Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

An den
Vorstand der
Audi BKK
Ferdinand-Braun-Straße 6
85053 Ingolstadt

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET
Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der Audi BKK gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die Audi BKK gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 28. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

An den
Vorstand der
Bertelsmann BKK Carl-
Miele-Str. 214 33311
Gütersloh

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der Bertelsmann BKK gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die Bertelsmann BKK gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

An den
Vorstand der
BKK Deutsche Bank AG
Königsallee 60c
40212 Düsseldorf

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der BKK Deutsche Bank AG gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die BKK Deutsche Bank AG gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

An den
Vorstand der
BKK Diakonie
Königsweg 8
33617 Bielefeld

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der BKK Diakonie gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die BKK Diakonie gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

An den
Vorstand der
BKK exklusiv
Zum Blauen See 7
31275 Lehrte

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der BKK exklusiv gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die BKK exklusiv gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 29. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

An den
Vorstand der
Betriebskrankenkasse firmus Gottlieb-Daimler-Str. 11
28237 Bremen

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der Betriebskrankenkasse firmus gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die Betriebskrankenkasse firmus gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

An den
Vorstand der
BKK Freudenberg
Höhnerweg 2 - 4
69469 Weinheim

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON
FAX (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der BKK Freudenberg gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die BKK Freudenberg gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 28. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET
DATUM Bonn, 04.05.2021
GESCHÄFTSZ. 13-315/105#1147
Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

An den
Vorstand der
BKK GILDEMEISTER SEIDENSTICKER
Winterstraße 49
33649 Bielefeld

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der BKK GILDEMEISTER SEIDENSTICKER gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die BKK GILDEMEISTER SEIDENSTICKER gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

An den
Vorstand der
Betriebskrankenkasse Herford Minden
Ravensberg (BKK HMR)
Am Kleinbahnhof 5
32051 Herford

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der Betriebskrankenkasse Herford Minden Ravensberg (BKK HMR) gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die Betriebskrankenkasse Herford Minden Ravensberg (BKK HMR) gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET
DATUM Bonn, 04.05.2021
GESCHÄFTSZ. 13-315/105#1147
Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

An den
Vorstand der
BKK Linde
Konrad-Adenauer-Ring 33
65187 Wiesbaden

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der BKK Linde gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die BKK Linde gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder

An den
Vorstand der
BKK Melitta Plus
Marienstr. 122
32425 Minden

INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der BKK Melitta Plus gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die BKK Melitta Plus gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 28. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

An den
Vorstand der
Betriebskrankenkasse Miele
Carl-Miele-Straße 29
33332 Gütersloh

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der Betriebskrankenkasse Miele gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die Betriebskrankenkasse Miele gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

An den
Vorstand der
Mobil Betriebskrankenkasse
Friedenheimer Brücke 29
80639 München

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der Mobil Betriebskrankenkasse gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die Mobil Betriebskrankenkasse gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 29. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder

An den
Vorstand der
BKK MTU
Hochstraße 40
88045 Friedrichshafen

INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der BKK MTU gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die BKK MTU gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET
DATUM Bonn, 04.05.2021
GESCHÄFTSZ. 13-315/105#1147
Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

An den
Vorstand der
BKK Pfalz
Lichtenbergerstraße 16
67059 Ludwigshafen

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der BKK Pfalz gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die BKK Pfalz gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

An den
Vorstand der
BKK ProVita
Rotkreuzplatz 8
80634 München

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der BKK ProVita gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die BKK ProVita gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 28. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

An den
Vorstand der
BKK PwC
Burgstraße 1 - 3
34212 Melsungen

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der BKK PwC gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die BKK PwC gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 28. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

An den
Vorstand der
Betriebskrankenkasse RWE
Welfenallee 32
29225 Celle

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der Betriebskrankenkasse RWE gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die Betriebskrankenkasse RWE gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 28. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

An den
Vorstand der
BKK Salzgitter
Thiestr. 15
38226 Salzgitter

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der BKK Salzgitter gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die BKK Salzgitter gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

