Deutscher Bundestag **Drucksache 19/23243**

19. Wahlperiode 08.10.2020

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Dr. Wieland Schinnenburg, Michael Theurer, Renata Alt, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/22825 –

Umsetzung des Patientendaten-Schutz-Gesetzes vor dem Hintergrund europarechtlicher Vorgaben zum Datenschutz

Vorbemerkung der Fragesteller

Am 3. Juli 2020 hat der Deutsche Bundestag das Patientendaten-Schutz-Gesetz (PDSG) beschlossen und dem Bundesrat zur Beratung zugewiesen (Bundesratsdrucksache 470/20). Das Gesetz sieht eine umfassende Neustrukturierung der Regelungen zur Telematikinfrastruktur und ihrer Anwendungen vor. Insbesondere sollen digitale Angebote wie das E-Rezept oder die elektronische Patientenakte (ePA) nutzbar gemacht und sensible Gesundheitsdaten gleichzeitig bestmöglich in Übereinstimmung mit den Vorgaben der Datenschutz-Grundverordnung sowie der einschlägigen nationalen Datenschutzregelungen geschützt werden (https://www.bundesgesundheitsministerium.de/patientendaten-schutz-gesetz.html; Bundestagsdrucksache 19/18793, S. 2). Ob das Gesetz diesen Ansprüchen insbesondere mit Blick auf den Schutz personenbezogener Gesundheitsdaten gerecht wird, ist aus Sicht der Fragesteller mehr als fraglich.

Nach Auffassung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) Professor Ulrich Kelber „verstößt eine Einführung der ePA ausschließlich nach den Vorgaben des PDSG an wichtigen Stellen gegen die europäische Datenschutz-Grundverordnung“. Sollte das PDSG unverändert beschlossen werden, müsse er „die seiner Aufsicht unterliegenden gesetzlichen Krankenkassen mit rund 44,5 Millionen Versicherten formell davor warnen, die ePA nur nach den Vorgaben des PDSG umzusetzen, da dies ein europarechtswidriges Verhalten darstellen würde“.

Er bereite Maßnahmen vor, um einer europarechtswidrigen Umsetzung der ePA abzuhelfen, wobei er ausdrücklich darauf hinweist, dass ihm nach der Datenschutz-Grundverordnung (DSGVO) neben Anweisungen auch Untersagungen zur Verfügung stünden. Insbesondere die Möglichkeiten eines „feingranularen Zugriffs“ auf die Patientendaten werden als nicht ausreichend erachtet. Defizitär aus Datenschutzsicht seien zudem die fehlende dokumentengenaue Kontrolle über die Einsichtsrechte der Beteiligten (jedenfalls für das Jahr 2021) und das Authentifizierungsverfahren für die ePA. Der BfDI habe in seinen Stellungnahmen während des Gesetzgebungsverfahrens „mehrfach darauf hingewiesen, dass Patientinnen und Patienten bei Einführung der ePA die

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Gesundheit vom 8. Oktober 2020 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

volle Hoheit über ihre Daten besitzen müssen“ (https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2020/20_BfDI-zu-PDSG.html).

Vorbemerkung der Bundesregierung

Die elektronische Patientenakte (ePA) als Kernelement der digitalen medizinischen Anwendungen bietet mit Blick auf die aktuellen und zukünftigen Herausforderungen im Gesundheitswesen große Chancen zur Gewährleistung einer effizienten und qualitativ guten Gesundheitsversorgung der Versicherten.

Mit der ePA 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.

Durch die bessere Verfügbarkeit der medizinischen Daten kann die ePA für die Therapieentscheidung der Leistungserbringer einen wesentlichen Mehrwert leisten. Zeitaufwendige, medizinisch belastende und kostenintensive Mehrfachuntersuchungen können vermieden und mehr Zeit für die individuelle Betreuung der Versicherten gewonnen werden. Auch die Versicherten selbst werden besser über ihre Gesundheitsdaten informiert, indem vielfältig eingehende Informationen aus unterschiedlichen Quellen des Gesundheitswesens einfach und transparent zugänglich an einem zentralen Ort gebündelt werden.

Die Nutzung einer ePA ist für Versicherte freiwillig. Sowohl die Bereitstellung als auch der Zugriff auf die medizinischen Daten durch die sie behandelnden Ärztinnen und Ärzte, Zahnärztinnen und Zahnärzte, Apothekerinnen und Apotheker und der weiteren gesetzlich geregelten, zugriffsberechtigten Leistungserbringer, die in die Behandlung der Versicherten eingebunden sind, bedarf der Einwilligung der Versicherten.

