften zu den Anwendungen der Telematikinfrastruktur in das SGB V eingefügt, namentlich als Erster Titel (§§ 334–340 SGB V) des Fünften Abschnitts, welcher insgesamt die Anwendungen der Telematikinfrastruktur regelt. 336 SGB V regelt die Zugriffsrechte der Versicherten auf einzelne Anwendungen der Telematikinfrastruktur. Die Vorschrift lautet:

> „(1) Jeder Versicherte ist berechtigt, auf Daten in einer Anwendung nach § 334 Absatz 1 Satz 2 Nummer 1 bis 3 und 6 mittels seiner elektronischen Gesundheitskarte barrierefrei zuzugreifen, wenn er sich für diesen Zugriff jeweils durch ein geeignetes technisches Verfahren authentifiziert hat."

Zu den Anwendungen, für die dies gilt, gehört insbesondere die ePA gemäß § 334 Abs. 1 Satz 2 Nr. 1 SGB V.[3]

Es ist hiernach also unter den genannten Voraussetzungen jeder Versicherte berechtigt, mittels seiner elektronischen Gesundheitskarte („eGK") auf seine ePA zuzugreifen.

Darüber hinaus besteht nach § 336 Abs. 2 SGB V die Möglichkeit des Zugriffs auf die ePA für jeden Versicherten auch ohne Verwendung der elektronischen Gesundheitskarte. Diese Vorschrift lautet:

> „(2) Jeder Versicherte ist berechtigt, auf Daten in einer Anwendung nach § 334 Absatz 1 Satz 2 Nummer 1 [das ist die ePA; Hinweis d. Verf.] auch ohne den Einsatz seiner elektronischen Gesundheitskarte mittels einer Benutzeroberfläche eines geeigneten Endgeräts zuzugreifen, wenn
> […]
> 2. der Versicherte sich für diesen Zugriff auf Daten in einer Anwendung nach § 334 Absatz 1 Satz 2 Nummer 1 [die ePA; Hinweis d. Verf.] jeweils durch ein geeignetes technisches Verfahren, das einen hohen Sicherheitsstandard gewährleistet, authentifiziert hat."

[3] Der ebenfalls in Bezug genommene § 334 Abs. 1 Satz 2 Nr. 2 SGB V n.F. betrifft die Erklärungen und diesbezügliche Aufbewahrungsorthinweise der Versicherten zu Organ- und Gewebespenden und § 334 Abs. 1 Satz 2 Nr. 3 SGB V n.F. die Hinweise der Versicherten zum Vorhandensein und zum Aufbewahrungsort von Versorgungsvollmachten und Patientenverfügungen nach § 1901a BGB und nach § 334 Abs. 1 Satz 2 Nr. 6 SGB V n.F. elektronische Verordnungen.

Im Sinne einer Stärkung der Patientensouveränität[4] bezwecken diese Anforderungen an die einzusetzenden technischen Verfahren, dem hohen Schutzbedarf der verarbeiteten Daten – Authentifizierungs- und Gesundheitsdaten – gerecht zu werden.[5]

Was konkret unter einem „hohen Sicherheitsstandard" im Sinne des § 336 Abs. 2 Nr. 2 SGB V zu verstehen ist, wird nicht explizit geregelt. Insbesondere sieht das Gesetz selbst keine konkreten Maßnahmen vor, die als „geeignetes technisches Verfahren" gelten. Die Gesetzesbegründung enthält hierzu aber den Hinweis, dass „beispielsweise eine Zwei-Faktor-Authentifizierung ein hinreichendes Schutzniveau gewährleisten" kann.[6]

III. Datenschutzrechtliche Verantwortlichkeit und Betroffene

Zugriffe und diesbezügliche Authentifizierungen nach dem PDSG fallen in den Anwendungsbereich der DS-GVO sowie unter die besonderen zum Sozialdatenschutz.

Die Krankenkassen verarbeiten mit der ePA personenbezogene Daten der Betroffenen. Personenbezogene Daten sind gem. Art. 4 Nr. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt identifiziert werden kann. Bei den hier konkret verarbeiteten personenbezogenen Daten handelt es sich einerseits um sogenannte Stammdaten, d.h. beispielsweise Name und Adressdaten, und andererseits um Daten, die einen Bezug zur Gesundheit aufweisen und in der DS-GVO nach Art. 9 DS-GVO besonders geschützt werden. Da die personenbezogenen Daten hier durch einen Leistungsträger i.S.d. § 35 Abs. 1 SGB I, die Krankenkassen, verarbeitet werden, handelt es sich nach der Definition in § 67 Abs. 2 Satz 1 SGB X auch um sog. Sozialdaten.

Für jede datenschutzrechtliche Bewertung kommt es zentral darauf an, wer gemäß Art. 4 Nr. 7 DS-GVO diejenige Stelle ist, die über Mittel und Zwecke einer Datenverarbeitung entscheidet. Im SGB V ist die datenschutzrechtliche Verantwortlichkeit der elektronischen Patientenakte (ePA) festgelegt worden, was unionsrechtlich gemäß Art. 4 Nr. 7 HS 2 DS-GVO zulässig ist, wenn Mittel und Zwecke vom mitgliedstaatlichen Recht festgelegt werden. Näheres findet sich hierzu in § 307 SGB V. Danach

---

4 BT-Drs. 19/18793, S. 108.
5 BT-Drs. 19/18793, S. 109.
6 BT-Drs. 19/18793, S. 109.

orientiert sich die Zuweisung der Verantwortlichkeit, die für die ePA als Anwendung der Telematikinfrastruktur (§ 334 Abs.1 Nr. 1 SGB V) gilt, an den für die jeweilige Stelle überblickbaren und beherrschbaren Strukturen. Jeder Verantwortliche ist für den Bereich zuständig, in dem er über die konkrete Datenverarbeitung entscheidet.[7]

Die Krankenkassen, die ihren Patienten die ePA zur Verfügung stellen, sind als Anbieter eines Dienstes der Anwendungsinfrastruktur nach §§ 307 Abs. 4, 341 Abs. 4 SGB V

> „die für die Verarbeitung der Daten zum Zweck der Nutzung der elektronischen Patientenakte Verantwortlichen nach Artikel 4 Nummer 7 der Verordnung (EU) 2016/679."

Die Leistungserbringer sind wiederum für die Verarbeitung der Gesundheitsdaten der Versicherten mittels der in ihrer Umgebung genutzten Komponenten der dezentralen Infrastruktur im Sinne des § 306 Abs. 2 Nr. 1 SGB V verantwortlich. Die Verantwortlichkeit erstreckt sich schwerpunktmäßig auf die Sicherstellung der bestimmungsgemäßen Nutzung der Komponenten, deren ordnungsgemäßen Anschluss und die Durchführung der erforderlichen fortlaufenden Software-Updates.[8]

Um zur Gewährleistung der Betroffenenrechte eine lückenlose datenschutzrechtliche Verantwortlichkeit zu garantieren, enthält § 307 Abs. 5 SGB V eine Art von Auffangverantwortlichkeit der Gesellschaft für Telematik, die stets dann greift, wenn sich aus den vorherigen Absätzen des § 307 SGB V keine spezielle Verantwortlichkeit ergibt. Inhaltlich orientiert sich die Verantwortlichkeit an dem Aufbau der TI (§ 306 Absatz 2 SGB V).

Nach den Art. 12 ff. DS-GVO ist der Verantwortliche für die Einhaltung der Rechte der Betroffenen (z.B. Informationspflichten, Auskunfts- und Löschungsrechte, etc.) verantwortlich und zuständiger Ansprechpartner, wenn Betroffene eine Verletzung ihrer personenbezogenen Daten vermuten. Zur Gewährleistung hoher Transparenz für die Betroffenen enthält § 307 Abs. 5 S. 2 SGB V den Auftrag an die Gesellschaft für Telematik, eine koordinierende Stelle für Betroffenen einzurichten, um die Wahrnehmung von Betroffenenrechten nach der DS-GVO lückenlos zu ermöglichen.

---

7 BR-Drs. 164/20, S. 108.
8 BR-Drs. 164/20, S. 108 f.

IV. Kritik von Datenschutz-Aufsichtsbehörden am PDSG und Ankündigung von Aufsichtsmaßnahmen

1. Vereinbarkeit der Zugriffserteilungsmöglichkeiten des § 342 Abs. 2 Nr. 1 lit. c und Nr. 2 lit. c SGB V mit deutschem und europäischen Datenschutzrecht

Der BfDI kritisiert die Regelung der Erteilung von Zugriffsmöglichkeiten auf Daten der ePA in § 342 Abs. 2 Nr. 1 lit. c und Nr. 2 lit. c SGB V[9]. Zugriffe dürfen hiernach nur aufgrund einer Einwilligung des Patienten erfolgen. Weil nach dieser Regelung der Versicherte Zugriffsmöglichkeiten in bestimmten Fallkonstellationen nur mittelgranular erteilen kann – namentlich im Hinblick auf Kategorien von Dokumenten und Datensätzen der ePA –, nicht aber spezifischer, etwa für ein einzelnes Dokument in der ePA (z.B. einen bestimmten Arztbericht), sei der Patient im Grunde gezwungen, zwischen ganz oder gar nicht zu entscheiden, wenn er einwilligt oder nicht. Aus den Aussagen des BfDI lässt sich folgern, dass die Datenschutz-Aufsichtsbehörden die Freiwilligkeit der Einwilligungen bezweifeln und sie insofern für unionsrechtswidrig und mithin unwirksam halten. § 342 Abs. 2 Nr. 1 lit. c und Nr. 2 lit. c SGB V verstießen daher ihrerseits gegen höherrangiges Recht.

Vergleichbar positioniert sich auch die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) in einer Entschließung vom 01.09.2020[10], in der sie ausführt, im Jahr 2021 seien Nutzende der ePA gleichsam nach einem „alles-oder-nichts-Prinzip“ gezwungen, die Daten den Leistungserbringern ohne weitere Einschränkung zur Verfügung zu stellen, auch wenn dies für die konkrete Behandlungssituation nicht erforderlich sei.

Der BfDI beschränkte sich in einer Warnung nach Art. 58 Abs. 2 lit. a DS-GVO vom 06.11.2020 seine an die Krankenkassen in seinem Zuständigkeitsbereich auf die Frage der ausreichenden technischen und organisatorischen Maßnahmen i.S.v. Art. 25 DS-GVO. Die in der ersten Ausbaustufe in 2021 vorgesehene Granularität des Berechtigungsmanagements entspreche nicht dem Stand der Technik und verstoße somit gegen Art. 25 DS-GVO sowie diverse Datenschutzgrundsätze in Art. 5 DS-GVO. Zudem ist

---

9 Vgl. Pressemitteilung des BfDI vom 19.08.2020 „BfDI zu Folgen der Gesetzgebung des PDSG“, abrufbar unter: https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2020/20_BfDI-zu-PDSG.html;jsessionid=6DA481ADC850BAA269AB23777326DFB6.1_cid319, zuletzt aufgerufen am 18.11.2020.

10 Entschließung der Konferenz der unabhängigen Datenschutz-Aufsichtsbehörden des Bundes und der Länder vom 01.09.2020, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/20200901_PDSG_Entschlie%C3%9Fung.pdf, zuletzt aufgerufen am 04.11.2020.

er der Ansicht, dass ein Wertungswiderspruch bestehe, der sich im Hinblick auf eine Benachteiligung derjenigen Versicherten ergebe, die nicht über ein geeignetes Endgerät verfügten.

2. Vereinbarkeit der Authentifizierungsanforderungen in § 336 Abs. 2 Nr. 2 SGB V mit deutschem und europäischen Datenschutzrecht

Die Regelung in § 336 Abs. 2 Nr. 2 SGB V, die eine Authentifizierung durch ein geeignetes technisches Verfahren vorschreibt, das einen hohen Sicherheitsstandard gewährleistet, wird vom BfDI ebenfalls kritisiert.[11]

Der Begriff sei zu unbestimmt und würde insbesondere der Verarbeitung besonders sensibler Gesundheitsdaten nicht gerecht.[12] Es bedürfe daher einer Konkretisierung durch den Gesetzgeber, bestenfalls durch die unmittelbare Anwendung der eIDAS-Verordnung[13], der Durchführungsverordnung (EU) 2015/1502 zur eIDAS-Verordnung und der Technischen Richtlinien des Bundesamts für Sicherheit in der Informationstechnik (BSI). Diese würden auf international anerkannten Standards beruhen und ihre Erfüllung entspreche dem Stand der Technik, sodass sie technologieneutral Anwendung fänden.[14]

Der BfDI ist darüber hinaus der Ansicht, aus höherrangigem Recht folge, dass diese Standards und insbesondere der Standard der europäischen eIDAS-Verordnung auf dem Niveau „hoch“ eingehalten werden müssen. Dies müsse daher auch § 336 Abs. 2 Nr. 2 SGB V so vorsehen.[15]

---

11 Der BfDI beruft sich dazu auch auf eine Stellungnahme des Chaos Computer Clubs, der eine ähnliche Auffassung vertritt, vgl. Stellungnahme des BfDI vom 09.06.2020 (Patientendaten-Schutz-Gesetz (PDSG) - BT-Drs. 19/18793; Formulierungshilfen für Änderungsanträge), S. 7.

12 Vgl. Dt. Bundestag, Ausschuss f. Gesundheit, Ausschussdrucksache 19(14)169 vom 25.05.2020, zweite Stellungnahme zum Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur, S. 10.

13 Vgl. Dt. Bundestag, Ausschuss f. Gesundheit, Ausschussdrucksache 19(14)169 vom 25.05.2020, zweite Stellungnahme zum Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur, S. 2; Stellungnahme des BfDI im Rahmen der Ressortabstimmung zum Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutzgesetz-PDSG) vom 20.02.2020, S. 11.