An den
Vorstand der
BKK Technoform
August-Spindler-Straße 1
37079 Göttingen

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der BKK Technoform gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die BKK Technoform gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 28. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET
DATUM Bonn, 04.05.2021
GESCHÄFTSZ. 13-315/105#1147
Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

An den
Vorstand der
BKK VBU
Lindenstraße 67
10969 Berlin

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der BKK VBU gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die BKK VBU gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET
DATUM Bonn, 04.05.2021
GESCHÄFTSZ. 13-315/105#1147
Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

An den
Vorstand der
BKK VerbundPlus
Zeppelinring 13
88400 Biberach

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der BKK VerbundPlus gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die BKK VerbundPlus gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 28. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

An den
Vorstand der
BKK WIRTSCHAFT & FINANZEN
Bahnhofstraße 19
34212 Melsungen

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn

FON (0228) 997799-1301
FAX (0228) 997799-5550

E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET www.bfdi.bund.de
DATUM Bonn, 04.05.2021
GESCHÄFTSZ. 13-315/105#1147

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

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

ANHÖRUNG

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der BKK WIRTSCHAFT & FINANZEN gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die BKK WIRTSCHAFT & FINANZEN gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

An den
Vorstand der
BKK Würth
Gartenstraße 11
74653 Künzelsau

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der BKK Würth gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die BKK Würth gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

An den
Vorstand der
BKK ZF & Partner
Am Wöllershof 12
56068 Koblenz

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der BKK ZF & Partner gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die BKK ZF & Partner gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder

An den
Vorstand der
BMW BKK
Mengkofener Str. 6
84130 Dingolfing

INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der BMW BKK gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die BMW BKK gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

An den
Vorstand der
Bosch BKK
Kruppstraße 19
70469 Stuttgart

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der Bosch BKK gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die Bosch BKK gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET
DATUM Bonn, 04.05.2021
GESCHÄFTSZ. 13-315/105#1147
Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

An den
Vorstand der
Continentale Betriebskrankenkasse
Sengelmannstr. 120
22335 Hamburg

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der Continentale Betriebskrankenkasse gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die Continentale Betriebskrankenkasse gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 28. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder

An den
Vorstand der
Daimler BKK
Mercedesstr.1
28309 Bremen

INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der Daimler BKK gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die Daimler BKK gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 28. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder

An den
Vorstand der
Debeka BKK
Im Metternicher Feld 40
56072 Koblenz

INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der Debeka BKK gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die Debeka BKK gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 29. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

An den
Vorstand der
energie-BKK
Oldenburger Allee 24
30659 Hannover

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der energie-BKK gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die energie-BKK gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 28. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder

An den
Vorstand der
Ernst & Young BKK
Rotenburger Str. 16
34212 Melsungen

INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der Ernst & Young BKK gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die Ernst & Young BKK gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 29. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

An den
Vorstand der
Heimat Krankenkasse
Herforder Straße 23
33602 Bielefeld

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der Heimat Krankenkasse gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die Heimat Krankenkasse gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 28. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

An den
Vorstand der
mhplus Betriebskrankenkasse
Franckstraße 8
71636 Ludwigsburg

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn

FON (0228) 997799-1301
FAX (0228) 997799-5550

E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET www.bfdi.bund.de
DATUM Bonn, 04.05.2021
GESCHÄFTSZ. 13-315/105#1147

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

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

ANHÖRUNG

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der mhplus Betriebskrankenkasse gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die mhplus Betriebskrankenkasse gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET
DATUM Bonn, 04.05.2021
GESCHÄFTSZ. 13-315/105#1147
Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

An den
Vorstand der
Novitas BKK
Schifferstraße 92-100
47059 Duisburg

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der Novitas BKK gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die Novitas BKK gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

An den
Vorstand der
pronova BKK
Rheinallee 13
67061 Ludwigshafen

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der pronova BKK gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die pronova BKK gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

