BfDI zu Folgen der Gesetzgebung des PDSG

Berlin, 19. August 2020

Ausgabe 20/2020
Datum 19.08.2020

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) *Professor Ulrich Kelber* weist auf die Folgen einer europarechtswidrigen Verarbeitung personenbezogener Gesundheitsdaten als Folge des Patientendaten-Schutz-Gesetzes (PDSG) hin: Meine Behörde wird aufsichtsrechtliche Maßnahmen gegen die gesetzlichen Krankenkassen in meiner Zuständigkeit ergreifen müssen, wenn das PDSG in seiner derzeitigen Fassung umgesetzt werden sollte. Meiner Auffassung nach verstößt eine Einführung der elektronischen Patientenakte (ePA) ausschließlich nach den Vorgaben des PDSG an wichtigen Stellen gegen die europäische Datenschutz-Grundverordnung (DSGVO).

Der BfDI hat in seinen Stellungnahmen während des Gesetzgebungsverfahrens mehrfach darauf hingewiesen, dass Patientinnen und Patienten bei Einführung der ePA die volle Hoheit über ihre Daten besitzen müssen. Hier weist das vom Deutschen Bundestag beschlossene PDSG, das derzeit im Bundesrat beraten wird, Defizite auf: Gesundheitsdaten offenbaren intimste Informationen über die Bürgerinnen und Bürger. Deswegen sind sie in der europaweit geltenden DSGVO auch besonders geschützt. Sollte das PDSG unverändert beschlossen werden, muss ich die meiner 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. Außerdem bereite ich in diesem Zusammenhang weitere Maßnahmen vor, um einer europarechtswidrigen Umsetzung der ePA abzuhelfen. Nach der DSGVO stehen mir dazu neben Anweisungen auch Untersagungen zur Verfügung.

Das PDSG sieht nur für Nutzende von geeigneten Endgeräten wie Mobiltelefonen oder Tablets einen datenschutzrechtlich ausreichenden Zugriff auf ihre eigene ePA vor, nämlich eine dokumentengenaue Kontrolle, welche Beteiligten welche Informationen einsehen können. Und selbst diese Möglichkeit soll es erst ein Jahr nach Einführung der ePA geben. Das bedeutet, dass 2021 keine Steuerung auf Dokumentenebene vorgesehen ist. Die Nutzerinnen und Nutzer werden in Bezug auf die von den Leistungserbringern in der ePA gespeicherten Daten zu einem „Alles oder Nichts“ gezwungen. Jede Person, der die Versicherten Einsicht in diese Daten gewähren, kann alle dort enthaltenen Informationen einsehen. Beispielsweise könnte der behandelnde Zahnarzt alle Befunde des konsultierten Psychiaters sehen.

Dass es die für den Start der ePA am 1.1.2021 maßgebenden Spezifikationen den Krankenkassen nicht ermöglichen, ihren Versicherten über die gesetzlichen Vorgaben hinausgehend einen sogenannten feingranularen Zugriff auf die von den Leistungserbringern gespeicherten Inhalte der ePA zu gewähren, sieht *der Bundesbeauftragte* mit Unverständnis: Digitalisierung kann niemals Selbstzweck sein. Der Schutz der Versicherten und ihrer Gesundheitsdaten muss immer im Vordergrund stehen.

Darüber hinaus ist im PDSG für die Menschen, die das so genannte Frontend auf Handy oder Tablet nicht nutzen können oder wollen, keine eigenständige Einsicht in die ePA und auch keine Prüfung von erfolgten Zugriffen auf die Daten geregelt. Ab 2022 soll alternativ für diese Frontend-Nicht-Nutzenden eine vertretende Person die Steuerung und Einsicht vornehmen können, der die Versicherten dann aber volle Kontrolle über ihre Daten einräumen müssten.

Der BfDI stellt sich entschieden gegen diese Ungleichbehandlung beim Grundrecht der Bürgerinnen und Bürger auf informationelle Selbstbestimmung: Die ePA ist ein wichtiger Schritt zu weiteren Verbesserungen in der Gesundheitsversorgung. Die dabei anfallenden Gesundheitsdaten benötigen ein Datenschutzniveau, wie es die DSGVO vorschreibt und wie es seit Jahren in Deutschland für die ePA fest vereinbart war. Das PDSG in seiner aktuellen Form wird dem nicht ausreichend gerecht. Als zuständige Aufsichtsbehörde für einen Großteil der gesetzlichen Krankenkassen werde ich deshalb mit den mir zur Verfügung stehenden aufsichtsrechtlichen Mitteln dafür Sorge tragen, dass diese Krankenkassen mit der von ihnen angebotenen ePA nicht gegen europäisches Recht verstoßen.

Ein weiterer Kritikpunkt ist das Authentifizierungsverfahren für die ePA, mit dem sich Versicherte per Frontend anmelden. Dieses ist bisher aus Datenschutzsicht nicht ausreichend sicher und entspricht nicht den Vorgaben der DSGVO. Der BfDI bereitet entsprechende Warnungen und Weisungen vor, damit die Krankenkassen nur nach Nutzung eines nach Stand der Technik hochsicheren Authentifizierungsverfahrens Zugriffe auf Gesundheitsdaten erlauben. Dies gilt insbesondere für Authentifizierungsverfahren ohne Einsatz der elektronischen Gesundheitskarte (so genannte alternative Authentifizierungen), für die eine gewährte Übergangsfrist im Mai 2021 abläuft.

Der BfDI ist zuständig für 65 gesetzliche Krankenkassen. Eine Liste der betroffenen Krankenkassen ist auf der Internetseite des BfDI abrufbar.