14 Vgl. Dt. Bundestag, Ausschuss f. Gesundheit, Ausschussdrucksache 19(14)169 vom 25.05.2020, zweite Stellungnahme zum Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur, S. 10; dazu auch MinR Raum, Video-Fachtagung, Datenschutz in der Medizin- Update 2020“ vom 4. November 2020, Folie 13.

15 Vgl. Stellungnahme des BfDI im Rahmen der Ressortabstimmung zum Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutzgesetz-PDSG) vom 20.02.2020, Geschäftszeichen 21-400-5/001#0001, S. 11.

In eine ähnliche Richtung zielt die Kritik der DSK in der Entschließung vom 01.09.2020[16]: Da es sich bei den Daten um Gesundheitsdaten und damit um „höchst sensible persönliche Informationen“ handele, müsse „nach den Vorgaben der DS-GVO die Authentifizierung ein höchstmögliches Sicherheitsniveau nach dem Stand der Technik“ gewährleisten.

C.
Rechtliche Würdigung

I. Vereinbarkeit der Zugriffserteilungsmöglichkeiten des § 342 Abs. 2 Nr. 1 lit. c und Nr. 2 lit. c SGB V mit deutschem und europäischen Datenschutzrecht

Die Regelungen zur Berechtigungserteilung von Zugriffen auf Kategorien von Dokumenten und Datensätzen der ePA in § 342 Abs. 2 Nr. 1 lit. c und Nr. 2 lit. c SGB V durch Leistungserbringer sind mit höherrangigem Datenschutzrecht vereinbar, da die diesbezüglich zu erteilenden Einwilligungen den Anforderungen der DS-GVO entsprechen und folglich wirksam erteilt werden können.

Im Einzelnen:

1. Berechtigungsmanagement gemäß §§ 339 Abs. 1, 353, 342 Abs. 2 Nr. 1 lit. c SGB V

a) Bestimmung des Prüfungsgegenstandes: Kein „Alles-oder-nichts-Prinzip“ bei der Erteilung von Zugriffsmöglichkeiten nach dem PDSG

Ein wesentlicher Kritikpunkt der Datenschutz-Aufsichtsbehörden besteht darin, dass der Zugriff auf die Dokumente und Datensätze in der ePA zwar auf Einwilligungsbasis geschehe, jedoch die Betroffenen gezwungen seien, Freigaben nach einem „Alles-

[16] Entschließung der Konferenz der unabhängigen Datenschutz-Aufsichtsbehörden des Bundes und der Länder vom 01.09.2020, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/20200901_PDSG_Entschlie%C3%9Fung.pdf, zuletzt aufgerufen am 04.11.2020.

oder-nichts-Prinzip“ zu erteilen oder aber ganz auf den Service der ePA verzichten zu müssen. Was genau unter dem „Alles-oder-Nichts-Prinzip“ zu verstehen ist, wird dabei in der Regel nicht konkretisiert. Die Landesbeauftragte für den Datenschutz Niedersachsen führt aus, dass die Betroffenen im ersten Jahr nur die Möglichkeit hätten „sämtliche Datensätze für alle Behandler freizugeben oder für keinen“; dies widerspreche der Patientensouveränität im Umgang mit den eigenen Gesundheitsdaten.[17] Diese Aussage findet jedoch weder in der gesetzlichen Konzeption noch in der praktischen Umsetzung der Telematikinfrastruktur eine Grundlage und trifft nicht zu.

Betroffene können frei und mit jeweiliger Einwilligung in die konkrete Datenverarbeitung selbst entscheiden, ob sie den Zugriff auf die Daten in der ePA allen zugriffsberechtigten oder nur einzelnen zugriffsberechtigten Leistungserbringern (sowie ggf. deren berufsmäßigen Gehilfen) i.S.v. § 352 SGB V erteilen. Zu trennen ist die Frage, welche *Personen* zugriffsberechtigt sind, von der stufenweisen Granularität der Zugriffserteilung auf die unterschiedlichen *Dokumente* der ePA, die in der Tat in einer dokumenten- bzw. kategoriengenauen Zugriffserteilung durch Einwilligung technisch erst ab 2022 möglich sein wird.[18]

Nach § 339 Abs. 1 SGB V dürfen nur zugriffsberechtigte Leistungserbringer auf die Gesundheitsdaten der Versicherten in der ePA zugreifen, *soweit* die Versicherten diesen jeweils hierzu ihre Einwilligung erteilt haben. Zugriffsberechtigt können nur Angehörige derjenigen Berufsgruppen werden, die in § 352 SGB V aufgelistet sind.

Die Einwilligung der Betroffenen ist in § 353 Abs. 1 und 2 SGB V geregelt. Wer konkret im jeweiligen Einzelfall auf die Dokumente der ePA eines einzelnen Versicherten zugreifen kann, hängt von der individuellen Einwilligung durch eine „eindeutige bestätigende Handlung durch technische Zugriffsfreigabe“ (vgl. § 339 Abs. 1 S. 2, 353 Abs. 1 S. 2 SGB V) ab. Dass diese Einwilligung für einzelne Leistungserbringer und nicht für sämtliche Leistungserbringer, z.B. Ärzte, die mit der Behandlung des Patienten gar nichts zu tun haben, erteilt werden muss, ergibt sich schon aus der Formulierung „s*oweit*“ in § 339 Abs. 1 SGB V. Nur soweit die Patienten ihre Einwilligung durch technische Zugriffsfreigabe erteilen, werden die potentiell Zugriffsberechtigten tatsächlich technisch in die Lage versetzt, auf die ePA zuzugreifen. Zudem wird diese Möglichkeit der Feinsteuerung von den Pflichtinformationen der Krankenkassen umfasst sein: Aus § 343 Abs. 1 Nr. 11 SGB V ergibt sich nämlich, dass die Patienten

---

17 Pressemittelung vom 19.08.2020; https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/thiel-warnt-vor-datenschutzverstossen-durch-elektronische-patientenakte-191688.html.

18 Siehe dazu im Einzelnen unter G. I. 1. d) aa) (2).

durch die Krankenkassen als datenschutzrechtlich Verantwortliche über die Möglichkeit informiert werden müssen, dass sie bei der Datenverarbeitung in der ePA beim Leistungserbringer durch technische Zugriffsfreigabe in die *konkrete* Datenverarbeitung einwilligen können. Gleiches gilt für § 343 Abs. 1 Nr. 18 SGB V, der die Informationspflicht enthält, dass Patienten auch gegenüber Ärzten, die für den öffentlichen Gesundheitsdienst tätig sind, sowie Fachärzten für Arbeitsmedizin und Betriebsärzten ihre Einwilligung erteilen können.

Festzuhalten ist mithin, dass ein Zugriff eines Facharztes auf Dokumente, die gegebenenfalls nur für einen anderen Facharzt relevant und notwendig sind, nur dann möglich ist, wenn der Patient beiden zuvor seine Einwilligung in den Zugriff auf die ePA erteilt hat.

Der Gesetzgeber hat neben der genauen Zugriffserteilung je Leistungserbringer per Einwilligung weitere rechtliche Hürden in das Gesetz aufgenommen, die die Leistungserbringer rechtlich hindern, grundlos auf die ePA zuzugreifen. So ergibt sich aus § 352 SGB V, der die grundsätzlich zugriffsberechtigten Leistungserbringer auflistet, dass diese auch mit Einwilligung des jeweiligen Patienten nur auf die ePA zugreifen dürfen, *soweit* dies für die Versorgung der Versicherten *erforderlich* ist. Ein nicht erforderlicher und damit missbräuchlicher Zugriff auf die Patientendaten ist mit gravierenden haftungsrechtlichen Konsequenzen bewehrt.

Der unberechtigte Zugriff ist beispielsweise explizit gemäß § 397 Absatz 1 Nummer 1 SGB V strafbewehrt. Zudem können sich aus der DS-GVO bei einer Verarbeitung von Daten durch die Leistungserbringer, die nicht auf einer rechtfertigenden Rechtsgrundlage beruht, bei Beanstandung Sanktionen und hohe Bußgelder ergeben (vgl. Art. 83 DS-GVO) – soweit die Leistungserbringer als Verantwortliche tätig werden.

Schließlich drohen potentiell auch berufsrechtliche Konsequenzen für die Leistungserbringer. So haben beispielsweise Ärzte nach § 2 Abs. 2 der (Muster-)Berufsordnung (MBO)[19]

> „ihren Beruf gewissenhaft auszuüben und dem ihnen bei ihrer Berufsausübung entgegengebrachten Vertrauen zu entsprechen. Sie haben dabei ihr ärztliches Handeln am

[19] (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte – MBO-Ä 1997 – in der Fassung der Beschlüsse des 121. Deutschen Ärztetages 2018 in Erfurt, geändert durch Beschluss des Vorstandes der Bundesärztekammer am 14.12.2018.

> Wohl der Patientinnen und Patienten auszurichten. Insbesondere dürfen sie nicht das Interesse Dritter über das Wohl der Patientinnen und Patienten stellen."

Nach § 2 Abs. 5 MBO sind sie zudem

> „verpflichtet, die für die Berufsausübung geltenden Vorschriften zu beachten."

Diese Normen gelten rechtsverbindlich für die Ärzte, soweit die jeweiligen Berufsordnungen der Ärzte der Kammern Regelungen enthalten, die denen der MBO-Ä entsprechen. Verstöße gegen die jeweilige Berufsordnung, welche bei einem für die Behandlung nicht erforderlichen Zugriff auf die ePA vorlägen, können nach den jeweiligen Heilsberufsgesetzen der Bundesländer mit empfindlichen Geldbußen bis hin zur Untersagung der Ausübung des Berufs geahndet werden (vgl. etwa § 60 HeilBerG NRW). Ein solch unberechtigter Zugriff wäre auch nachweisbar, da jeweils dokumentiert werden muss, durch wen und auf welche Dokumente zugegriffen wurde (vgl. § 339 Abs. 3 SGB V).

Bereits im Jahr 2021 kann gemäß § 342 Abs. 2 Nr. 1 lit. c SGB V nicht nur in den Zugriff durch zugriffsberechtigte Leistungserbringer auf Daten in der elektronischen Patientenakte insgesamt, sondern auch in den Zugriff entweder ausschließlich auf Daten nach § 341 Absatz 2 Nummer 1 oder auf Daten nach § 341 Absatz 2 Nummer 6 SGB V eingewilligt werden. Von einem Alles-oder-nichts-Prinzip zu sprechen ist insofern sachlich unzutreffend und steht mit dem Wortlaut der Norm nicht in Einklang.

Im Übrigen kann der Service der ePA – wenn auch mit deutlich eingeschränkter Funktionalität – von Versicherten, die keinen Zugriff entsprechend den Optionen nach § 342 Abs. 2 Nr. 1 lit. c SGB V gewähren wollen, jedenfalls als persönlicher digitaler Ablageort für medizinische Dokumente genutzt werden, auf den nur die betroffene Person selbst Zugriff hat. Sie kann Dokumente in der ePA sammeln und bei Bedarf abrufen.

b) Maßstab: DS-GVO

§§ 339 Abs. 1, 353, 342 Abs. 2 Nr. 1 lit. c SGB V verlangen für den Zugriff auf die in der ePA gespeicherten Gesundheitsdaten gemäß § 341 Abs. 2 SGB V durch Leistungserbringer und andere potentiell zugriffsberechtigte Personen eine Einwilligung im Sinne des Art. 6 Abs. 1 lit. a bzw. Art. 9 Abs. 2 lit. a DS-GVO.

Damit verzichtet der Bundesgesetzgeber in Wahrnehmung der ihm durch die Öffnungsklauseln der DS-GVO eingeräumten Regelungsräume, insbesondere gem. Art. 9 Abs. 2 lit. h DS-GVO, für diese Verarbeitungen eine eigene Rechtsgrundlage zu schaffen, die das Einholen von Einwilligungen überflüssig machte. Ebenso verzichtet der Bundesgesetzgeber auf ein ihm durch Art. 9 Abs. 1 lit. a DS-GVO ermöglichtes Verbot von Einwilligungen für die Verarbeitung personenbezogener Daten besonderer Kategorien nach Art. 9 Abs. 1 DS-GVO wie Gesundheitsdaten i.S.v. Art. 4 Nr. 15 DS-GVO.

Angesichts dessen ergibt sich unmittelbar aus der DS-GVO, dass und unter welchen Voraussetzungen Zugriffe auf die ePA aufgrund einer Einwilligung rechtmäßig sind.

Die von den Krankenkassen bei der Ausgestaltung der ePA zu berücksichtigende Möglichkeit eines Zugriffs durch Leistungserbringer auf die ePA ist gem. Art. 4 Nr. 2 DS-VO eine Verarbeitung in Form der Offenlegung. Hierfür ist datenschutzrechtlich Verantwortlicher i.S.v. Art. 4 Nr. 7 DS-GVO gem. § 341 Abs. 4 SGB V die Krankenkasse. Sie ist kraft Unionsrechts verpflichtet, die Einwilligungen, auf die sie die Erteilung der Zugriffsmöglichkeit stützen will, sowie die Erteilung selbst so auszugestalten, dass die Voraussetzungen der DS-GVO gewahrt werden.