An den
Vorstand der
R+V Betriebskrankenkasse
Kreuzberger Ring 21
65205 Wiesbaden

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der R+V Betriebskrankenkasse gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die R+V Betriebskrankenkasse gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 28. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

An den
Vorstand der
Salus BKK
Züricher Straße 27
81476 München

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON
FAX (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET
Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der Salus BKK gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die Salus BKK gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder

An den
Vorstand der
SECURVITA BKK
Lübeckertordamm 1-3
20099 Hamburg

INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der SECURVITA BKK gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die SECURVITA BKK gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 28. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder

An den
Vorstand der
SIEMAG BKK
Hillnhütter Str. 89
57271 Hilchenbach

INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der SIEMAG BKK gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die SIEMAG BKK gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

An den
Vorstand der
SBK Siemens-Betriebskrankenkasse
In den Seewiesen 26
89520 Heidenheim

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der SBK Siemens-Betriebskrankenkasse gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die SBK Siemens-Betriebskrankenkasse gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 28. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder

An den
Vorstand der
Südzucker BKK
Joseph-Meyer-Str. 13-15
68167 Mannheim

INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der Südzucker BKK gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die Südzucker BKK gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder

An den
Vorstand der
TUI BKK
Karl-Wiechert-Allee 23
30625 Hannover

INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der TUI BKK gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die TUI BKK gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET
DATUM Bonn, 04.05.2021
GESCHÄFTSZ. 13-315/105#1147
Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

An den
Vorstand der
VIACTIV Krankenkasse
Universitätsstraße 43
44789 Bochum

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der VIACTIV Krankenkasse gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die VIACTIV Krankenkasse gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 29. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

An den
Vorstand der
vivida bkk
Spittelstraße 50
78056 Villingen-Schwenningen

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn

FON (0228) 997799-1301
FAX (0228) 997799-5550

E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET www.bfdi.bund.de
DATUM Bonn, 04.05.2021
GESCHÄFTSZ. 13-315/105#1147

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

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

ANHÖRUNG

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der vivida bkk gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die vivida bkk gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 28. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

An den
Vorstand der
Wieland BKK
Graf-Arco Straße 36
89079 Ulm

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der Wieland BKK gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die Wieland BKK gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 29. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

An den
Vorstand der
WMF Betriebskrankenkasse
Eberhardstraße
73312 Geislingen

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der WMF Betriebskrankenkasse gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die WMF Betriebskrankenkasse gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

An den
Vorstand der
BundesInnungskrankenkasse Gesundheit
(BIG direkt gesund)
Rheinische Straße 1
44137 Dortmund

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn

FON (0228) 997799-1301
FAX (0228) 997799-5550

E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET www.bfdi.bund.de
DATUM Bonn, 04.05.2021
GESCHÄFTSZ. 13-315/105#1147

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

BETREFF **Anhörung**

HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)

BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

ANHÖRUNG

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der BundesInnungskrankenkasse Gesundheit (BIG direkt gesund) gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die BundesInnungskrankenkasse Gesundheit (BIG direkt gesund) gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

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

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 28. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET
DATUM Bonn, 04.05.2021
GESCHÄFTSZ. 13-315/105#1147
Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

An den
Vorstand der
IKK classic
Tannenstraße 4 b
01099 Dresden

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der IKK classic gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die IKK classic gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 29. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

An den
Vorstand der
IKK gesund plus
Umfassungsstraße 85
39124 Magdeburg

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der IKK gesund plus gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die IKK gesund plus gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 28. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

An den
Vorstand der
IKK - Die Innovationskasse
Lachswehrallee 1
23558 Lübeck

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der IKK - Die Innovationskasse gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die IKK - Die Innovationskasse gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET
DATUM Bonn, 04.05.2021
GESCHÄFTSZ. 13-315/105#1147
Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

An den
Vorstand der
BARMER
Axel-Springer-Straße 44
10969 Berlin

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der BARMER gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die BARMER gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 28. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder

An den
Vorstand der
BARMER
Lichtscheider Str. 89 - 95
42285 Wuppertal

INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der BARMER gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die BARMER gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 28. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