Datenschutz und Datensicherheit haben neben dem Patientenwohl bei der Ausgestaltung der ePA im Patientendaten-Schutz-Gesetz (PDSG) von Beginn an eine herausragende Rolle gespielt. Dem tragen insbesondere das vorgesehene differenzierte Zugriffsmanagement, die umfangreich geregelten Informationspflichten der Krankenkassen sowie das ausdrückliche Diskriminierungsverbot (§ 335 SGB V in der Fassung des PDSG) Rechnung.

Die Bundesregierung ist der Auffassung, dass die ePA bereits in ihrer ersten Umsetzungsstufe datenschutzkonform ausgestaltet ist. Dies ist das Ergebnis eines intensiven Abstimmungsprozesses innerhalb der Bundesregierung sowie der Beratungen im Gesetzgebungsverfahren.

1. Welche Schlussfolgerungen zieht die Bundesregierung aus der Mitteilung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), und welche Handlungserfordernisse ergeben sich insbesondere mit Blick auf die rechtlichen Bedenken?

Der BfDI prüft Gesetzentwürfe nach datenschutzrechtlichen Gesichtspunkten. Die Bundesregierung nimmt diesbezügliche fachliche Bedenken des BfDI ernst. Allerdings wurde der Regierungsentwurf des PDSG von den sog. Verfassungsressorts (Bundesministerium der Justiz und für Verbraucherschutz sowie Bundesministerium des Innern, für Bau und Heimat) rechtlich umfassend insbesondere auch auf dessen Vereinbarkeit mit übergeordnetem Recht geprüft. Vor diesem Hintergrund teilt die Bundesregierung die Bedenken des BfDI an der Rechtskonformität des PDSG nicht.

Das Bundesministerium für Gesundheit befindet sich in einem kontinuierlichen fachlichen Austausch mit dem BfDI. Darüber hinaus ist das Bundesministerium für Gesundheit hierzu auch mit dem GKV-Spitzenverband und den Aufsichtsbehörden der Krankenkassen in Bund und Ländern in Gesprächen. Diesen ist insbesondere nach § 16 Absatz 1 Bundesdatenschutzgesetz (BDSG) vom BfDI Gelegenheit zur Stellungnahme zu geben, bevor datenschutzrechtliche Maßnahmen gegen einzelne Krankenkassen gerichtet würden.

2. Wie, und mit welcher Begründung ist den Bedenken des BfDI, die während des Gesetzgebungsverfahrens geäußert wurden, insbesondere zu den Spezifika der Datenschutz-Grundverordnung und des vorgesehenen Datenschutzniveaus, Rechnung getragen worden (bitte anhand der einzelnen Regelungsvorschläge begründen)?

Der BfDI war fortlaufend in die fachlichen Diskussionen eingebunden und hat maßgeblich an der Erarbeitung der Regelungen im Gesetzentwurf zum PDSG mitgewirkt. Dies betrifft zum Beispiel auch die technischen Vorgaben (Spezifikationen) der elektronischen Patientenakte durch die Gesellschaft für Telematik.

Die Bundesregierung ist indes, anders als der BfDI, nach wie vor der Auffassung, dass die Regelungen zur ePA gemessen an den Anforderungen der Datenschutz-Grundverordnung (DSGVO) bereits mit ihrem Start ab dem 1. Januar 2021 auch ohne ein differenziertes sog. feingranulares Rollen- und Rechtemanagement datenschutzkonform ausgestaltet sind. Ein wichtiges Kriterium hierfür ist die Ausgestaltung der ePA als freiwillige Anwendung, über deren Funktionsweise die Krankenkassen umfassend informieren müssen. Das ausdrücklich normierte Diskriminierungsverbot in § 335 SGB V in der Fassung des PDSG gewährleistet zudem eine echte Wahlfreiheit. Die Behandlung durch die Leistungserbringer darf nicht etwa vom Vorhandensein einer ePA bzw. von einer Zugriffserteilung auf die ePA abhängig gemacht werden.