Hierbei sind die Krankenkassen freilich auch an §§ 339 Abs. 1, 353, 342 Abs. 2 Nr. 1 lit. c SGB V gebunden. Sie dürften also kraft Bundesgesetzes die Gestaltungsspielräume der DS-GVO, die sie als Verantwortliche hätten, nur eingeschränkt nutzen. Das betrifft zunächst die Verarbeitungen, für die sie die Verantwortlichen sind – hier: die Offenlegung in einer Form der Bereitstellung gem. Art. 4 Nr. 2 DS-GVO in bestimmter „Granularität“ der personenbezogenen Daten gem. Art. 4 Nr. 1 DS-GVO, die in der jeweiligen ePA gespeichert sind. Da die Krankenkassen im Hinblick auf diese Offenlegungen gem. §§ 339 Abs. 1, 353, 342 Abs. 2 Nr. 1 lit. c SGB V darauf beschränkt sind, sich auf die Rechtsgrundlage einer Einwilligung zu stützen, stellt sich die Frage, ob die insoweit vorgegebenen Inhalte der Einwilligung mit den diesbezüglichen Vorgaben des Unionsrechts vereinbar sind. Das sind Art. 6 Abs. 1 lit. a bzw. Art. 9 Abs. 2 lit. a, Art. 7 und Art. 4 Nr. 11 DS-GVO.

c) Kein Maßstab: „Datensouveränität“

Nach der Ansicht des BfDI ist ein feingranulares Zugriffsmanagement der Versicherten auf die ePA zur Wahrung der „Datensouveränität“ geboten. Die DS-GVO stellt indes jenseits der 6 Abs. 1 lit. a bzw. Art. 9 Abs. 2 lit. a, Art. 7 und Art. 4 Nr. 11 DS-

GVO keine zusätzlichen Wirksamkeitsanforderungen an Einwilligungen. Sie enthält vor allem keinen Grundsatz einer „Datensouveränität".

Vielmehr handelt es sich bei der „Datensouveränität" um ein Schlagwort in der politischen Auseinandersetzung.[20] Aus der Alltagssprache entnommen, wird der Begriff der „Souveränität" mit selbstbestimmtem Handeln assoziiert und als Symbol absoluter Herrschaft über die eigenen persönlichen Daten verwendet.[21] Einen solchen – *a priori* abwägungsresistenten – absoluten Bereich personenbezogener Daten, die mit oder ohne Einwilligung nie verarbeitet werden dürften, kennt die DS-GVO grundsätzlich nicht. Das entspricht im Übrigen der Rechtsprechung des Bundesverfassungsgerichts (BVerfG) welches das Recht auf informationelle Selbstbestimmung zwar als Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, beschreibt; dies jedoch nicht ohne anzumerken, dass dieses „Recht auf ‚informationelle Selbstbestimmung' […] nicht schrankenlos gewährleistet" ist.[22] Der Einzelne hat demnach gerade „nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über ‚seine' Daten"."[23]

Die DS-GVO gestaltet den unionsrechtlich verbürgten Anspruch auf den Schutz personenbezogener Daten nach Art. 8 GRCh aus. Ein Eingriff in dieses Recht ist gerechtfertigt, wenn eine Rechtsgrundlage vorhanden ist und der Grundsatz der Zweckbindung eingehalten wird.[24] Das – und nicht eine wie auch immer postulierte „Datensouveränität" – ist auch vorliegend der rechtliche Maßstab für die zu prüfenden Verarbeitungen personenbezogener Daten.

d) Einhaltung der Anforderungen der DS-GVO

Art. 6 Abs. 1 lit. a bzw. Art. 9 Abs. 2 lit. a, Art. 7 und Art. 4 Nr. 11 DS-GVO werden durch die gemäß §§ 339 Abs. 1, 353, 342 Abs. 2 Nr. 1 lit. c SGB V einzuholenden Einwilligungen erfüllt.

---

20 So auch die DSK, Grundsatzpositionen und Forderungen für die neue Legislaturperiode, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/DSK_GrundsatzpositionenForderungenLegislaturperiode.pdf;jsessionid=48637B0E3E71CFA2483C42BA6F5A795B.2_cid507?__blob=publicationFile&v=2, abgerufen am 14.09.2020.

21 *Spiecker gen. Döhmann/Bretthauer*, Dokumentation zum Datenschutz, 78. EL. 2020, G 2.4.56, Grundsatzpositionen und Forderungen für die neue Legislaturperiode.

22 BVerfGE 65, 1.

23 BVerfGE 65, 1 (39 f.).

24 Vgl. *Ziegenhorn/von Heckel*, Datenverarbeitung durch Private nach der europäischen Datenschutzreform, NVwZ 2016, 1585 f.

Im Einzelnen:

aa) Anforderungen aus Art. 4 Nr. 11 DS-GVO

Eine Einwilligung ist gem. Art. 4 Nr. 11 DS-GVO jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der der Betroffene zu verstehen gibt, dass er mit der Verarbeitung der ihn betreffenden personenbezogenen Daten einverstanden ist.[25]

(1) Freiwilligkeit

Eine Einwilligung gemäß §§ 339 Abs. 1, 353, 342 Abs. 2 Nr. 1 lit. c SGB V wird, wie oben beschrieben, nicht zwingend für den Zugriff durch zugriffsberechtigte Leistungserbringer auf Daten in der ePA allgemein erteilt, sondern kann auch nur für den Zugriff entweder ausschließlich auf medizinische Informationen über den Versicherten oder auf Gesundheitsdaten, die durch den Versicherten zur Verfügung gestellt werden. Zudem wird sie – wie ausgeführt – in der Regel für einzelne Leistungserbringer erteilt werden. Hierdurch sowie über weitere im Gesetz angelegte Schutzmechanismen wird gewährleistet, dass Einwilligungen „freiwillig für den bestimmten Fall“ im Sinne des Art. 4 Nr. 11 DS-GVO erteilt werden können. Selbst eine Einwilligung in den Zugriff auf Daten in der ePA insgesamt, ohne die Gewährleistung einer gewissen Granularität, würde diese Anforderungen erfüllen.

Das Tatbestandsmerkmal „freiwillig“ impliziert, dass die betroffenen Personen eine echte Wahl und die Kontrolle haben müssen.[26] Nach der DS-GVO ist eine Einwilligung nicht gültig, wenn die betroffene Person keine wirkliche Wahl hat, sich zur Einwilligung gedrängt fühlt oder negative Auswirkungen erdulden muss, wenn sie nicht einwilligt. Dementsprechend wird eine Einwilligung nicht als freiwillig angesehen, wenn die betroffene Person die Einwilligung nicht verweigern oder zurückziehen kann, ohne Nachteile zu erleiden.[27] Im Allgemeinen wird eine Einwilligung als unwirksam angesehen, wenn sie unter unangemessenem Druck oder der Einflussnahme auf die betroffene Person, die diese von der Ausübung ihres freien Willens abhalten,

---

25 Vgl. Art. 4 Nr. 11 DS-GVO.

26 Vgl. ErwGr. 42 der DS-GVO; Artikel-29-Datenschutzgruppe, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, angenommen am 28. November 2017, zuletzt überarbeitet und angenommen am 10. April 2018 (WP 259 rev. 01), S. 6; dort auch zum folgenden Text; *Ernst*, in: Paal/Pauly, DS-GVO BDSG 2. Aufl. 2018, DS-GVO Art. 4 Rn. 69; *Ingold*, in: Sydow, DS-GVO Art. 7 Rn. 35.

27 Vgl. ErwGr. 42 DS-GVO; *Stemmer*, in: BeckOK DatenschutzR, 33. Ed. 01.08.2020, DS-GVO Art. 7 Rn. 38.

abgegeben wird.[28] Für eine solche Annahme ist nichts ersichtlich. Beantragung und Nutzung der ePA und damit auch die Entscheidung über den Zugriff durch Leistungserbringer erfolgen insofern freiwillig. Dies ist zunächst eine tatsächliche Frage. Für die Annahme, dass Versicherte nicht wie beschrieben freiwillig handeln werden, gibt es keine Anhaltspunkte.

Die tatsächliche Freiwilligkeit wird gesetzlich abgesichert. Dies erfolgt insbesondere durch das Diskriminierungsverbot gemäß § 335 SGB V. Hiernach dürfen dem Versicherten keinerlei Nachteile entstehen, wenn er sich dazu entschließt, die ePA nicht zu nutzen oder Zugriffe auf die Daten nicht zu erteilen. Gleiches gilt mithin, wenn er seine Einwilligung in den Zugriff nachträglich widerruft. Bei der ePA handelt es sich um ein *zusätzliches* Angebot an die Versicherten.

Das Diskriminierungsverbot sichert, dass die Behandlungen der Leistungserbringer auch ohne Zugriff auf die ePA nach denselben Standards erbracht werden, wie dies im Falle des Zugriffs geschuldet wäre. Es entspricht der berufsrechtlichen Pflicht der Ärzte, ihrer Aufgabenerfüllung gewissenhaft nachzukommen und im Zuge dessen eine umfassende Anamnese vorzunehmen und ggf. erforderliche Informationen und Dokumente abzufragen.

Die Freiwilligkeit folgt außerdem daraus, dass es dem Versicherten auch in Zukunft unbenommen bleibt, dem behandelnden Leistungserbringer den Zugriff auf die ePA zu verweigern und ihm stattdessen auf herkömmlichem Wege einzelne Dokumente zu Vorbefunden und Vorerkrankungen zur Verfügung zu stellen oder einzuwilligen, dass der Leistungserbringer fachärztliche Befunde anderer Leistungserbringer anfordert. Eine solche Anforderung kann er beispielsweise dann stellen, wenn er die unvoreingenommene Meinung eines zweiten Facharztes einholen will. Das bedeutet indes nicht einmal, dass der Versicherte gänzlich auf den Service der Bereitstellung der ePA verzichten müsste. Er kann aufgrund des im SGB V vorgesehenen differenzierten Einwilligungssystems die Nutzung der ePA beantragen und in die dafür erforderliche Verarbeitung administrativer personenbezogenen Daten durch die Krankenkasse einwilligen, ohne gleichzeitig in den Zugriff auf seine Gesundheitsdaten durch behandelnde Leistungserbringer einzuwilligen.

---

[28] Vgl. *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 21.

Aus der Freiwilligkeit, die eine Wirksamkeitsvoraussetzung der Einwilligung ist, ergibt sich indes kein Anspruch auf eine bestimmte technisch-organisatorische Ausgestaltung einer eingesetzten IT-Anwendung nach den individuellen Vorstellungen der einwilligenden Person. Sie stellt im Gegenteil das erklärte Einverständnis mit den vom Verantwortlichen zu gestaltenden Verarbeitungen dar. Da die freiwillige Nutzung der ePA zu einer Rechtsgrundlage zu Gunsten des Verantwortlichen für seine diesbezügliche Datenverarbeitung führt, muss sich die konkrete Ausgestaltung (nur) im Rahmen der hierfür geltenden Vorgaben der DS-GVO halten, insbesondere des Art. 32 Abs. 1 DS-GVO. Die auf der ersten Umsetzungsstufe begrenztere Steuerungsmöglichkeit steht auch angesichts dessen der Freiwilligkeit der Einwilligung nicht entgegen, da sich ein Anspruch auf eine bestimmte Ausgestaltung nicht begründen lässt.[29]

(2) Keine Granularität der Einwilligung

Der Freiwilligkeit steht nicht entgegen, dass die Versicherten auf der ersten Umsetzungsstufe keine fein- oder mittelgranulare (dokumenten- oder kategorienbezogene) Einwilligung erteilen können. Anhaltspunkte dafür, dass die DS-GVO eine gewisse Granularität der Einwilligung hinsichtlich der konkreten Daten fordert, sind nicht ersichtlich.

Das Erfordernis der Granularität wird bislang von Aufsichtsbehörden und Literatur nur hinsichtlich der Einwilligung in die Verarbeitung personenbezogener Daten zu mehreren unterschiedlichen Zwecken diskutiert.[30] Teilweise wird die Granularität dem Tatbestandsmerkmal der „Freiwilligkeit“, teilweise dem des „bestimmten Falls“ gem. Art. 4 Nr. 11 DS-GVO entnommen. Ein Teil der Literatur lehnt das Erfordernis einer Granularität der Einwilligung aber selbst hinsichtlich unterschiedlicher Zwecke von Datenverarbeitungen ab.[31]

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) stellt in diesem Zusammenhang fest:

> „Eine Dienstleistung kann zahlreiche Verarbeitungsvorgänge für mehr als einen Zweck umfassen. In solchen

---

29 Siehe dazu auch die Ausführungen zu den Datenschutzgrundsätzen sowie Art. 25 DS-GVO unter C. I. 1. d) cc).

30 *Krüger*, in: Datensouveränität und Digitalisierung, ZRP 2016, 190 f.

31 *Arning/Rothkegel*, in: Taeger/Gabel, DS-GVO BDSG, 3. Aufl. 2019, DS-GVO Art. 4 Rn. 269.

> Fällen sollten die betroffenen Personen frei wählen können, welchen Zweck sie annehmen, statt in ein Bündel an Verarbeitungszwecken einwilligen zu müssen.“[32]

Gemäß Erwägungsgrund Nr. 32 der DS-GVO sollte,

> „wenn die Verarbeitung mehreren Zwecken dient, […] für alle diese Verarbeitungszwecke eine Einwilligung gegeben werden“.

Hierbei heißt es in demselben Erwägungsgrund:

> „Die Einwilligung sollte sich auf alle zu demselben Zweck oder denselben Zwecken vorgenommenen Verarbeitungsvorgänge beziehen“.

Hieraus folgt, dass für alle Datenverarbeitungsvorgänge, die *zu demselben Zweck* erfolgen, nur *eine* Einwilligung eingeholt werden sollte. Die Ansicht, dass im Hinblick auf eine „Granularität“ für *unterschiedliche personenbezogene Daten* die Einholung jeweils einer Einwilligung notwendig sein soll, steht diesem Erwägungsgrund diametral entgegen.