An den
Vorstand der DAK-
Gesundheit Nagelsweg
27 - 31 20097 Hamburg

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON
FAX (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der DAK-Gesundheit gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die DAK-Gesundheit gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 28. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET
DATUM Bonn, 04.05.2021
GESCHÄFTSZ. 13-315/105#1147
Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

An den
Vorstand der
HEK - Hanseatische Krankenkasse
Wandsbeker Zollstraße 86 - 90
22041 Hamburg

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der HEK - Hanseatische Krankenkasse gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die HEK - Hanseatische Krankenkasse gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 27. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON
FAX (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

An den
Vorstand der
Handelskrankenkasse (hkk)
Martinistraße 26
28195 Bremen

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

ANHÖRUNG

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der Handelskrankenkasse (hkk) gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die Handelskrankenkasse (hkk) gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 28. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET Bonn, 04.05.2021
DATUM 13-315/105#1147
GESCHÄFTSZ. **Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

An den
Vorstand der
Kaufmännische Krankenkasse - KKH
Karl-Wiechert-Allee 61
30625 Hannover

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der Kaufmännische Krankenkasse - KKH gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die Kaufmännische Krankenkasse - KKH gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 28. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
F O N
F A X (0228) 997799-1301
(0228) 997799-5550
E-MAIL referat13@bfdi.bund.de
BEARBEITET VON Frau Dr. Schräder
INTERNET
DATUM Bonn, 04.05.2021
GESCHÄFTSZ. 13-315/105#1147
Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

An den
Vorstand der
Techniker Krankenkasse
Bramfelder Straße 140
22305 Hamburg

BETREFF **Anhörung**
HIER Anhörung nach § 28 VwVfG zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 lit. d) DSGVO (Anweisung)
BEZUG Mein Schreiben vom 6. November 2020 - 13-315/105#1147
(Datenschutzrechtliche Warnung nach Artikel 58 Absatz 2 lit. a) DSGVO)

A N H Ö R U N G

Sehr geehrte Damen und Herren,

ich beabsichtige gegenüber der Techniker Krankenkasse gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) im Hinblick auf die die Einführung der elektronischen Patientenakte (ePA) folgende Abhilfemaßnahmen zu erlassen:

Ich beabsichtige, die Techniker Krankenkasse gemäß Art. 58 Abs. 2 lit. d) DSGVO anzuweisen, das Zugriffsmanagement der ePA bis zum 31. Dezember 2021 so auszugestalten, das ein feingranulares Zugriffsmanagement für alle Versicherten möglich ist. Das Zugriffsmanagement ist so auszugestalten, dass die Versicherten – auch ohne die Bestellung eines Vertreters –

a. eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 Fünftes Buch Sozialgesetzbuch (SGB V) in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen können.
b. in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.

VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Begründung:

I.
Zum Sachverhalt

1. Sozialgesetzliche Grundlagen der ePA

Das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 (BGBl. I, S. 2115) trat am 20. Oktober 2020 in Kraft.

Mit diesem Gesetz 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 gesetzlichen Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Diese Pflicht 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 gemäß § 342 Abs. 2 Nr. 2 lit. 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 Zeitpunkt ist im SGB V vorgesehen, dass diese Versicherten die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können. Bis dahin ist nach § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich ein Differenzierung nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten des Versicherten, z.B. aus Fitnesstrakkern) geregelt. Hinsichtlich der wichtigen medizinischen Informationen gilt demnach das „Alles oder Nichts-Prinzip“, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) eingestellte Dokumente berechtigt werden kann oder auf keine.

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

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 habe ich Sie gemäß Art. 58 Abs. 2 lit. a) DSGVO gewarnt, dass Sie gegen Art. 25 und 32 DSGVO verstoßen werden, wenn sie sich lediglich auf die im SGV V enthaltenen Vorgaben zur technischen Ausgestaltung der ePA beschränken und auf ein feingranulares Berechtigungsmanagement bei der Einführung der ePA verzichten.