Darüber hinaus können die Versicherten bereits in der ersten Umsetzungsstufe ab dem 1. Januar 2021 frei entscheiden, welche Daten im Einzelnen in der ePA gespeichert und welche Daten dort nicht aufgenommen oder wieder gelöscht werden sollen. Frei entscheiden können sie ebenfalls, welcher Ärztin oder welchem Arzt sie Zugriff erteilen oder aber versagen wollen, und nötigenfalls einzelne Dokumente in einem geschützten Bereich speichern. Denn es gilt auch schon in der ersten Ausbaustufe nicht das „Alles-oder-nichts-Prinzip“. Vielmehr besteht die Wahlmöglichkeit, indem der Zugriff zum Beispiel ausdrücklich nicht für die durch die Versicherten selbst eingestellten Daten erteilt oder – alternativ – ausschließlich hierauf begrenzt wird. Auch steht es den Versicherten frei, jederzeit alle Daten der ePA zu löschen.

Der Freiwilligkeit steht auch nicht entgegen, dass die Versicherten in der ersten Umsetzungsstufe der ePA keine dokumentenbezogene Einwilligung erteilen können. Anhaltspunkte dafür, dass die DSGVO eine bestimmte Granularität der Einwilligung hinsichtlich der konkreten Daten fordert, sind nicht ersichtlich. Die DSGVO gibt auch nicht zwingend eine bestimmte Form der ePA als einzig europarechtskonform vor. Vielmehr eröffnet sie den Mitgliedstaaten weitreichende Gestaltungsspielräume. Das zeigt das heterogene Bild in der Europäischen Union. Die Bundesregierung hat mit dem PDSG von den Gestaltungsspielräumen der DSGVO im Sinne des absoluten Vorrangs der Patientensouveränität Gebrauch gemacht.

3. Warum ist für Nutzende von geeigneten Endgeräten wie Mobiltelefonen oder Tablets eine dokumentengenaue Kontrolle in der ePA erst ab 2022 vorgesehen?

   a) Warum fehlen Regelungen für Patientinnen und Patienten, die nicht im Besitz von geeigneten Endgeräten sind?

   b) Wie wird sichergestellt, dass auch Personen ohne geeignete Endgeräte einen datenschutzrechtlich ausreichenden Zugriff auf ihre ePA erhalten?

Die Fragen 3 bis 3b werden gemeinsam beantwortet.

Die Einführung der ePA erfolgt stufenweise. Ab dem 1. Januar 2021 wird in der ersten Umsetzungsstufe für die Versicherten die Möglichkeit geschaffen, umfassende medizinische Informationen im Rahmen ihrer persönlichen medizinischen Behandlung bereitzustellen und durch eine bessere Verfügbarkeit dieser Daten die Therapieentscheidung der sie mit- und weiterbehandelnden Ärztinnen und Ärzte zu unterstützen.

Das technisch aufwändigere feingranulare Berechtigungskonzept folgt zum 1. Januar 2022.

Somit steht die ePA bereits 2021 all den Versicherten zur Verfügung, die diese auch ohne die Möglichkeit der Erteilung feingranularer Zugriffsrechte schon nutzen möchten.

Versicherte ohne ein geeignetes Endgerät können zum einen – soweit möglich – auf die Nutzung von Geräten vertrauter Personen, wie zum Beispiel Familienangehöriger, zurückgreifen. Zum anderen können sie über eine Vollmachterteilung an eine Vertreterin oder einen Vertreter ihre Rechte wahrnehmen lassen. Hierüber werden sie über das geeignete Informationsmaterial der Krankenkassen nach § 343 SGB V in der Fassung des PDSG umfassend aufgeklärt. Auf diese Weise wird sichergestellt, dass sich auch Versicherte, die eine ePA nicht selbst über eine Benutzeroberfläche eines geeigneten Endgeräts verwalten wollen oder können, ohne wesentliche Abstriche bei den Funktionalitäten für eine ePA entscheiden können. Dies ist auch datenschutzkonform. Denn weder die DSGVO noch das Recht auf informationelle Selbstbestimmung gewähren einen Anspruch auf ein bestimmtes System. Das Recht, jederzeit bestimmen zu können, wer Kenntnis von den eigenen Daten erhält, ist gewahrt, wenn die oder der Betroffene, wie im Konzept für die ePA vorgesehen, eine Alternative hat, auch wenn diese nicht alle möglichen technischen Vorteile beinhaltet.

4. Aus welchen Gründen ist auf eine Regelung verzichtet worden, die es den Krankenkassen ermöglicht hätte, ihren Versicherten über die gesetzlichen Vorgaben hinaus einen „feingranularen Zugriff“ auf die von den Leistungserbringern gespeicherten Inhalte der ePA zu gewähren?