Diese Sichtweise, dass die DS-GVO keine feingranulare, dokumentenspezifische Einwilligung fordert, bestätigt Art. 14 Abs. 1 lit. c DS-GVO. Hiernach teilt der Verantwortliche der betroffenen Person, wenn personenbezogene Daten nicht bei ihr erhoben werden, die Kategorien personenbezogener Daten mit, die er verarbeitet. Das heißt, die DS-GVO verlangt nicht, dass die betroffene Person die konkreten Daten kennt, um wirksam einzuwilligen. Vielmehr reicht es aus, wenn sich die Information darauf beschränkt, dass etwa „Gesundheitsdaten“ erhoben werden. Die betroffene Person kennt in diesen Fällen regelmäßig nicht einmal die konkreten personenbezogenen Daten. Insofern ist es folgerichtig, dass die DS-GVO auch für eine wirksame Einwilligung keine Granularität hinsichtlich Daten in bestimmten Dokumenten verlangt.

---

[32] Artikel-29-Datenschutzgruppe, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, angenommen am 28. November 2017, zuletzt überarbeitet und angenommen am 10. April 2018 (WP 259 rev. 01), S. 11.

Schließlich hat auch die Artikel-29-Datenschutzgruppe, der Vorgänger des Europäischen Datenschutzausschusses gem. Art. 68 DS-GVO, in ihrem Arbeitspapier zur Verarbeitung von Patientendaten in elektronischen Patientenakten[33] kein datenschutzrechtliches Gebot zur Gewährleistung eines granularen Zugriffsberechtigungsmanagements angenommen. Darin konstatiert sie, dass es sich im Grunde anbieten würde, innerhalb eines ePA-Systems je nach Vertraulichkeit der Daten verschiedene Datenmodule mit unterschiedlichen Zugangsvoraussetzungen einzurichten. Datenmodule, die nicht allzu sensible Daten enthielten (beispielsweise ein „Impfmodul"), könnten für die betroffene Person jederzeit zugänglich sein und auch einem größeren Kreis von Mitarbeitern im Gesundheitsdienst zugänglich gemacht werden. Sensiblere Daten könnten hingegen etwa nur einem kleinen Kreis von Ärzten zugänglich gemacht werden. Hierbei handelt es sich um *Empfehlungen* zur Gewährleistung eines weitreichenden *Datenschutzes*. Ein datenschutz*rechtliches* Gebot wird demgegenüber an keiner Stelle dieses Arbeitspapiers angenommen, geschweige denn begründet.

Der oben bereits erwähnte Ansatz, aus dem Tatbestandsmerkmal „für den bestimmten Fall" eine besondere Granularität zu fordern, geht inhaltlich fehl, da der bestimmte Fall sich nicht auf eine bestimmte Informationsmenge bezieht, sondern vielmehr eine zeitliche Dimension adressiert. Gerade diese zeitliche Komponente in Form einer Befristung von Zugriffsrechten für einzelne Behandler oder Institutionen ist nach den Regelungen des PDSG jedoch gewährleistet. Unabhängig von der Anzahl der Dokumente oder der Anzahl der Zugriffsberechtigten können Versicherte den Zugriff zeitlich festlegen (§ 342 Abs. 2 Nr. 1 lit. f bzw. Nr. 2 lit. f SGB V).

(3) In informierter Weise

Gemäß Art. 4 Nr. 11 DS-GVO müssen die Einwilligungen in „informierter Weise" erfolgen. Es besteht hier kein Anlass zu Zweifeln, dass das der Fall sein wird, insbesondere angesichts der ausführlichen auch darüberhinausgehenden Informationspflichten der Leistungserbringer gegenüber den Frontend-Nichtnutzern gem. § 353 Abs. 2 SGB V.

Eine Einwilligung ist dann informiert und gemäß der DS-GVO insofern wirksam, wenn sie sich auf einen der betroffenen Person zur Verfügung gestellten Text bezieht,

---

33 WP 131, 2007, S. 20.

der neben den Zwecken der Datenverarbeitungen[34] die zu verarbeitenden personenbezogenen Daten zumindest ihrer Kategorie nach, ggf. spezifische Verarbeitungsarten und bei Offenlegungen personenbezogener Daten deren Empfänger zumindest der Kategorie nach bezeichnet.[35] Im Hinblick auf personenbezogene Daten besonderer Kategorien i.S.v. Art. 9 Abs. 1 DS-GVO empfiehlt es sich, darauf hinzuweisen, dass die zu verarbeitenden Daten, ebensolchen Kategorien zugehörig sind (insbesondere Gesundheitsdaten i.S.v. Art. 4 Nr. 15 DS-GVO).

Außerdem muss die betroffene Person gemäß Art. 7 Abs. 3 DS-GVO davon in Kenntnis gesetzt werden, dass sie das Recht hat, ihre Einwilligung jederzeit zu widerrufen und dass der Widerruf der Einwilligung die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt.

Neben der Anforderung, dass die Einwilligung als solche informiert sein muss, ergeben sich weitere Informationspflichten aus Art. 13 und 14 DS-GVO, wobei die allgemeinen Anforderungen des Art. 12 DS-GVO zu beachten sind. Diese Informationen sollten zugleich mit den für die Wirksamkeit der Einwilligung essentiellen (siehe oben) Informationen erteilt werden.

Daneben sind die gegenüber der DS-GVO extensiveren Informationspflichten des SGB V, insbesondere §§ 343, 353 Abs. 2 SGB V zu beachten.

(4) Unmissverständlich

Ebenso ist anzunehmen, dass die Einwilligungen so eingeholt werden, dass die von den betroffenen Personen abgegebenen Willensbekundungen als „unmissverständlich“ i.S.v. Art. 4 Nr. 11 DS-GVO anzusehen sind. Das gilt erst recht mit Blick auf die weitere Anforderung, dass der Verantwortliche, also die Krankenkasse, gemäß Art. 7 Abs. 1 DS-GVO nachweisen können muss, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.[36]

---

34 *Buchner/Kühling,* in: Kühling/Buchner, DS-GVO BDSG, 2. Aufl. 2018, DS-GVO, Art. 7 Rn. 59; *Mester*, in: Taeger/Gabel, DS-GVO BDSG, 3. Aufl. 2019, DS-GVO, Art. 9 Rn. 18.

35 *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 34; *Kühling/Buchner*, in: Kühling/Buchner, DS-GVO BDSG, 2. Aufl. 2018, DS-GVO Art. 7 Rn. 59.

36 *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, DS-GVO Art. 7 Rn. 6.

bb) Kein Verstoß gegen das Kopplungsverbot gemäß Art. 7 Abs. 4 DS-GVO

Auch ein möglicher Verstoß gegen das Kopplungsverbot gemäß Art. 7 Abs. 4 DS-GVO ist nicht ersichtlich. Hiernach muss bei der Beurteilung, ob die Einwilligung freiwillig erfolgt ist, dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich ist.[37] Wird die Einwilligung in eine solche Verarbeitung personenbezogener Daten erteilt, gilt sie gem. Art. 7 Abs. 4 DS-GVO regelmäßig als nicht freiwillig erteilt.[38]

Ein Verstoß gegen das Kopplungsverbot scheidet vorliegend schon deshalb aus, weil die Erteilung der Zugriffsmöglichkeit auf die Gesundheitsdaten der Versicherten in der ePA an die Leistungserbringer demselben Zweck dient wie das krankenkassenversicherungsrechtliche Grundverhältnis mit dem Versicherten. Beides erfolgt zur Gewährleistung einer effizienten und qualitativ guten Gesundheitsversorgung der Versicherten. Die mit der Zugriffserteilung einhergehenden Datenverarbeitungen dienen mithin dem krankenkassenversicherungsrechtlichen Grundverhältnis. Das Gesetz stellt in § 352 SGB V sogar *expressis verbis* sicher, dass der Zugriff nur dann erfolgen darf, wenn er für die Versorgung des Versicherten erforderlich ist.

cc) Kein Verstoß gegen Art. 5 DS-GVO und Art. 25 DS-GVO

Vor dem Hintergrund einer insoweit freiwilligen und informierten Einwilligung, der insbesondere die Information über die Granularität der Freigaben zugrunde liegt, kann kein abweichendes Ergebnis durch die Heranziehung der Grundsätze der Art. 25, 32 DS-GVO begründet werden.[39] Die von der legitimierenden Einwilligung umfasste Granularität ist mit der DS-GVO vereinbar.

Das Berechtigungsmanagement nach §§ 339 Abs. 1, 353, 342 Abs. 2 Nr. 1 lit. c SGB V (erste Umsetzungsstufe) genügt den Datenschutzgrundsätzen der Datenminimierung (Erforderlichkeit), Zweckbindung und Vertraulichkeit (Art. 5 DS-GVO). Auf eine Prüfung des Art. 25 DS-GVO kommt es insofern nicht mehr an.

---

37 *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 24.

38 ErwGr. 43 der DS-GVO.

39 Siehe dazu ausführlich unter C. I. 1. d) cc) (4).

Die Anforderungen des Art. 5 bzw. 25 DS-GVO richten sich – wie die Anforderungen für die Wirksamkeit der Einwilligung – an den jeweils für die Datenverarbeitung Verantwortlichen. Dies sind für die Bereitstellung der ePA die Krankenkassen.

(1) Kein Verstoß gegen die Grundsätze der Datenminimierung und Erforderlichkeit

Ein Verstoß gegen die Grundsätze der Datenminimierung bzw. der Erforderlichkeit (Art. 5 Abs. 1 lit. c DS-GVO) liegt nicht vor.

Nach Art. 5 Abs. 1 lit. c DS-GVO dürfen nur solche Daten verarbeitet werden, die bezogen auf den Zweck der Datenverarbeitung *angemessen*, *erheblich* und für den Zweck der Verarbeitung auch *erforderlich* sind.[40] Der Grundsatz der Erforderlichkeit stellt somit eine Ausprägung des Grundsatzes der Datenminimierung dar.[41] Allen drei Prüfungspunkten gemein ist ihre Bestimmung in Abhängigkeit zum Zweck der Datenverarbeitung.

Die Datenverarbeitung steht hier zunächst in einem *angemessenen* Verhältnis zu dem mit der Datenverarbeitung in der ePA verfolgten Zweck. Dies ist dann der Fall, wenn ihre Zuordnung zu dem Zweck nicht beanstandet werden kann, m.a.W. eine zweckwidrige Zuordnung stattfände.[42] *Zweck* der Verarbeitung ist die Gewährleistung einer effizienten und qualitativ guten Gesundheitsversorgung der Versicherten. Die Verarbeitung der eigenen Gesundheitsdaten in der ePA durch Leistungserbringer dient genau dem Zweck, eine optimale Gesundheitsversorgung sicherzustellen und ist insofern *angemessen* im oben genannten Sinne.

Zudem müssen die Daten *zweckerheblich*, also kausal für die Zweckförderung sein. Durch die Bereitstellung der Daten in der ePA und die Erteilung der Zugriffsberechtigung wird der Zweck der optimalen Gesundheitsversorgung gefördert.

Ob die Datenmenge, die die Versicherten im ersten Ausbaujahr der ePA den zugriffsberechtigten Leistungsgerbringern zur Verfügung stellen müssen, da keine dokumentengenaue Zugriffssteuerung möglich ist, zudem *erforderlich* ist, ist im Rahmen einer

---

40 *Herbst*, in: Kühling/Buchner, 3. Aufl. 2020, DS-GVO Art. 5 Rn. 57; *Spiecker gen. Döhmann*, in: Simitis/Hornung, Datenschutzrecht, DSGVO Art. 5 Rn. 116; *Reimer*, in: Sydow, DSGVO Art. 5 Rn. 32.

41 *Wolff*, in: BeckOK DatenschutzR, Syst. A. Prinzipien des Datenschutzrechts Rn. 57.1; *Schantz*, in: BeckOK DatenschutzR, 33. Ed. 1.5.2020, DS-GVO Art. 5 Rn. 25.

42 *Frenzel*, in: Paal/Pauly, DS-GVO Art. 5 Rn. 35.

einwilligungsbasierten Datenverarbeitung gerade nicht zu prüfen. Der Erforderlichkeitsgrundsatz als Ausprägung des Grundsatzes der Datenminimierung findet auf einwilligungsbasierte Datenverarbeitungen nämlich keine Anwendung.[43]

Jede Verarbeitung personenbezogener Daten muss nach der DS-GVO auf einer Rechtsgrundlage i.S.d. Art. 6 bzw. Art. 9 DS-GVO beruhen. Nahezu alle Rechtsgrundlagen erfordern eine Prüfung der Erforderlichkeit der Datenverarbeitung; dies sind letztlich spezielle Ausprägungen des Erforderlichkeitsgrundsatzes i.S.v. Art. 5 Abs. 1 lit. c DS-GVO.[44] Die einzige Ausnahme bildet der Wortlaut der Rechtsgrundlage der Einwilligung in Art. 6 Abs. 1 lit. a bzw. Art. 9 Abs. 2 lit. a DS-GVO. Eine Erforderlichkeitsprüfung findet hier nach dem Wortlaut nicht statt. Voraussetzung ist allein, dass die betroffene Person wirksam, d.h. freiwillig und informiert für einen oder mehrere festgelegte Zwecke in die Datenverarbeitung ausdrücklich eingewilligt hat. Die Datenverarbeitung auf der Grundlage einer Einwilligung ist letztlich Ausdruck der informationellen Selbstbestimmung.[45] Die betroffene Person entscheidet – sofern sie über alle erforderlichen Informationen verfügt und keinem Zwang ausgesetzt ist – selbst darüber, ob die eigenen personenbezogenen Daten in der gegebenen Form verarbeitet werden sollen oder nicht. Eine weitere Prüfung der Erforderlichkeit, die diese Datenverarbeitung möglicherweise hindern würde, stünde einer solchen selbstbestimmten Umgang hinsichtlich der eigenen Daten gerade entgegen.