Außerdem habe ich um Mitteilung gebeten, in welcher Form Sie Ihren Versicherten die ePA ab dem 1. Januar 2021 anbieten werden.

Hierzu haben Sie mir mit Schreiben vom 28. Januar 2021 mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement nach § 342 Abs. 2 Nr. 2 lit. b) SGB V für Versicherte, die über die Benutzeroberfläche eines geeigneten Endgerätes zugreifen können, nicht vorsehe. Dieses sei jedoch Regelungsinhalt der zum 30. Juni 2020 verabschiedeten Spezifikation der ePA der gematik ab der Version 2.0 (Release 4.0.0), deren technische Umsetzung bis zum 1. Januar 2021 zeitlich unmöglich gewesen sei. Daher sei die Umsetzung dieser Spezifikation für die sogenannte zweite Stufe der ePA vorgesehen, die den Versicherten durch die Krankenkassen ab dem 1. Januar 2022 zur Verfügung zu stellen ist. Dies entspreche der Vorgabe des § 342 Abs. 2 Nr. 2 SGB V.

Nach dem mir derzeit bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihnen Versicherten seit 1. Januar 2021 eine ePA anbieten, die kein feingranulares Zugriffsmanagement aufweist. Die Versicherten ohne Frontend (Benutzeroberfläche eines geeigneten Endgerätes wie z.B. Smartphone, Tablet) können keine Einsicht in ihre eigene patientengeführte ePA nehmen.

II.
Rechtliche Würdigung

Gemäß Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen, wenn er mit Verarbeitungsvorgängen gegen die DSGVO verstößt.

Diese Voraussetzungen sind nach den bisherigen Sachverhaltsermittlungen hier erfüllt.

1. Datenschutzrechtliche Verantwortlichkeit

Die Verantwortlichkeit für die Datenverarbeitung in der ePA hat der Gesetzgeber den Krankenkassen zugewiesen (Art. 4 Nr. 7, 2. Alt. DSGVO i. V. m. § 341 Abs. 4 SGB V), so dass Sie für die Einhaltung der DSGVO verantwortlich sind und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Gegenwärtiger Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten, ohne allen Versicherten ein feingranulares Zugriffsmanagement bereitzustellen.

2.1. Verpflichtung auf ein feingranulares Zugriffsmanagement nach der DSGVO

Gemäß Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik, geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Verarbeitungsgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nach aktuellem Stand der Technik ist ein dokumentenspezifisches, feingranulares Berechtigungsmanagement möglich, wie es in einer Vielzahl von Anwendungen bereits auf dem Markt angeboten wird. Die technische Realisierung feingranularer benutzerspezifischer Zugriffsrechte ist in der Informatik heute selbstverständlich.

Nach Art. 5 Abs. 1 lit. b) DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“).

Zudem müssen die personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden.

Wird also eine Berechtigung nur nach dem „Alles oder Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und verstößt gegen die Vorgaben in Artikel 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. b), c) und f) DSGVO.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V vermögen diese nach der DSGVO erforderlichen Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, nicht abzubedingen.

Denn die DSGVO ist als unionsrechtliche Verordnung unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Im Falle von Widersprüchen oder eines Normenkonflikts genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang, sodass abweichendes nationales Recht in einem solchen Fall nicht angewendet werden kann. Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Insbesondere sind Regelungen des SGB V insoweit von keiner Öffnungsklausel gedeckt, bzw. bewegt sich nicht in deren Grenzen. 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.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die geltenden Regelungen im SGB V nicht gerecht werden. Insbesondere lässt das SGB V die Einwilligung in Bezug auf „medizinische Informationen“ nach § 341 Abs. 2 Nr. 1 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen ist nicht möglich. Es ist nach dar DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen („Alles-oder-Nichts“), s.o. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar anzuwenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen und sich darauf beschränken, insbesondere kein feingranulares Zugriffsmanagement vorsehen, verstoßen Sie damit gegen Ihre unmittelbaren auf Sie anwendbaren Pflichten des europäischen Datenschutzrechts. Entsprechend bleibt auch Ihre – nach meiner derzeitigen unter I.2. geschilderten Sachverhaltsfeststellung – Umsetzung der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Patientensouveränität