Die Spezifikationen zu den feingranularen Zugriffsrechten wurden von der Gesellschaft für Telematik veröffentlicht und können entsprechend von den Krankenkassen umgesetzt werden. Um die Interoperabilität zu gewährleisten, müssen aber die Softwarekomponenten koordiniert von allen Krankenkassen, Arztpraxen, Krankenhäusern und weiteren Leistungserbringern angepasst werden. Dies ist zum 1. Januar 2022 vorgesehen.

5. Welche datenschutzrechtlichen Anforderungen werden an das Authentifizierungsverfahren für die ePA per Frontend gestellt?

6. Worauf ist mit Blick auf die Authentifizierungsverfahren ohne Einsatz der elektronischen Gesundheitskarte während der Übergangsfrist nach Auffassung der Bundesregierung zu achten, um den Vorgaben der DSGVO nachzukommen?

Die Fragen 5 und 6 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Ziel der ePA ist es, möglichst vielen Versicherten eine sichere und gleichzeitig benutzerfreundliche Möglichkeit zur Verwaltung ihrer persönlichen Gesundheitsdaten anzubieten – auch ohne Nutzung einer Chipkarte wie der elektronischen Gesundheitskarte (eGK) oder des neuen elektronischen Personalausweises. Für den benutzerfreundlichen und sicheren Zugriff auf die ePA stehen den Versicherten mehrere Möglichkeiten zur Verfügung, über deren Besonderheiten die Versicherten umfassend informiert werden müssen.

Im Kern ergeben sich die Anforderungen an diese sicheren Verfahren aus Artikel 32 Absatz 1 und 2 DSGVO. Hiernach ist der Verantwortliche – hier die jeweilige Krankenkasse – 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. Der Stand der Technik wird durch die enge Einbindung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) gewährleistet.

Für alternative Authentifizierungsverfahren ohne Nutzung der elektronischen Gesundheitskarte fordert das PDSG für den Zugriff auf die elektronische Patientenakte „ein geeignetes technisches Verfahren, das einen hohen Sicherheitsstandard gewährleistet“. Damit sind die Anforderungen der DSGVO jedenfalls erfüllt. Art. 32 Absatz 1 und 2 DSGVO – ebenso wie Art. 25 Absatz 1 DSGVO – geben keine konkreten technischen Methoden der Datensicherheit vor. Insbesondere schreiben sie nicht vor, dass im speziellen Fall eines Authentifizierungsverfahrens bestimmte Sicherheitsmaßnahmen zu ergreifen wären.

Die konkreten sicheren Verfahren werden im kontinuierlichen Austausch mit dem BfDI und dem BSI sowie der Gesellschaft für Telematik unter Berücksichtigung des jeweiligen Stands der Technik weiterentwickelt.

7. Wie stellt die Bundesregierung sicher, dass alle Anwendungen der Telematikinfrastruktur, insbesondere die ePA, allen europarechtlichen Datenschutzbestimmungen entsprechen?

8. Welche Maßnahmen plant die Bundesregierung für Verstöße gegen den Datenschutz in der ePA, und wie sollen Verstöße geahndet werden?

Die Fragen 7 und 8 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die Einhaltung eines hohen Datenschutz- und Datensicherheitsniveaus, das auch den europarechtlichen Datenschutzbestimmungen entspricht, wird durch technische und rechtliche Vorgaben sichergestellt.

Alle Anwendungen, Komponenten und Dienste, die in der Telematikinfrastruktur zum Einsatz kommen, unterliegen strengen Sicherheitsvorgaben, deren Ein-

haltung sowohl im Rahmen aufwändiger Zulassungsverfahren als auch später im Betrieb durch die Gesellschaft für Telematik nach den entsprechenden Sicherheitsvorgaben des BSI überwacht werden.

Die Verarbeitung der Gesundheitsdaten in der Telematikinfrastruktur darf nur im Rahmen der engen gesetzlichen, auch technisch abgebildeten Vorgaben und mit dem Einverständnis der Versicherten erfolgen. Um einen Missbrauch von Daten der medizinischen Anwendungen der elektronischen Gesundheitskarte ahnden zu können, sind Zuwiderhandlungen straf- bzw. bußgeldbewehrt. Das PDSG sieht dabei mit Blick auf die mit der Einführung von medizinischen Anwendungen gewachsenen Abhängigkeit von der Sicherheit der Telematikinfrastruktur eine deutliche Erhöhung des Bußgeldrahmens sowie weitere Bußgeldtatbestände vor.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333