Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Prof. Ulrich Kelber
Bundesbeauftragter
für den Datenschutz und
die Informationsfreiheit

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

An den
Vorsitzenden des Vorstandes der
Gesetzliche Krankenkasse
Vorstand

(Name, Anschrift ergänzen)

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON (0228) 997799-5000
E-MAIL referat13@bfdi.bund.de
INTERNET www.bfdi.bund.de

DATUM Bonn, 16.08.2021
GESCHÄFTSZ. 13-315/105#1147

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

nachrichtlich:

Bundesamt für Soziale Sicherung
Datenschutzbeauftragte
Friedrich-Ebert-Alle 38
53113 Bonn

BETREFF Datenschutzaufsichtsbehördliches Verfahren
BEZUG 1. Mein Anhörungsschreiben vom 4. Mai 2021
2. Ihre Stellungnahme vom (individuell bezogen auf die Krankenkasse ergänzen)

Sehr geehrte Damen und Herren,

hiermit ergeht gegen die […] gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) folgender

B E S C H E I D

1. Die […] wird gemäß Art. 58 Abs. 2 lit. d) DSGVO angewiesen, das Zugriffsmanagement der elektronischen Patientenakte (ePA) so auszugestalten, dass Versicherte 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 („feingranulares Zugriffsmanagement“) können. Dies kann für Versicherte, die keine Benutzeroberfläche eines geeigneten Endgeräts verwenden (Frontend-Nichtnutzer), insbesondere mittels der

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

dezentralen Infrastruktur der Leistungserbringer oder durch sonstige technische Einrichtungen bei den Leistungserbringern bzw. in Ihren Geschäftsraumen oder in Kooperation mit anderen Krankenkassen oder Stellen erfüllt werden.

2. Die […] wird gemäß Art. 58 Abs. 2 lit. d) DSGVO angewiesen, das Zugriffsmanagement der ePA so auszugestalten, dass auch Frontend-Nichtnutzer auch ohne die Bestellung eines Vertreters in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können. Dies kann ebenfalls insbesondere mittels der dezentralen Infrastruktur der Leistungserbringer oder durch sonstige technische Einrichtungen bei den Leistungserbringern bzw. in Ihren Geschäftsraumen oder in Kooperation mit anderen Krankenkassen oder Stellen erfüllt werden.

3. Für Versicherte, die die Benutzeroberfläche eines geeigneten Endgeräts verwenden (Frontend-Nutzer), hat die Umsetzung der Ziffer 1 **bis zum 31.12.2021,** spätestens jedoch **innerhalb von einem Monat** nach Rechtskraft eines etwaigen abschließenden Urteils zu erfolgen.

4. Für Frontend-Nichtnutzer hat die Umsetzung der Ziffern 1 und 2 **binnen eines Jahres** zu erfolgen.

Begründung:

I.

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 dem PDSG wurden im Fünften Buch Sozialgesetzbuch (SGB V) u.a. die Vorgaben zur elektronischen Gesundheitskarte neu gefasst und Regelungen mit bundesgesetzlichen Mindestanforderungen für eine ePA ausgestaltet. § 341 Abs. 1 SGB V verpflichtet die

Krankenkassen, ihren Versicherten eine versichertengeführte ePA zur Verfügung zu stellen. Die Pflicht, eine ePA zur Verfügung zu stellen, gilt gemäß § 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 wird dabei gemäß § 342 Abs. 2 Nr. 2 lit. b) SGB V bundesgesetzlich als Mindestvorgabe vorgesehen, dass spätestens bis zum 1. Januar 2022 ein sog. feingranulares Zugriffsmanagement für Frontend-Nutzer zu gewährleisten ist. Spätestens ab diesem Zeitpunkt ist auch bundesgesetzlich als Mindestvorgabe zwingend vorgesehen, dass die Frontend-Nutzer die Erteilung der Zugriffsberechtigung auf spezifische Dokumente und Datensätze beschränken können müssen. Bis dahin ist bundesrechtlich gemäß § 342 Abs. 2 Nr. 1 lit. c) SGB V als Mindestvoraussetzung für alle Versicherten lediglich eine Differenzierung entweder nach Daten gemäß § 341 Abs. 2 Nr. 1 SGB V (medizinische Daten: Befunde, Arztberichte, Medikationsplan, Notfalldatensatz u.a.) oder/und gemäß § 341 Abs. 2 Nr. 6 SGB V (Gesundheitsdaten der Versicherten, z.B. aus Fitnesstrackern) vorgesehen. Hinsichtlich der wichtigen medizinischen Informationen würde bei der bloßen Umsetzung des § 342 Abs. 2 Nr. 1 lit. c) SGB V lediglich nach dem „Alles-oder-Nichts-Prinzip“ verfahren, da entweder nur auf alle von Leistungserbringern (z.B. Ärzte) oder vom Versicherten selbst eingestellte Dokumente berechtigt werden kann oder auf keine.