Die Frage, ob ein grob granulares Berechtigungsmanagement gegen den Grundsatz der Erforderlichkeit verstößt, ist also auch im Prüfkontext des Art. 5 Abs. 1 lit. c DS-GVO eine Frage der Wirksamkeit – und hier im Speziellen der Reichweite[46] – der Einwilligung als Rechtsgrundlage für diese Datenverarbeitung. Liegt nämlich eine wirksame Einwilligungserklärung vor, so beruht die Datenverarbeitung auf einer ausreichenden Rechtsgrundlage, die gerade keine Prüfung der Erforderlichkeit der Datenverarbeitung verlangt. Ihre Grenze findet die Rechtfertigung durch Einwilligung einer (auch nicht erforderlichen) Datenverarbeitung ausschließlich in ihrer Wirksamkeit.[47] Hätten die Versicherten hier tatsächlich oder auch nur mittelbar keine andere Wahl, als die ePA zu einer optimalen medizinischen Versorgung zu nutzen, wäre diese Grenze überschritten. Da aber auch weiterhin eine vollständig analoge Kommunikation möglich

---

43 *Wolff*, in: BeckOK DatenschutzR, Syst. A. Prinzipien des Datenschutzrechts Rn. 57, 57.1.

44 *Wolff*, in: BeckOK DatenschutzR, Syst. A. Prinzipien des Datenschutzrechts Rn. 56.

45 „Realisierung informationeller Autonomie als primärrechtlich garantierte Grundrechtsausübung“, *Ingold*, in: Sydow, DSGVO, Art. 7 Rn. 10.

46 *Wolff*, in: BeckOK DatenschutzR, Syst. A. Prinzipien des Datenschutzrechts, Rn. 57.1.

47 *Wolff*, in: BeckOK DatenschutzR, Syst. A. Prinzipien des Datenschutzrechts Rn. 57.

ist, besteht eine echte Wahl der Versicherten.[48] Auch die Frage der Granularität der Einwilligung in der ersten Ausbaustufe steht der Freiwilligkeit – wie gezeigt – nicht entgegen.[49]

(2) Kein Verstoß gegen den Grundsatz der Vertraulichkeit

Schließlich liegt auch kein Verstoß gegen den Grundsatz der Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DS-GVO) vor. Nach diesem Grundsatz ist durch geeignete technische und organisatorische Maßnahmen eine angemessene Sicherheit der personenbezogenen Daten zu gewährleisten, einschließlich dem Schutz vor *unbefugter oder unrechtmäßiger Verarbeitung* und vor *unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.* Damit nimmt Art. 5 Abs. 1 lit. f DS-GVO Bezug auf Art. 32 Abs. 1 DS-GVO, der dem jeweils Verantwortlichen jedoch keine konkreten Maßnahmen der Datensicherheit vorschreibt[50].

Art. 5 Abs. 1 lit. f DS-GVO schützt vor unrechtmäßiger und unbefugter Verwendung. *Unrechtmäßige Verarbeitung* meint die Verarbeitung der Daten durch Dritte, die nicht auf einer datenschutzrechtlichen Rechtsgrundlage beruht.[51] Hier könnten im ersten Umsetzungsjahr der ePA aufgrund der fehlenden Feinsteuerung der Zugriffsfreigabe zugriffsberechtigte Leistungserbringer auf alle Daten der ePA zugreifen. Dass sie daran *rechtlich* gehindert sind, ist eine Frage der Verhinderung der *unbefugten Verarbeitung* (siehe sogleich). Dass diese Datenverarbeitung aber gleichwohl nicht eine unrechtmäßige Verarbeitung i.S.d. der DS-GVO darstellt, ergibt sich aus der wirksamen Einwilligung als Rechtsgrundlage in genau diese Zugriffsfreigabe, die die Datenverarbeitung datenschutzrechtlich rechtfertigt. Die Gefahr einer unrechtmäßigen Verarbeitung liegt somit nicht vor.

Zum Schutz vor einer *unbefugten Verarbeitung* grundsätzlich zugriffsberechtigter Leistungserbringer, die im ersten Umsetzungsjahr der ePA mit Einwilligung der Versicherten auch in mehr als die zur Behandlung notwendigen Daten Einblick haben könnten, greift § 352 SGB V: Danach sind die Leistungserbringer – sofern die Einsichtnahme *nicht* für Behandlung erforderlich ist – rechtlich gehindert, die Daten zu verarbeiten. Zusätzlichen Schutz der Integrität der Daten bietet das Berufsgeheimnis, dem nahezu alle potentiell zugriffsberechtigten Leistungserbringer i.S.d. § 352 SGB

---

48 Siehe dazu auch unter C. I. 1. d) aa) (1).

49 Siehe dazu ausführlich unter C. I. 1. d) aa) (2).

50 Vgl. dazu ausführlich bei C. II. 3.

51 *Herbst*, in: Kühling/Buchner, 3. Aufl. 2020, DS-GVO Art. 5 Rn. 74; *Reimer*, in: Sydow, Europäische Datenschutzgrundverordnung, DSGVO Art. 5 Rn. 48.

V unterliegen. Für Personen, die dem Berufsgeheimnis nicht unterliegen, hat der Gesetzgeber besondere Schutzmechanismen geregelt (vgl. § 352 Nr. 12 SGB V).

Anhaltspunkte dafür, dass keine hinreichenden technisch-organisatorischen Maßnahmen zum Schutz vor *unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung* durch die verantwortlichen Krankenkassen vorgenommen werden, sind nicht ersichtlich.

(3) Kein Verstoß gegen den Grundsatz der Zweckbindung

Zudem liegt kein Verstoß gegen den Zweckbindungsgrundsatz (Art. 5 Abs. 1 lit. b DS-GVO) vor. Die Versicherten geben ihre Einwilligung im Hinblick auf einen bestimmten Zweck ab. Dies tun sie in informierter und freiwilliger Weise (s.o.). Eine Verarbeitung der Daten in der ePA zu anderen Zwecken ist nicht vorgesehen. Sofern eine zweckändernde Verarbeitung ab 2023 für wissenschaftliche Zwecke ermöglicht werden soll, erfolgt dies ausschließlich aufgrund einer erneuten für diesen Zweck erteilten Einwilligung der Versicherten (§ 342 Abs. 1 Nr. 4 SGB V).

(4) Kein Verstoß gegen Art. 25 DS-GVO

Schließlich liegt auch kein Verstoß gegen Art. 25 DS-GVO vor. Auch über Art. 25 DS-GVO ergibt sich kein indirekter Verstoß gegen die Datenschutzgrundsätze, der – wie bereits dargelegt – schon direkt nicht gegeben ist.

Art. 25 DS-GVO ist eine spezielle Ausprägung der Datenschutzgrundsätze; explizit verweist er auf den Grundsatz der Datenminimierung (Abs. 1) und nimmt die Erforderlichkeit in Bezug (Abs. 2). Der Norm kommt hinsichtlich der Datenschutzgrundsätze in Art. 5 DS-GVO eine ausschließlich konkretisierende Funktion zu:[52] Die Frage nach der Einhaltung der Datenschutzgrundsätze durch Technikgestaltung und datenschutzrechtliche Voreinstellungen ist im Rahmen von Art. 25 DS-GVO – entsprechend zu Art. 5 DS-GVO – ebenfalls stets in Abhängigkeit vom Zweck der Datenverarbeitung zu bestimmen.[53]

Bei der Auswahl der technisch-organisatorischen Maßnahmen hat der Verantwortliche eine Reihe von abstrakten ausfüllungsbedürftigen Kriterien, wie etwa den Stand der Technik, innerhalb einer Abwägung zu berücksichtigen. Da hier jedoch – wie gezeigt

---

52 *Voigt*, in: Taeger/Gabel, 3. Aufl. 2019, DS-GVO Art. 5 Rn. 29; *Heberlei*n, in: Ehmann/Selmayr, 2. Aufl. 2018, DS-GVO Art. 5 Rn. 23; *Pötters*, in: Gola DS-GVO, 2. Aufl. 2018, DS-GVO Art. 5 Rn. 23; *Herbst*, in: Kühling/Buchner, 3. Aufl. 2020, DS-GVO Art. 5 Rn. 59.

53 *Herbst*, in: Kühling/Buchner, 3. Aufl. 2020, DS-GVO Art. 5 Rn. 56.

– von vorneherein kein Verstoß gegen die Datenschutzgrundsätze, und insbesondere aufgrund der wirksamen Einwilligungen der Betroffenen kein Verstoß gegen den explizit erwähnten Grundsatz der Datenminimierung vorliegt, kann das weitere Prüfprogramm des Art. 25 DS-GVO bei der Ausgestaltung des Datenverarbeitungsvorgangs hier nicht zu einem anderen Ergebnis führen.

Gleichwohl hat der Gesetzgeber eine Reihe von letztlich überschießenden Regelungen in das PDSG aufgenommen, die ein über die unionsrechtlichen Anforderungen hinausgehendes, hohes Datenschutzniveau bei der Verarbeitung personenbezogener Daten in der ePA sichern:

So dürfen grundsätzlich zugriffsberechtigte Leistungsgerbringer auch mit Einwilligung der Versicherten nur dann auf deren Daten zugreifen, soweit dies für die Behandlung *erforderlich* ist (§ 352 SGB V). Diese rechtliche Schranke greift die Prüfung der Erforderlichkeit explizit auf, auch wenn eine solche Prüfung im Rahmen einer einwilligungsbasierten Datenverarbeitung an sich durch die DS-GVO nicht geboten wäre.[54]

Zudem hat der Gesetzgeber datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO) der ePA gesetzlich verankert: Selbst nach Einwilligung in die Nutzung der ePA gegenüber der jeweiligen Krankenkasse kann nach der Grundeinstellung ohne weitere Einwilligungen durch technische Zugriffsfreigabe nur durch den oder die Versicherte auf die ePA zugegriffen werden. Voreingestellte Freigaben für Dritte bestehen nicht. Freigaben müssen durch die Inhaber der ePA aktiv erteilt werden. Das Zugriffsmanagement nach § 352 wird dabei nicht nur rechtlich, sondern auch technisch gewährleistet („Privacy by design“). Die Freigabe der Daten gegenüber dem jeweiligen Leistungserbringer durch Einwilligung der Versicherten ist standardmäßig auf eine Woche begrenzt (vgl. § 342 Abs. 2 lit. e SGB V). Zudem wird der Versicherte vor jeder Einwilligung in die jeweils konkrete Datenverarbeitung stets erneut umfassend informiert, insbesondere auch über den Umstand, dass im ersten Umsetzungsjahr der ePA nur eine grobe Steuerung der Zugriffsbeschränkung hinsichtlich der Dokumente erfolgen kann (§§ 342 Abs. 2 lit. g, 343 SGB V). Willigt der Versicherte dann ein, so ist dies genuiner Ausdruck der Wahrnehmung seiner grundrechtlichen Freiheit, über die eigenen Daten im Rahmen der informationellen Selbstbestimmung selbstständig zu verfügen.

---

54 Unbeschadet hiervon sind die Voraussetzungen des Art. 7 Abs. 4 DS-GVO zu beachten.

2. Berechtigungsmanagement gemäß §§ 339 Abs. 1, 353, 342 Abs. 2 Nr. 2 lit. b SGB V.

Wie aus den obigen Ausführungen ersichtlich, sind Rechtsgrundlage für die Verarbeitung personenbezogener Daten beim Zugriff auf die ePA die von den betroffenen Personen erteilten Einwilligungen gemäß Art. 6 Abs. 1 lit. a bzw. Art. 9 Abs. 2 lit. a DS-GVO. Es bestehen keine Anhaltspunkte dafür, dass die (noch einzuholenden) Einwilligungen die hierfür geltenden Anforderungen, insbesondere Art. 4 Nr. 11 und Art. 7 DS-GVO, nicht einhalten werden und deshalb unwirksam wären. Insbesondere ist die erforderliche „Freiwilligkeit“ gegeben. Eine „Granularität“ hinsichtlich einzelner Daten ist insofern nicht geboten.

Insofern kann für die Frage, ob die Regelungen zur „mittelgranularen“ Berechtigungserteilung auf der zweiten Umsetzungsstufe, die also gegenüber der ersten Umsetzungsstufe eine feinere Granularität aufweisen, datenschutzkonform sind, auf obige Ausführungen verwiesen werden. Demnach ist eine bestimmte Granularität der Einwilligung hinsichtlich der konkreten Daten nicht gefordert. Deshalb sind die Verarbeitungen personenbezogener Daten, die auf der zweiten Umsetzungsstufe mit einem Berechtigungsmanagement einer feineren Granularität einhergehen, angesichts der insofern einzuholenden Einwilligungen erst recht vereinbar mit der DS-GVO.