Die einschlägigen gesetzlichen Vorgaben enthalten bereits einen Wertungswiderspruch zu der in § 341 Absatz 1 Satz 1 SGB V 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 Gesetz selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der ePA, einer Anwendung nach § 334 Absatz 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Absatz 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Absatz 2 SGB V). Dieser im Gesetz selbst zum Ausdruck kommenden Souveränität des Versicherten bezüglich seiner Daten werden die Regelungen in § 342 SGB V nicht gerecht.

Abgesehen davon, dass in diesem Sinne dem Versicherten ermöglicht werden muss, selbst zu entscheiden, wem er Zugriffsberechtigungen auf spezifische Dokumente und Datensätze in der ePA erteilt, ist es darüber hinaus datenschutzrechtlich geboten, dass alle Versicherten in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze in der ePA als auch Protokolldaten) Einblick nehmen können. Der datenschutzrechtliche Grundsatz der Transparenz gebietet, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 lit. a) DSGVO). Die geforderte Einblickmöglichkeit ist erforderlich für eine Führung der ePA durch die Versicherten selbst und entspricht der im Fünften Buch Sozialgesetzbuch angelegten Patientensouveränität (vgl. z. B. § 336 SGB V).
Lediglich den Versicherten mit einem Frontend ermöglichen Sie die Einsicht in die eigene ePA. Die Versicherten ohne Frontend haben diese Möglichkeit nicht und sind daher nicht in der Lage, ihre ePA selbst zu führen.

3. Zur Ermessensausübung und Verhältnismäßigkeit

Die von mir beabsichtigte Anweisung dient dem legitimen Zweck der Herstellung eines datenschutzkonformen Zustandes. Sie ist für diesen Zweck geeignet und es drängt sich kein milderes Mittel auf, das ihn ebenso wirksam erreichen würde. Zudem ist nicht ersichtlich, dass zwischen diesem Ziel, dem Mittel und den möglichen Folgen ein offensichtliches Missverhältnis bestünde. Sie stellt sich nach der mir derzeit bekannten Sachlage daher als ermessensgerecht und verhältnismäßig dar.

3.1. Geeignetheit der Maßnahme

Der abzustellende Datenschutzverstoß besteht in einer unzureichenden Gestaltung der Verarbeitung personenbezogener Daten. Nach Art. 25 DSGVO erforderliche technische und organisatorische Maßnahmen werden nicht getroffen. Indem diese erforderlichen Maßnahmen in Folge der Anweisung getroffen werden, lässt sich der Datenschutzverstoß für die Zukunft abstellen. Die beabsichtigte Anweisung nach Art. 58 Abs. 2 lit. d) DSGVO hat die erforderlichen Maßnahmen zum Gegenstand und stellt sich somit als geeignete Handlungsform dar, einen rechtmäßigen Zustand herbeizuführen.

3.2. Erforderlichkeit

Meine Möglichkeiten, andere gleich geeignete Mittel zu ergreifen, habe ich bereits ausgeschöpft. Ich habe bereits vor Einführung der ePA eine ausdrückliche Warnung nach Art. 58 Abs. 2 lit. a) DSGVO an Sie sowie an alle meiner Aufsicht unterstehenden Krankenversicherungsträger ausgesprochen. Sie haben die Verarbeitung gleichwohl in nicht datenschutzkonformer Art und Weise aufgenommen.

Andere gleich geeignete Abhilfemaßnahmen kommen als mildere Mittel nicht in Betracht:

- Eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO wäre nicht in gleicher Weise wie die in Aussicht genommene Anweisung geeignet, da sie lediglich auf die Feststellung eines in der Vergangenheit erfolgten Verstoßes gegen die DSGVO gerichtet wäre, ohne eine Rechtspflicht für die Zukunft aufzuerlegen.
- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen nach Art. 58 Abs. 2 lit. f) DSGVO wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

3.3. Angemessenheit

Vor dem Hintergrund, dass in der ePA insbesondere Gesundheitsdaten, also besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, einer Vielzahl von betroffenen Personen in großem Umfang verarbeitet werden, wäre es nicht pflichtgemäß, auf Abhilfemaßnahmen zu verzichten.