Für die Frontend-Nichtnutzer ist bundesrechtlich als Mindestanforderung spätestens ab dem 1. Januar 2022 die Erteilung der Zugriffsberechtigung lediglich auf Kategorien von Dokumenten durch die Regelungen des SGB V als zwingende bundesgesetzliche Voraussetzung vorgesehen (sog. mittelgranulares Zugriffsmanagement). Bei Umsetzung bloß dieser bundesgesetzlichen Mindestanforderungen für die Gruppe der Frontend-Nutzer würde diesen Versicherten als Alternative faktisch nur verbleiben, entgegen der eigenen informationellen Selbstbestimmung einen Dritten als fremdverwaltenden Vertreter zu bestimmen und diesen zu berechtigen, die ePA-Daten zu verwalten (§ 342 Abs. 2 Nr. 2 lit. b) und lit. e) SGB V), d. h Zugriffsrechte auf spezifische Dokumente zu erteilen .

2. Meine bisherigen Maßnahmen und Sachverhaltsermittlungen

Mit Schreiben vom 6. November 2020 hatte ich gegen Sie eine Warnung gemäß Art. 58 Abs. 2 lit. a) DSGVO ausgesprochen und dabei klargestellt, dass eine Einhaltung lediglich der im PDSG bundesgesetzlich enthaltenen Mindestvorgaben zur technischen Ausgestaltung der elektronischen Patientenakte (ePA) unter Verzicht auf ein feingranulares Berechtigungsmanagement schon bei der Einführung der ePA zum 1. Januar 2021 einen Verstoß gegen Ihre Pflichten nach Art. 25 und 32 DSGVO darstellen würde.

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 … mitgeteilt, dass die maßgebliche Spezifikation der Gesellschaft für Telematik (gematik) ein feingranulares Zugriffsmanagement gemäß § 342 Abs. 2 Nr. 2 lit. b) SGB V für Frontend-Nutzer 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.

Mit meinem Anhörungsschreiben nach § 28 Verwaltungsverfahrensgesetz (VwVfG) vom 4. Mai 2021 habe ich Ihnen Gelegenheit zur Stellungnahme gegeben. In Ihrer Stellungnahme vom … verweisen Sie auf das Schreiben vom … Außerdem führen Sie aus, dass Sie die rechtlichen Argumente für einen Verstoß gegen die DSGVO nicht für zwingend halten und Sie als Körperschaft des öffentlichen Rechts zur Ausführung der Bundesgesetze verpflichtet seien.

Mit Schreiben vom 4. Mai 2021 habe ich die Rechtsaufsichtsbehörde gemäß § 90 Viertes Buch Sozialgesetzbuch (SGB IV), das Bundesamt für Soziale Sicherung (BAS), gemäß § 16 Abs. 1 Satz 2 Bundesdatenschutzgesetz (BDSG) um Stellungnahme gebeten.

Das BAS hat in seiner Stellungnahme vom 28. Juni 2021 mitgeteilt, dass es meine Rechtsauffassung nicht teile. Das BAS könne im Ergebnis keinen Verstoß gegen europäisches oder nationales Datenschutzrecht erkennen.

Nach dem mir bekannten Sachverhalt und unter Würdigung Ihrer bisherigen Einlassungen gehe ich davon aus, dass Sie den bei Ihrer Krankenkasse Versicherten seit 1. Januar 2021 eine ePA anbieten, welche kein feingranulares Zugriffsmanagement aufweist. Zudem können die Frontend-Nichtnutzer keine eigenständige Einsicht in ihre eigene patientengeführte ePA nehmen.

II.

Meine Zuständigkeit für die datenschutzrechtliche Aufsicht über die Krankenkasse folgt aus § 9 Abs. 1 i. V. m. § 2 Bundesdatenschutzgesetz (BDSG) i. V. m. Art. 87 Abs. 2 Grundgesetz (GG) und § 90 Viertes Buch Sozialgesetzbuch (SGB IV).

Gemäß § 16 Abs. 1 S. 1 BDSG i. V. m. Art. 58 Abs. 2 lit. d) DSGVO bin ich befugt, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen.

Diese Voraussetzungen sind vorliegend 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 und aufsichtsrechtliche Maßnahmen an Sie zu adressieren sind.

2. Verstoß gegen die DSGVO

Sie verstoßen gegen die DSGVO, indem Sie personenbezogene Daten Ihrer Versicherten in einer ePA verarbeiten und dabei darauf verzichten, allen Versicherten ein feingranulares Zugriffsmanagement sowie die Einsichtnahmemöglichkeit in die eigene ePA bereitzustellen.

2.1. Verpflichtung zu einem feingranularen 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.

Art. 5 Abs. 1 lit. a) DSGVO verlangt, dass personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“).

Gemäß 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“).

Daneben 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“).