Mit Blick auf die Frontend-Nichtnutzer besteht auch kein Wertungswiderspruch innerhalb des PDSG. § 341 Abs. 1 SGB V fordert die Einführung einer vollständigen versichertengeführten ePA. Dies ist ein *zusätzlicher* Online-Dienst zu der bisher rein analogen Verarbeitung der Gesundheitsdaten bei den jeweiligen Leistungserbringern, der grundsätzlich eine gewisse technische Grundausstattung bei den Nutzungswilligen voraussetzt. Verfügen die Versicherten über ein geeignetes Endgerät, so können sie die ePA auch problemlos in ihrer jeweiligen Ausbaustufe nutzen. Insofern verhält es sich mit der ePA wie mit allen anderen neuen digitalen Angeboten auf dem Markt. Ein ständiger Zugriff und die selbstständige Verwaltung sämtlicher eigener personenbezogener Daten auch ohne eine bestimmte technische Grundausstattung wird auch nicht von der DS-GVO gefordert, die eine Reihe von Rechten der Betroffenen gegenüber dem Verantwortlichen bereithält. Im Hinblick auf Informationsrechte über die eigenen personenbezogenen Daten regelt Art. 15 DS-GVO lediglich einen Anspruch auf Auskunft über die personenbezogenen Daten, die vom Verantwortlichen verarbeitet werden. Die ePA ermöglicht für Besitzer eines geeigneten Endgeräts nun ein weit über Art. 15 DS-GVO hinausgehendes Angebot, einen vollständigen elektronischen Überblick über alle bei verschiedenen Leistungserbringern verarbeiteten (Gesundheits-)

Daten zu erhalten und diese selbstständig zu verwalten. Den Anspruch, ein solch *zusätzliches* Angebot auch ohne die entsprechende technische Ausstattung nutzen zu können, ergibt sich aus der DS-GVO nicht, zumal die Versicherten auf die ePA zum Zweck einer medizinischen Versorgung nicht angewiesen sind. Dass also die elektronische Patientenakte an bestimmte technische Voraussetzungen geknüpft ist, steht nicht im Widerspruch zu dem grundsätzlichen Anspruch der ePA, einen barrierefreien, versichertengeführten Service anzubieten. [55]

3. Kein Verstoß gegen Art. 3 Abs. 1 GG

Die unterschiedliche Ausgestaltung des Berechtigungsmanagements von Frontend-Nutzern (feingranular) und Frontend-Nichtnutzern (mittelgranular) auf der zweiten Umsetzungsstufe verstößt zudem nicht gegen Art. 3 Abs. 1 GG.

Es kann bereits bezweifelt werden, ob hier – im abschließend unionsrechtlich harmonisierten Bereich der einwilligungsbasierten Verarbeitung personenbezogener Daten – eine Vorschrift des deutschen Rechts, hier die des Art. 3 Abs. 1 GG – anwendbar ist.[56] Das kann aber letztlich dahinstehen.[57] Wäre Art. 3 Abs. 1 GG anwendbar, stellte die unterschiedliche Ausgestaltung des Berechtigungsmanagements von Frontend-Nutzern und Frontend-Nichtnutzern auf der zweiten Umsetzungsstufe keine ungerechtfertigte Ungleichbehandlung im Sinne des Art. 3 Abs. 1 GG dar.

Der Gesetzgeber stellt die ePA als freiwillige Zusatzleistung für die Versicherten zur Verfügung, ohne ihre Rechte im Bereich der Gesundheitsversorgung zu beschränken. Deshalb käme hier Art. 3 Abs. 1 GG hier allenfalls in seiner sog. derivativen Teilhabefunktion[58] zur Anwendung. Im Ausgangspunkt kann grundsätzlich jeder die ePA nutzen. Die Ungleichbehandlung besteht somit nicht hinsichtlich des „Obs“ der Nutzung der ePA, sondern lediglich in der Art und Weise der Zugriffsberechtigungserteilung („Wie“). Die mittelgranulare Zugriffserteilung über die Infrastruktur der Leistungserbringer und die Ermächtigung eines Vertreters stellen gegenüber der Alternative, Versicherten ohne ein eigenes Endgerät die Nutzung der ePA vollständig zu verwehren, das mildere Mittel dar.

---

55 Zu der Frage einer Ungleichbehandlung siehe auch sogleich unter 3.

56 Vgl. dazu BVerfG, Beschluss vom 06.11.2019 – 1 BvR 276/17 – Recht auf Vergessen II, BVerfGE 152, 216, Rn. 42 ff.

57 Zudem liegt ferner jedenfalls keine ungerechtfertigte Ungleichbehandlung i.S.v. Art. 20 GRCh vor.

58 Vgl. dazu BVerfG, Urteil vom 19.12.2017 – 1 BvL 3/14 –, BVerfGE 147, 253.

4. Ergebnis

Die Vorschriften des SGB V, die den Zugriff der Leistungserbringer auf die in der ePA gespeicherten Daten gemäß § 341 Abs. 2 SGB V regeln und insofern eine Einwilligung vorsehen, stehen in ihrer auf der jeweiligen Umsetzungsstufe vorgesehen Ausgestaltung im Einklang mit höherrangigem Recht.

II. Vereinbarkeit der Authentifizierungsanforderungen in § 336 Abs. 2 Nr. 2 SGB V mit deutschem und europäischen Datenschutzrecht

Ein Zugriff des Versicherten auf seine ePA gemäß § 336 Abs. 2 Nr. 2 SGB V ohne Verwendung der elektronischen Gesundheitskarte setzt voraus, dass er sich für diesen Zugriff jeweils durch ein „geeignetes technisches Verfahren, das einen hohen Sicherheitsstandard gewährleistet", authentifiziert hat. Insofern ist zu prüfen, ob die Voraussetzungen eines „hohen Sicherheitsstandards" gegen die Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienst für elektronische Transaktionen im Binnenmarkt (eIDAS-VO)[59] verstößt, namentlich gegen deren Regelung eines „Sicherheitsniveaus ‚hoch'" gemäß Art. 8 Abs. 2 lit. c eIDAS-VO (siehe 1.). Darüber hinaus ist die Frage aufgeworfen, ob sich ein Verstoß des § 336 Abs. 2 Nr. 2 SGB V gegen die eIDAS-VO aus diesbezüglichen Richtlinien des Bundesamts für Sicherheit in der Informationstechnik (BSI) ergibt, einer Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern für Bau und Heimat (siehe 2.).

Schließlich ist zu prüfen, ob § 336 Abs. 2 Nr. 2 SGB V gegen eine anderweitige Vorschrift des höherrangigen Rechts verstößt, die *in der Sache* ein „Sicherheitsniveau ‚hoch'", Art. 8 Abs. 2 lit. c eIDAS-VO entsprechend, für ein technisches Authentifizierungsverfahren in einer Situation vorschreibt, die dem Zugriff der betroffenen Person auf seine Daten, wie sie in einer elektronischen Patientenakte gespeichert sind, vergleichbar ist. Insofern ist insbesondere Art. 32 Abs. 1 und 2 DS-GVO zu prüfen (siehe 3.).

---

[59] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl. EU L 257 vom 28.08.2014, S. 73.

1. Kein Verstoß gegen die eIDAS-VO

§ 336 Abs. 2 Nr. 2 SGB V verstößt nicht gegen die eIDAS-VO. Das ergibt sich aus Folgendem:

Im Rahmen der Beurteilung, ob § 336 Abs. 2 Nr. 2 SGB V die europäischen datenschutzrechtlichen Anforderungen erfüllt, kommt es maßgeblich auf die Bestimmungen zur elektronischen Identifizierung der eIDAS-VO (Art. 6–12) an. Denn § 336 Abs. 2 Nr. 2 SGB V betrifft das für den Zugriff auf die elektronische Patientenakte („ePA“) erforderliche Authentifizierungsverfahren.

a) Räumlicher Anwendungsbereich

Es kann bereits bezweifelt werden, ob § 336 Abs. 2 Nr. 2 SGB V in den räumlichen Anwendungsbereich der eIDAS-VO fällt.

Für den Bereich der elektronischen Identifizierung regelt die eIDAS-VO auf der EU-Ebene die Anerkennung von Identifizierungssystemen anderer Mitgliedstaaten für grenzüberschreitende Abwicklungen von Verwaltungsleistungen.[60] Rein nationale Sachverhalte sind nicht erfasst.[61] Es bedarf für die Anwendung der eIDAS-VO eines Binnenmarktbezugs, insbesondere, weil sie auf der Binnenmarktharmonisierungkompetenz der EU gem. Art. 114 AEUV beruht. Dieser ist Grundlage für Harmonisierungsmaßnahmen, „welche die Errichtung und das Funktionieren des Binnenmarktes zum Gegenstand haben“ (Abs. 1 Satz 2). Es ist fraglich, ob § 336 Abs. 2 Nr. 2 SGB V einen solchen Binnenmarktbezug aufweist. Denn es geht um die Einsicht eines in Deutschland Versicherten in seine von einer deutschen Krankenkasse geführten ePA.

Allerdings hat der europäische Gesetzgeber durchaus Sachverhalte wie den einer elektronischen Patientenakte im Blick.

Erwägungsgrund Nr. 10 der DS-GVO lautet insofern:

> „[…] Die gegenseitige Anerkennung der elektronischen Identifizierung und Authentifizierung ist der Schlüssel zur Verwirklichung einer grenzüberschreitenden Gesundheitsversorgung der europäischen Bürger. Wenn sich Personen im Ausland behandeln lassen wollen,

---

60 *Binder*, in: NK-VwGO, 5. Aufl. 2018, VwGO § 55a Rn. 30.

61 *Binder*, in: NK-VwGO, 5. Aufl. 2018, VwGO § 55a Rn. 28.

> müssen ihre medizinischen Daten im Behandlungsland zur Verfügung stehen. Dies setzt einen soliden, sicheren und vertrauenswürdigen Rahmen für die elektronische Identifizierung voraus."

Es ist aber fraglich, ob § 336 Abs. 2 Nr. 2 SGB V überhaupt für solche Zugriffe auf die ePA durch einen Versicherten, wenn er sich im Ausland befindet, Anwendung findet. Das SGB V ist als solches im Ausland nämlich grundsätzlich nicht anwendbar, ein derartiger Auslandssachverhalt daher möglicherweise gar nicht von § 336 Abs. 2 Nr. 2 SGB V erfasst. Das kann hier aber mit Blick auf den sachlichen Anwendungsbereich der eIDAS-VO letztlich dahinstehen (siehe sogleich).

b) Sachlicher Anwendungsbereich

§ 336 Abs. 2 Nr. 2 SGB V fällt jedenfalls nicht in den sachlichen Anwendungsbereich der eIDAS-VO.

Die Verordnung gilt nach Art. 288 Abs. 2 AEUV unmittelbar und verbindlich in jedem Mitgliedsstaat. Allgemein gefasst enthält die eIDAS-VO Regelungen in den Bereichen „Elektronische Identifizierung" und „Elektronische Vertrauensdienste", die das Vertrauen in elektronische Transaktionen im Binnenmarkt stärken sollen.[62] Konkreter Gegenstand der Regelung ist nach Art. 1 lit. a) eIDAS-VO die Festlegung von Bedingungen, unter denen ein Mitgliedstaat elektronische Identifizierungsmittel eines anderen Mitgliedstaats seit dem 18.09.2018 anerkennen muss.[63] Die Bedingungen gelten gemäß Art. 2 Abs. 1 eIDAS-VO jedoch *nur*, soweit das Identifizierungsmittel einem nach Art. 9 eIDAS-VO *notifizierten* elektronischen Identifizierungssystem unterliegt.

Das ist bei § 336 Abs. 2 Nr. 2 SGB V nicht der Fall. Hiernach muss beim Zugriff des Versicherten ohne Verwendung der elektronischen Gesundheitskarte auf die ePA eine Authentifizierung lediglich „durch ein geeignetes technisches Verfahren, das einen

---

62 Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl. EU L 257 vom 28.08.2014, ErwGr. 2.

63 Dabei soll sich die Wahl der Identifizierungsmittel nach dem jeweils benötigten Vertrauensniveau der Verwaltungsdienstleistung richten. Besonders sichere Identifizierungsmittel sind in Verwaltungsdienstleistungen mit hohem Vertrauensniveau einzusetzen; bei Verwaltungsdienstleistungen mit niedrigerem Vertrauensniveau werden geringere Anforderungen an das Identifizierungsmittel gestellt, vgl. www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/eIDAS/Elektronische_Identifizierung/Elektronische_Identifizierung_node.html, zuletzt aufgerufen am 03.09.2020.

hohen Sicherheitsstandard gewährleistet“ erfolgen. Dieses unterliegt *nicht* einem gemäß Art. 9 eIDAS-VO *notifizierten* elektronischen Identifizierungssystem.

Dieses Ergebnis entspricht dem Gesamtregelungsansatz der eIDAS-VO:

- Nach Erwägungsgrund Nr. 12 soll die eIDAS-VO nicht in bestehende Identitätsmanagementsysteme und die dazugehörigen Infrastrukturen eines Mitgliedstaats eingreifen. Sie verpflichtet deshalb gerade *nicht* zur Einführung oder *Notifizierung* von bestimmten Identitätsmanagementsystemen.

- Erwägungsgrund 13 der eIDAS-VO stellt zudem klar, dass keine *Verpflichtung zur Notifizierung* von elektronischen Identifizierungssystemen besteht, sondern ausschließlich eine *Anerkennungspflicht* für notifizierte elektronische Identifizierungssysteme.[64]

- Nach Erwägungsgrund Nr. 54 ist die gegenseitige Anerkennung von nach dieser Verordnung *notifizierten* elektronischen Identifizierungen die Vorbedingung für die Interoperabilität der mitgliedstaatlichen Online-Dienste. Sinn und Zweck der eIDAS-VO ist mithin allein, durch gegenseitige Anerkennung den Zugang zu allen mitgliedstaatlichen Online-Diensten grenzüberschreitend zu gewähren.[65]

- Die Kommission hatte zwar konkret auch die Authentifizierung in elektronischen Patientenakten im Blick, wenn sie ausführt, „[o]hne gegenseitig anerkannte elektronische Identifizierungsmittel kann ein Arzt dagegen auf behandlungsrelevante medizinische Daten seiner Patienten nicht zugreifen, sodass Untersuchungen und Labortests, denen sie sich bereits unterzogen hatten, erneut durchgeführt werden müssen.“[66] Auch insofern soll aber gerade das System der gegenseitigen Anerkennung von nach der eIDAS-VO *notifizierten* Identifizierungssystemen Anwendung finden.