Auch der Umstand, dass nach § 342 Abs. 2 Nr. 2 SGB V die zweite Umsetzungsstufe für den 1. Januar 2022 vorgesehen ist, führt nicht zu einer Unverhältnismäßigkeit der Maßnahme. Sie haben meiner Warnung zum Trotz die Verarbeitung in einer nicht der DSGVO entsprechenden Weise ab dem 1 Januar 2021 aufgenommen. Als Verantwortlicher sind Sie bereits

aktuell nach europäischem Datenschutzrecht zur Herstellung eines datenschutzkonformen Zustands im Zugriffsmanagement der ePA verpflichtet. Dass ein feingranulares Zugriffsmanagement für die Frontend-Nutzer ab dem 1. Januar 2022 zusätzlich auch nach nationalem Sozialrecht erforderlich werden wird, ändert nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt. Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten - also auch die Nicht-Frontend-Nutzer - betrifft.

In meine Ermessenserwägungen habe ich auch Ihre Einlassung einbezogen, dass eine technische Umsetzung grundsätzlich möglich und in späteren Spezifikationen der gematik bereits vorgesehen ist. Dies habe ich durch Einsichtnahme in die entsprechenden Spezifikationen bestätigt gefunden.

Um die Angemessenheit meiner Anweisung sicherzustellen, beabsichtige ich die Einräumung einer angemessenen Umsetzungsfrist bis zum 31. Dezember 2021. Diese Frist ist auch in Hinblick auf die Üblichkeit feingranularer Zugriffsgestaltung sowie der bereits vorliegenden Spezifikationen als (mehr als) ausreichend anzusehen. Es wäre nicht hinnehmbar, dass sich die datenschutzwidrige Verarbeitungspraxis über die Umsetzungsfrist hinaus fortsetzt.

Durch meine frühzeitige, eindeutige und konsequente Verdeutlichung der datenschutzrechtlichen Pflicht zur Gestaltung des Zugriffsmanagements sowie meine bereits am 6. November 2020 ausgesprochene Warnung mussten Sie sich auf die Erfüllung Ihrer datenschutzrechtlichen Pflichten einstellen. Eine entsprechende Anweisung ist nicht überraschend und stellt sich als angemessen im engeren Sinne dar.

4. Mitteilung an das Bundesamt für Soziale Sicherung

Das Bundesamt für Soziale Sicherung als ihrer nach § 90 Abs. 1 S. 1 Viertes Buch Sozialgesetzbuch (SGB IV) zuständigen Aufsichtsbehörde werde ich informieren, dass ich von den oben dargelegten Verstößen gegen die Vorschriften über den Datenschutz beziehungsweise von Mängeln bei der Verarbeitung personenbezogener Daten ausgehe, und ihm vor der Ausübung meiner Befugnisse gemäß § 16 Abs. 1 S. 2 Bundesdatenschutzgesetz Gelegenheit zur Stellungnahme geben werde.

III.
Gelegenheit zur Stellungnahme

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

7. Juni 2021

gemäß § 28 Verwaltungsverfahrensgesetz (VwVfG) Gelegenheit, sich zur Sache zu äußern. Bitte nehmen Sie insbesondere zur Ausgestaltung des Zugriffsmanagements der ePA Stellung. Darüber hinaus bitte ich um Darlegung, wie viele Ihrer Versicherten die ePA nutzen.

Sollte ich von Ihnen bis dahin keine Nachricht erhalten haben, behalte ich mir vor, weitere Ermittlungen einzuleiten oder nach Aktenlage zu entscheiden.

Mit freundlichen Grüßen
In Vertretung

Jürgen H. Müller