Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Prof. Ulrich Kelber
Bundesbeauftragter
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 1468, 53004 Bonn

An die
gesetzlichen Krankenkassen
im Zuständigkeitsbereich des
Bundesbeauftragten für den Datenschutz
und die Informationsfreiheit

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn

FON (0228) 997799-5000
FAX (0228) 997799-5550

E-MAIL referat13@bfdi.bund.de

INTERNET www.bfdi.bund.de

DATUM Bonn, 06.11.2020
GESCHÄFTSZ. 13-315/105#1147

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

BETREFF **Warnung nach Artikel 58 Abs. 2 Buchst. a) DSGVO**
HIER Defizitäres Berechtigungsmanagement bei der elektronischen Patientenakte
BEZUG Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (PDSG) vom 14. Oktober 2020 - BGBl. I S. 2115

Sehr geehrte Damen und Herren,

gemäß Art. 58 Abs. 2 Buchst. a) Datenschutz-Grundverordnung (DSGVO) warne ich hiermit davor, lediglich die im PDSG enthaltenen Vorgaben zur technischen Ausgestaltung der elektronischen Patientenakte (ePA) einzuhalten und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA zu verzichten. Dies würde gegen Artikel 25 und 32 DSGVO verstoßen.

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz, PDSG) vom 14. Oktober 2020 wurde im Bundesgesetzblatt vom 19. Oktober 2020 veröffentlicht (BGBl. 2020, S. 2115) und trat aufgrund seines Artikels 9 am Tag nach der Verkündung der Gesetzes am 20. Oktober 2020 in Kraft.

Die datenschutzrechtliche Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7 zweite Alternative DSGVO i.V.m. § 341 Abs. 4 SGB V), so dass diese Warnung an Sie zu adressieren ist.

ZUSTELL- UND LIEFERANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

I.

Mit dem PDSG wurden im Fünften Buch Sozialgesetzbuch (SGB V) u.a. die Vorgaben zur elektronischen Gesundheitskarte neu gefasst und Regelungen für eine ePA ausgestaltet. § 341 Abs. 1 SGB V verpflichtet die Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Die Pflicht, eine ePA zur Verfügung zu stellen, gilt nach § 342 Abs. 1 SGB V ab dem 1. Januar 2021.

Die weiteren technischen Vorgaben wurden in § 342 Abs. 2 SGB V geregelt. Hinsichtlich der Freigabe der Dokumente gilt dabei nach § 342 Abs. 2 Nr. 2 Buchst. b) SGB V erst ab dem 1. Januar 2022 ein sog. feingranulares Zugriffsmanagement für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgeräts zugreifen können. Erst ab diesem Zeit-punkt ist vorgesehen, dass die Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 Buchst. c) SGB V lediglich ein Differenzierung nach Daten nach § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und nach § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrackern) möglich. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann.

Für die Versicherten, die kein geeignetes Endgerät (Smartphone, PC), sondern die dezentrale Infrastruktur der Leistungserbringer nutzen , ist ab dem 1. Januar 2022 die Erteilung der Zugriffsberechtigung lediglich auf Kategorien von Dokumenten möglich (sogen. mittelgranulares Zugriffsmanagement).Alternativ können, diese Versicherten einen Vertreter bestimmen und diesen berechtigen, die ePA-Daten zu verwalten (§ 342 Abs. 2 Nr. 2 Buchst. e) SGB V).

II.

Diese Regelungen bleiben deutlich hinter den datenschutzrechtlichen Anforderungen zurück. Ich verweise insoweit auf meine Stellungnahmen gegenüber dem Gesundheitsausschuss des Deutschen Bundestages vom 3. April und 25. Mai 2020, die Sie auf meiner Homepage unter dem Menüpunkt Infothek/Transparenz/Stellungnahmen finden.

Die oben dargestellten Regelungen enthalten bereits einen Wertungswiderspruch zu der in § 341 Abs. 1 Satz 1 PDSG enthaltenen Prämisse, dass die ePA vom Versicherten eigenständig geführt wird. Unabdingbar für eine rechtskonforme, selbstbestimmte Nutzung der ePA durch die Versicherten ist, dass alle Versicherten auch ohne eigenes Endgerät eigenständig auf ihre ePA zugreifen können. Dies ist der Anspruch, den das PDSG selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Abs. 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Abs. 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Abs. 2 SGB V). Dieser im PDSG selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Zudem stehen die Regelungen im Widerspruch zu den Vorgaben der DSGVO.

Nach Art. 25 DSGVO trifft der Verantwortliche geeignete technische und organisatorische Maßnahmen um die Verarbeitungsgrundsätze wie Datenminimierung umzusetzen und Garantien zum Schutz der Rechte der betroffenen Person aufzunehmen. Hierzu gehören nach Art. 25 Abs. 2 DSGVO auch datenschutzfreundliche Voreinstellungen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Damit wird den datenschutzrechtlichen Verarbeitungsgrundsätzen der Datenminimierung (Art. 5 Abs. 1 Buchst. c) DSGVO), der Erforderlichkeit und Zweckbindung (Art. 5 Abs. 1 Buchst. b) DSGVO) sowie der Vertraulichkeit (Art. 5 Abs. 1 Buchst. f) DSGVO) entsprochen.

Sollte zu Beginn also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt werden, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Art. 25 sowie Art. 5 Abs. 1 Buchst. b), c) und f) DSGVO.

Wie ich bereits vor der Bundespressekonferenz am 19. August 2020 erklärt habe, werde ich im Fall, dass bei einem Angebot für eine ePA einer gesetzlichen Krankenkasse, in dem kein feingra¬nulares Zugriffsmanagement vorgesehen ist, prüfen, ob weitere Maßnahmen nach Art. 58 Abs. 2 DSGVO erforderlich werden, um die Einhaltung der datenschutzrechtlichen Vorgaben der DSGVO zu gewährleisten. Ich verweise insoweit auf meine Pressemitteilung vom 19 August 2020, die Sie auf meiner Homepage finden.

Ich rege daher dringend an, dass Ihre Krankenkasse ab dem 1. Januar 2021 ihren Versicherten nur eine solche elektronische Patientenakte anbietet, die den aufgezeigten Vorgaben der DSGVO entspricht.

Ich wäre Ihnen dankbar, wenn Sie mir mitteilen würden, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Mit freundlichen Grüßen

Ulrich Kelber