In der Tat besteht der Gesamtregelungsansatz der eIDAS-VO also gerade nicht in einer europaweiten Vereinheitlichung von Standards für Identifizierungsverfahren. Anerkennung bedeutet schon seinem Wortlaut nach gerade nicht die zwingende Vorgabe von einheitlichen Identifizierungsmaßnahmen. Schließlich ist sich auch die Europäi-

---

64 So auch COM(2012) 238 final, 2012/0146 (COD), S. 6.

65 COM (2012) 238 final, 2012/0146 (COD), S. 6.

66 COM (2012) 238 final, 2012/0146 (COD), S. 5.

sche Kommission darüber bewusst, dass kein umfassender sowie grenz- und sektorenübergreifender EU-Rahmen für sichere, vertrauenswürdige und einfach zu nutzende elektronische Identifizierungssysteme existiert[67] und daher jeder Mitgliedstaat eigene Systeme und Infrastrukturen entwickelt hat. Harmonisierungsmaßnahmen würden einen unverhältnismäßig großen finanziellen und in erheblichem Maße Ressourcen verbrauchenden Aufwand darstellen, sodass ein gemeinschaftlicher Rahmen nur durch gegenseitige Anerkennung bereits bestehender Identifikationssysteme geschaffen werden kann.

Demnach bleibt es dabei, dass Ziel der eIDAS-VO lediglich eine gegenseitige Anerkennung von Identifizierungssystemen ist.[68] *Hierfür* ist es notwendig, dass ein gemeinsames, d.h. EU-weites Verständnis der erforderlichen Sicherheitsanforderungen besteht.

Aus all dem ergibt sich aber nicht – insbesondere auch nicht aus der Durchführungsverordnung (EU) 2015/1502[69] – die Pflicht eines nationalen Gesetzgebers, die Standards, die in der eIDAS-VO und der Durchführungsverordnung normiert sind, zwingend zu übernehmen. Entspricht ein nationales Identifizierungssystem nicht den festgelegten Mindestanforderungen, läuft der jeweilige Mitgliedstaat nur Gefahr, dass sein (nicht notifiziertes) Identifizierungssystem nicht in anderen Mitgliedstaaten nach Art. 6 Abs. 1 eIDAS-VO anerkannt wird.

c) Zwischenergebnis

Ein Verstoß des § 336 Abs. 2 Nr. 2 SGB V gegen die eIDAS-VO liegt bereits deswegen nicht vor, weil diese Norm nicht in den Anwendungsbereich der eIDAS-VO fällt.

---

67 COM (2012) 238 final, 2012/0146 (COD), S. 2.

68 www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/eIDAS/Elektronische_Identifizierung/Elektronische_Identifizierung_node.html, zuletzt aufgerufen am 02.09.2020.

69 Zu der eIDAS-VO wurde eine Durchführungsverordnung erlassen (Durchführungsverordnung (EU) 2015/1502 der Kommission vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, ABl. L 235 vom 9.9.2015). Die eIDAS Durchführungsverordnung dient dem Zweck der eIDAS-VO, die gegenseitige Anerkennung von Identifizierungssystemen zu ermöglichen, und legt Mindestanforderungen an technische Spezifikationen und Verfahren nach dem jeweiligen Schutzniveau fest, vgl. S. 7 ff., ErwGr. 2.

2. BSI-Richtlinien

Der BfDI und der Chaos Computer Club (CCC) haben in den Gesetzgebungsverfahren vertreten, dass sich aus verschiedenen BSI-Richtlinien eine Anwendbarkeit der Vorgaben der eIDAS-VO, die von den Richtlinien des BSI übernommen werden, ergebe.[70]

a) BSI-Richtlinien kein höherrangiges Recht

Ein Verstoß des § 336 Abs. 2 Nr. 2 SGB V gegen die eIDAS-VO ergibt sich jedoch nicht daraus, dass Richtlinien des BSI von einer Anwendung der eIDAS-VO ausgehen oder hierauf verweisen. Selbst wenn Richtlinien des BSI ausdrücklich die Anwendung der eIDAS-VO anordneten – *quod non* –, führte dies keinesfalls zu einem Verstoß des § 336 Abs. 2 Nr. 2 SGB V gegen die eIDAS-VO. Denn hierzu müssten Richtlinien des BSI einen höheren rechtlichen Rang haben als das SGB V. Das Gegenteil ist aber der Fall. Das SGB V ist ein Parlamentsgesetz; Richtlinien des BSI haben – unabhängig von ihrem rechtlichen Charakter (siehe hierzu sogleich) – einen niedrigeren Rang als das SGB V.

Aber auch inhaltlich beanspruchen die Richtlinien nicht Maßstab für § 336 Abs. 2 Nr. 2 SGB V oder für ein anderes Bundesgesetz zu sein. Das ergibt sich aus Folgendem:

b) BSI-Richtlinie TR-03107-1: Elektronische Identitäten und Vertrauensdienste im E-Government Teil 1

aa) Keine Verpflichtung zur Einhaltung der eIDAS-VO

Es ist das Ziel der TR-03107-1, Verfahren des Identitätsmanagements für verschiedene Prozesse des E-Government und E-Business zu bewerten und diese den verschiedenen Vertrauensniveaus zuzuordnen. Die TR-03107-1 stellt dabei nicht nur auf Verwaltungsprozesse wie etwa die Inanspruchnahme von Verwaltungsleistungen ab, sondern ausdrücklich auch auf Geschäftsprozesse (E-Business) zwischen natürlichen und juristischen Personen sowie Behörden und anderen Dienstanbietern. Maßgeblich für die Einordnung eines Prozesses zu einem Vertrauensniveau ist der Prozess als solcher. Die TR-03107-1 Teil 1 unterteilt sämtliche Prozesse, sei es ein Verwaltungsprozess oder

---

[70] Zweite Stellungnahme des BfDI zum Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur vom 25.05.2020, S. 6 f.; Stellungnahme zum Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendatenschutzgesetz – PDSG), Stellungnahme zum Gesetzentwurf der Bundesregierung (BT-Drs. 19/18793), S. 3.

ein reiner Geschäftsprozess, in drei Kategorien, namentlich (1) Identifizierung von Personen, Organisationseinheiten oder Ressourcen, (2) Abgabe einer Willenserklärung/Transaktionsauthentisierung[71] und (3) elektronische Übermittlung von Dokumenten und Identitätsdaten. Für jede dieser Kategorien normiert die Richtlinie Eignungsvoraussetzungen eines Mechanismus, um diesen für ein Vertrauensniveau anwenden zu können. Welches Vertrauensniveau in einem konkreten Prozess eingesetzt wird, ist hiernach aber *durch den Betreiber des Verwaltungs- oder Geschäftsprozesses* unter Berücksichtigung der spezifischen Gefährdung *festzulegen*.[72]

Im vorliegenden Fall des E-Business zwischen Krankenkasse und Versicherten ist Betreiber der eGK und ePA die Krankenkasse als verantwortliches Unternehmen für die ePA nach §§ 307 Abs. 5, 1, 341 Abs. 4 SGB V Diese wird durch § 336 Abs. 2 Nr. 2 SGB V insoweit bei der Bestimmung des notwendigen Vertrauensniveaus gesetzlich gebunden, als diese Norm einen „hohen Sicherheitsstandard“ für den Zugriff auf die ePA vorschreibt.

Die TR-03107-1 sieht für Prozesse, die die Identifizierung einer Person betreffen – vorliegend die Identifizierung, um den Zugang zu ePA zu erhalten – und einem hohen Vertrauensniveau in Anlehnung an die Definition der eIDAS-VO zugeordnet sind, Maßnahmen wie den elektronischen Identitätsnachweis oder Kryptografische Hardwaretoken vor.[73] Für die Übermittlung von Daten im Rahmen der Einsicht in die ePA werden Verfahren der DE-Mail, OSCI sowie der Upload mit elektronischem Identitätsnachweis als statthafte Maßnahmen für ein hohes Vertrauensniveau dargelegt.[74]

Dieser Maßnahmenkatalog ist jedoch nicht verpflichtend; vielmehr verstehen sich die technischen Richtlinien des BSI lediglich als Empfehlungen.[75] Dies entspricht der dem BSI nach § 3 Abs. 1 S. 1 BSIG zugewiesenen Aufgabe. Das ist die Förderung der Sicherheit in der Informationstechnik. Zwar kann das BSI im Rahmen dieses Aufgabenbereichs auch einheitliche Sicherheitsstandards für die Bundesverwaltung erlassen,

---

71 Zum Beispiel als Zustimmung zu bestimmten Verwaltungsdienstleistungen, Geschäftsvorgängen oder Dokumenteninhalten.

72 BSI, Technische Richtlinie TR-03107-1 Elektronische Identitäten und Vertrauensdienste im E-Government Teil 1, 07.05.2019, S. 13.

73 BSI, Technische Richtlinie TR-03107-1 Elektronische Identitäten und Vertrauensdienste im E-Government Teil 1, 07.05.2019, S. 31

74 BSI, Technische Richtlinie TR-03107-1 Elektronische Identitäten und Vertrauensdienste im E-Government Teil 1, 07.05.2019, S. 41.

75 Vgl. *Illies/ Lochter/ Stein* in: Kilian/ Heussen, Computerrechts-Handbuch, 34. EL Mai 2018, Teil 15, Rn. 82.

§ 8 Abs. 1 S. 1 BSIG. Jedoch haben auch diese aus sich heraus noch nicht den Charakter einer Verwaltungsvorschrift, sondern müssen nach § 8 Abs. 1 S. 2 BSIG durch das Bundesministerium des Innern, für Bau und Heimat als solche erlassen werden. Den Parlamentsgesetzgeber binden derartige Verwaltungsvorschriften naturgemäß nicht.

bb) Keine normkonkretisierende Verwaltungsvorschrift

Der BfDI hat sich in seiner Kritik an § 336 Abs. 2 Nr. 2 SGB V im Gesetzgebungsverfahren auf eine entsprechende Stellungnahme des CCC bezogen.[76] Der CCC hat die Auffassung vertreten, dass die Richtlinien des BSI als sog. normkonkretisierende Verwaltungsvorschriften anzuwenden seien; nur so könne der Begriff des „hohen Sicherheitsstandards“ in § 336 Abs. 2 Nr. 2 SGB V hinreichend konkret verstanden und angewendet werden.

Selbst wenn dies richtig wäre, führte dies nicht zu einer Unvereinbarkeit des § 336 Abs. 2 Nr. 2 SGB V mit höherrangigem Recht, sondern nur zu einer – unter bestimmten Umständen verbindlichen – entsprechenden Auslegung eben dieser Vorschrift. Normkonkretisierende Verwaltungsvorschriften binden grundsätzlich nicht nur die Verwaltung, sondern können auch Gerichte binden.[77] In seltenen Ausnahmefällen ist aber eine Verwaltungsvorschrift auch eine normkonkretisierende Verwaltungsvorschrift, die die diesbezüglichen Anforderungen erfüllt.[78] Das ist vorliegend nicht der Fall.

Denn eine unmittelbare Anwendung der Richtlinien des BSI würde nur bestehen, soweit es sich bei den technischen Richtlinien um (normkonkretisierende) Verwaltungsvorschriften handelte.[79] Verwaltungsvorschriften werden innerhalb einer Verwaltungsorganisation von einer übergeordneten Behörde oder einem Vorgesetzten an nachgeordnete Behörden beziehungsweise Bedienstete erlassen. Die Krankenkassen

---

76 Stellungnahme des BfDI vom 09.06.2020 (Patientendaten-Schutz-Gesetz (PDSG) - BT-Drs. 19/18793; Formulierungshilfen für Änderungsanträge), S. 7.

77 Dabei müssen diese Verwaltungsvorschriften eine Reihe von Kriterien erfüllen, die die Rechtsprechung im Einzelnen aufgestellt hat, vgl. *Gerhardt*, Normkonkretisierende Verwaltungsvorschriften, NJW 1989, 2233, 2237; *Wolff*, in: Sodan/Ziekow, NK-VwGO, 5. Aufl. 2018, VwGO § 114 Rn. 384.

78 Anerkannt ist das etwa für die im Umweltrecht geltenden Verwaltungsvorschriften TA Lärm (vgl. BVerwG, Urt. v. 24.09.1992 = BVerwGE 91, 92, 94) und TA Luft (BVerwG 1 C 102/76, Urt. v. 17.02.1978 = BVerwGE 55, 250 ff., dort noch als antizipiertes Sachverständigengutachten bezeichnet, in der Sache aber bereits gleich).

79 Normkonkretisierende Verwaltungsvorschriften binden die Verwaltung, lediglich in atypischen Einzelfällen wird sie durch den Gleichheitssatz zu einer Abweichung berechtigt und verpflichtet. Auch für die Gerichte sind normkonkretisierende Verwaltungsvorschriften nach Ansicht der Rechtsprechung verpflichtend, vgl. *Voßkuhle/Kaufhold*, Verwaltungsvorschriften, JuS 2016, 314, 316.

als Betreiber der ePA stellen jedenfalls keine nachgeordneten Verwaltungsbehörden des BSI dar.

Es ist auch nicht der Sinn und Zweck der technischen Richtlinien, etwaige unbestimmte Rechtsbegriffe, wie den Begriff „hoher Sicherheitsstandards“ in § 336 Abs. 2 Nr. 2 SGB V, verbindlich zu konkretisieren. Insoweit können sie nur als entsprechende Orientierung verstanden werden.[80]

Unzutreffend ist schließlich auch die Annahme einer verbindlichen Anwendung der BSI TR-03107-1 beim Zugriff auf Gesundheitsdaten mit der Begründung, diese basierten auf internationalen Normen und dienten der Feststellung des „Stands der Technik“. Dieser Annahme ist – über das oben Gesagte hinaus – schon der Wortlaut der technischen Richtlinie selbst entgegenzuhalten, da diese ausdrücklich davon spricht, Prozesse den einzelnen Vertrauensniveaus (normal, substanziell, hoch) zuzuordnen. Demnach beansprucht die TR-03107-1 gerade nicht, selbst festzulegen, was als „Stand der Technik“ zu werten ist, sondern nur, verschiedene technische Maßnahmen darzulegen, die der jeweiligen Kategorie des Vertrauensniveaus entsprechen.[81]

c) TR-03147: Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen

Ein Verstoß des § 336 Abs. 2 Nr. 2 SGB V gegen höherrangiges Recht ergibt sich auch nicht aus der TR-03147. Insofern gelten zunächst die gleichen Erwägungen wie zur TR-03107-1 ausgeführt (siehe vorstehend).

Die Technische Richtlinie 03147 ergänzt die TR-03107-1 für Verfahren zum Identitätsnachweis und zur Identitätsprüfung natürlicher Personen basierend auf ID-Dokumenten hinsichtlich der Bedrohungen für und Anforderungen an diese Verfahren. Auch im Rahmen dieser Richtlinie ist das notwendige Vertrauensniveau anwendungsspezifisch *durch den Betreiber des Prozesses*, vorliegend der Krankenkassen, festzulegen, sodass auch diese technische Richtlinie kein bestimmtes Schutzniveau für Verfahren und Prozesse der Identitätsprüfung festlegt. Darüber hinaus werden keine technischen Maßnahmen betrachtet, die zur Sicherung der Vertraulichkeit übermittelter Daten notwendig sind. Der Inhalt der TR-03147 beschränkt sich auf die Darlegung möglicher Bedrohungen für im Rahmen der Identitätsprüfung verwendeter Prozesse. Sie nennt insbesondere die Gefahr für die Schutzziele (Eindeutigkeit, Existenz und

---

80 *Martini*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, DS-GVO Art. 32 Rn. 56.

81 BSI, Technische Richtlinie TR-03107-1 Elektronische Identitäten und Vertrauensdienste im E-Government Teil 1, 07.05.2019, S. 8.

Legitimität) des Identitätsnachweises durch Gültigkeitsverlust, gefälschter oder nicht ausschließlich einer Person zuordenbarer ID-Attribute. Schließlich nennt sie Anforderungen für den konkreten Identifizierungsabschnitt, die sich aus der konkreten Bedrohung ergeben.

Insoweit nennt die TR-03147 verschiedene Authentifizierungsprozesse, die den Anforderungen des „hohen Sicherheitsstandards" des § 336 Abs. 2 Nr. 2 SGB V genügen. Sie gibt insofern Anhaltspunkte für die Bewertung verschiedener Prozesse. Die Zuordnungen der verschiedenen Anforderungen zu einem konkreten Vertrauensniveau[82] entfalten keine Bindungswirkung, da auch sie aus den oben dargelegten Gründen nur Empfehlungen sind und insofern nur als Orientierungshilfe verstanden werden können.

3. Vereinbarkeit mit der DS-GVO

Schließlich ist zu fragen, ob § 336 Abs. 2 Nr. 2 SGB V, indem er einen „hohen Sicherheitsstandard" für das Authentifizierungsverfahren fordert, gegen die DS-GVO verstößt, etwa, weil diese die Einhaltung des „Schutzniveaus ‚hoch'" i.S.d. eIDAS-VO oder aber – der Kritik der Entschließung der DSK entsprechend – ein „höchstmögliches Sicherheitsniveau"[83] forderte.

a) Kein Erfordernis eines Schutzniveaus „hoch" i.S.d. eIDAS-Verordnung

In der Tat enthält die DS-GVO Vorgaben zur Datensicherheit. Im Kern ergeben sich die Anforderungen aus Art. 32 Abs. 1 und 2 DS-GVO. Hiernach ist der Verantwortliche – § 307 SGB V entsprechend entweder die jeweilige Krankenkasse, die Leistungserbringer oder die Gesellschaft für Telematik je nach Verarbeitungsvorgang – verpflichtet, „geeignete technische und organisatorische Maßnahmen" zu treffen, „um ein dem Risiko angemessenes Schutzniveau zu gewährleisten". Dies hat der Verantwortliche „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen" zu tun. Solche geeigneten Maßnahmen können

---

82 BSI, Technische Richtlinie TR-03147, Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen, 05.12.2018, S. 14 f.

83 Entschließung der Konferenz der unabhängigen Datenschutz-Aufsichtsbehörden des Bundes und der Länder vom 01.09.2020, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/20200901_PDSG_Entschlie%C3%9Fung.pdf, zuletzt aufgerufen am 04.11.2020.

auch sein, „notwendige Garantien in die Verarbeitung [selbst] aufzunehmen“; das sieht unter den gleichen Voraussetzungen Art. 25 Abs. 1 DS-GVO vor, der den Verantwortlichen zu Datenschutz durch Technikgestaltung verpflichtet.

Art. 32 Abs. 1 und 2 DS-GVO – ebenso wie Art. 25 Abs. 1 DS-GVO – verpflichten den Verantwortlichen gleichwohl nicht zu einer konkreten Maßnahme der Datensicherheit. Insbesondere verlangen sie nicht, dass im speziellen Fall eines Authentifizierungsverfahrens bestimmte Sicherheitsmaßnahmen zu ergreifen wären. Schon gar nicht verweisen diese Vorgaben auf die eIDAS-VO und deren Art. 8 Abs. 2 lit. c. Ausweislich ihrer allgemeinen Bestimmungen wird mit der eIDAS VO kein Datenschutz geregelt, vielmehr verweist Art. 5 Abs. 1 eIDAS VO i.V.m. Art. 94 Abs. 2 S. 1 DS-GVO auf die DS-GVO.

In der Sache schreiben Art. 32 Abs. 1 und 2 bzw. Art. 25 Abs. 1 DS-GVO dem Verantwortlichen ein Vorgehen vor, anhand dessen er selbst ermitteln muss, welche Maßnahmen er im Hinblick auf seine konkrete Verarbeitung personenbezogener Daten ergreifen wird. Hierbei muss der Verantwortliche zunächst das Risiko seiner Verarbeitung auf diese Weise ermitteln, sodann muss er die Schwere des Risikos durch eine Folgenabschätzung bestimmen. Darüber hinaus muss er die Wahrscheinlichkeit einer Realisierung des Risikos abschätzen. In einem letzten Schritt muss er ermitteln, durch welche technischen und organisatorischen Maßnahmen er das so ermittelte Risiko vermeiden oder mindern kann bzw. inwiefern es angemessen ist, dieses (zumindest zu einem Teil oder Rest) hinzunehmen.

Zusammengefasst schreibt die DS-GVO dem Verantwortlichen keine konkreten Maßnahmen der Datensicherheit vor, sondern Prüfungen, die er durchführen muss und anhand derer er selbst technische und organisatorische Maßnahmen zur Datensicherheit für seine Verarbeitung ermittelt. Außerdem muss er (nur) die so von ihm ermittelten Maßnahmen dann auch treffen. Bei der Auswahl der Maßnahmen hat der Verantwortliche den Stand der Technik als einen von vielen Aspekten zu berücksichtigen, nicht aber pauschal einzuhalten. Dabei verlangt die DS-GVO nur solche Maßnahmen für den Schutz von Daten, welche der verarbeitenden Stelle technisch möglich und von dieser praktisch realisierbar sind. Gleichwohl befreit es sie nicht von der Pflicht, im Laufe der Verarbeitung regelmäßige Überprüfungen und Anpassungen der technisch-organisatorischen Maßnahmen vorzunehmen.[84]

---

[84] *Martini*, in: Paal/Pauly, 2. Aufl. 2018, DS-GVO Art. 32 Rn. 56; *Schultze-Melling*, in: Taeger/Gabel, 3. Aufl. 2019, DS-GVO Art. 32 Rn. 13.

Diesen Vorgaben widerspricht § 336 Abs. 2 SGB V nicht. Denn er schreibt lediglich einen Sicherheitsstandard für solche Maßnahmen vor, namentlich einen „hohen". Letztlich stellt § 336 Abs. 2 Nr. 2 SGB V somit nur sicher, dass ein hoher Sicherheitsstandard nicht unterschritten werden darf. Nach der DS-GVO ist ein Verantwortlicher aber ohnehin frei, strengere Maßnahmen der Datensicherheit zu ergreifen, als sie i.S.d. Art. 32 Abs. 1 DS-GVO angemessen wären. Es ist also unschädlich, dass für die Verantwortlichen im Hinblick auf die Sicherheit des Authentifizierungsverfahrens bundesgesetzlich eine gewisse „Benchmark" vorgesehen ist.

Etwas anderes ergibt sich auch nicht aus Art. 35 DS-GVO. Dieser schreibt für bestimmte Formen der Verarbeitung personenbezogener Daten eine sog. Datenschutz-Folgenabschätzung vor. Das ist dann der Fall, wenn die Form der Verarbeitung voraussichtlich ein *hohes* Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, Art. 35 Abs. 1 S. 1 DS-GVO. Es bedarf hier keiner ins Detail gehenden Prüfung, inwiefern diese Voraussetzungen erfüllt sind. Denn im Kern verpflichten die Vorschriften zur Datenschutz-Folgenabschätzung den Verantwortlichen ebenfalls (nur) dazu, anhand einer bestimmten Vorgehensweise die für ihn geeigneten Maßnahmen zu ermitteln und die so ermittelten Maßnahmen dann zu treffen. Darüber hinaus ist er zu weiteren Prüfungen und insbesondere zu Dokumentationen verpflichtet. Konkrete Maßnahme der Datensicherheit selbst schreibt aber auch Art. 35 DS-GVO nicht vor.

Auch Art. 35 Abs. 1 S. 1 DS-GVO verpflichtet ausschließlich den Verantwortlichen – hier die jeweilige Krankenkasse. Art. 35 Abs. 1 S. 2 DS-GVO enthält aber insofern eine Erleichterung, als eine einzige Datenschutz-Folgenabschätzung dann vorgenommen werden kann, wenn es um ähnliche Verarbeitungsvorgänge mit ähnlich hohen Risiken geht. Das läuft nach hier vertretener Auffassung darauf hinaus, dass nicht jede Krankenkasse eine Datenschutz-Folgenabschätzung durchführen muss, sondern nur diejenigen, deren Authentifizierungsverfahren keine hinreichende Ähnlichkeit zu denjenigen anderer Krankenkassen aufweisen, die bereits eine entsprechende Datenschutz-Folgenabschätzung vorgenommen haben. Dies zeigt zudem, dass die DS-GVO selbst keinen Anhaltspunkt dafür bietet, dass bereits der Gesetzgeber im Vorhinein gehalten wäre, Einschränkungen vorzunehmen, die sich unmittelbar auf die Datenschutz-Folgenabschätzung der Verantwortlichen auswirken würden.

b) Kein Maßstab: „Höchstmögliches Sicherheitsniveau"

Die Bezeichnung „höchstmögliches Sicherheitsniveau" ist hingegen im Rahmen von Art. 32 DS-GVO keine rechtliche Kategorie, sondern wird in der öffentlichen Debatte

über das Patientendaten-Schutzgesetz vielmehr als zugehöriger Begriff der „höchst sensiblen Daten“ verwendet. Indes finden sich beide Bezeichnungen nicht in der DS-GVO. Für Gesundheitsdaten kennt Art. 9 DS-GVO allenfalls die Bezeichnung der „besonderen Kategorien personenbezogener Daten“, für deren Verarbeitung entsprechend besondere Anforderungen gelten. „Höchst sensibel“ taucht dort nicht auf. Art. 32 DS-GVO spricht ebenfalls nur von einem dem „Risiko angemessenen Schutzniveau“, nicht jedoch von einem „höchstmöglichen“. Die Frage des anzulegenden Maßstabs des Sicherheitsniveaus der Datenverarbeitung bemisst sich mithin – wie gezeigt – allein an den abstrakten Anforderungen des Art. 32 DS-GVO.

Die Maximalforderung nach einem „höchstmöglichen“ Sicherheitsniveau lässt schließlich auch außer Betracht, dass neben der Datensicherheit auch Art, Umfang, Umstände und *Zweck der Verarbeitung* in die Abwägung zugunsten eines angemessenen Schutzniveaus i.S.v. Art. 32 Abs. 1 DS-GVO einzustellen sind.[85] Darunter fällt im Rahmen der ePA insbesondere der Aspekt der Verfügbarkeit der Daten zu Zwecken eines optimalen Gesundheitsschutzes in einem vernetzten Gesundheitssystem. Durch den elektronischen Zugriff können schwerwiegende gesundheitliche Gefährdungen durch fehlende Daten vermieden werden, wenn etwa durch einen Orts- und Arztwechsel bereits erhobene Befunde und Erkenntnisse auf analogem Weg nicht übermittelt würden oder zum Erliegen kommen, wie auch insbesondere im gegenwärtigen Szenario einer Pandemie.[86]

4. Ergebnis

§ 336 Abs. 2 Nr. 2 SGB V verstößt nicht gegen höherrangiges Recht. Das gilt insbesondere für die Anforderungen eines „hohen Sicherheitsstandards“ für die hiernach einzusetzenden Authentifizierungsverfahren.

---

85 *Schultze-Melling*, in: Taeger/Gabel, 3. Aufl. 2019, DS-GVO Art. 32 Rn. 14.

86 Vgl. dazu auch die Stellungnahme des Wissenschaftlichen Beirats für Digitale Transformation der AOK vom 02.10.2020.

REDEKER SELLNER DAHS
Leipziger Platz 3, 10117 Berlin
Tel +49 30 885665-176
boellhoff@redeker.de

Rechtsanwälte, Partnerschaftsgesellschaft mbB
Sitz Bonn · Partnerschaftsregister · AG Essen PR 1947

Berlin · Bonn · Brüssel · Leipzig · London · München www.redeker.de