Außerdem müssen personenbezogene Daten gemäß Art. 5 Abs. 1 lit. f) DSGVO in einer Weise verarbeitet werden, die eine angemessene Sicherheit dieser Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

Diesen Verarbeitungsgrundsätzen kann nur durch ein feingranulares Berechtigungsmanagement entsprochen werden. Dem Versicherten muss das Recht eingeräumt werden, welches Dokument er welchem Dritten (Arzt, Therapeut etc.) zur Kenntnis geben möchte. Eine Umsetzung nach dem „Alles-oder-Nichts-Prinzip“ entspricht nicht dem Stand der Technik und verstößt gegen die Vorgaben in Art. 25 DSGVO sowie gegen die Datenschutzgrundsätze des Art. 5 Abs. 1 lit. a), b), c) und f) DSGVO. Von einer Freiwilligkeit der Einwilligung kann auch kaum gesprochen werden, wenn diese nach dem „Alles-oder-

nichts-Prinzip“ erfolgen muss. Gibt der Versicherte daher Gesundheitsdaten aus der ePA z. B. für seinen Orthopäden frei, kann nicht davon ausgegangen werden, dass der Versicherte dem Orthopäden auch die Gesundheitsdaten aus seinen Behandlungen beim Zahnarzt oder beim Psychologen oder Psychiater freigeben wollte. Der Versicherte möchte zunächst dem Orthopäden nur die Daten zur Verfügung stellen, die dieser für seine Behandlung für erforderlich hält. Diese Freiheit zu entscheiden, welche Daten er welchem Dritten (Arzt, Therapeuten etc.) zur Verfügung stellt, wird mit Ihrem Angebot nicht gewährleistet. Von einer echten Einwilligung des Versicherten kann also nicht gesprochen werden.

2.2. Keine Abbedingung der DSGVO durch das SGB V

Die unter I.1. dargestellten Regelungen des SGB V beschränken die unionrechtlichen Anforderungen nicht und können diese von der DSGVO aufgestellten Voraussetzungen und Anforderungen, die sich unmittelbar an den Verantwortlichen richten, auch rechtlich nicht abbedingen.

Das SGB V regelt lediglich bundesgesetzliche Mindestanforderungen. Insbesondere die Regelungen in § 342 Abs. 2 Nr. 1 und 2 SGB V sehen lediglich die Umsetzung bis „spätestens“ einem bestimmten Zeitpunkt vor und verbieten Ihnen nicht unionsrechtlich gebotene Anforderungen bereits vor diesen Zeitpunkten umzusetzen.

Unabhängig davon könnte eine bundesgesetzliche Regelung im SGB V unionsrechtliche Vorgaben der DSGVO aber auch nicht verbieten oder diese suspendieren.

Gemäß Art. 288 Abs. 2 Satz 1 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) besitzt die DSGVO als Verordnung allgemeine Geltung und ist gemäß Art. 288 Abs. 2 Satz 2 AEUV in all ihren Teilen verbindlich. Die DSGVO ist als unionsrechtliche Verordnung daher unmittelbar anwendbar und begründet unmittelbare Rechte und Pflichten für die Normadressaten. Nach der Rechtsprechung des Europäischen Gerichtshofes (EuGH) genießt das Unionsrecht Vorrang vor dem nationalen, im vorliegendem Fall dem deutschen Recht. Hieraus folgt ein Anwendungsvorrang des Unionsrechts. Im Kollisionsfall darf das nationale Recht nicht angewendet werden (statt vieler *Plath* in: Plath, DSGVO/BDSG, 3. Aufl. 2018, § 1 BDSG Rn. 47).

Widerspricht das deutsche Recht der Unionsverordnung, hier der DSGVO, so ist die unionsrechtliche Regelung von den nationalen Behörden und Gerichten anzuwenden, während die nationalen Gesetze nicht angewendet werden dürfen. Diese Pflicht zur Nichtanwendung haben nationale Gerichte jeder Instanz und auch nationale Behörden (u.a. EuGH, Urt. v. 9. März 1978 – C106/ 77 –). Dies gilt auch für öffentlich-rechtliche Körperschaften wie es die gesetzlichen Krankenkassen gemäß § 29 Abs. 1 SGB IV sind.

Soweit das SGB V geringere Vorgaben ausreichen lässt, können diese das gesetzlich in der DSGVO vorgegebene Schutzniveau nicht unterschreiten. Unabhängig davon, dass die Regelungen des SGB V ihrem Wortlaut nach die Anforderungen der DSGVO nicht ausschließen, wären solche auch von keiner Öffnungsklausel der DSGVO gedeckt bzw. bewegten sich nicht in deren Grenzen.

Erforderlich ist ein feingranulares Zugriffsmanagement auf Dokumentenebene, dem die bloße Umsetzung der Mindestanforderungen des SGB V nicht gerecht werden. Insbesondere ließen die bloßen Mindestanforderungen des SGB V die Einwilligung in Bezug auf „medizinische Informationen“ gemäß § 341 Abs. 2 Nr. 1 SGB V bzw. auf vom Versicherten eingestellte Gesundheitsdaten gemäß § 341 Abs. 2 Nr. 6 SGB V in der ersten Umsetzungsstufe nur nach dem „Alles-oder-Nichts“-Prinzip genügen; eine Auswahl von Dokumenten oder Datensätzen wäre nicht möglich. Es ist nach der DSGVO aber nicht ausreichend, nur auf ganze „Datentöpfe“ zu berechtigen. Eine Information über die fehlende Möglichkeit der feingranularen Beschränkung einer Einwilligung, wie sie nach den Mindestanforderungen des in § 342 Abs. 2 Nr. 1 lit. h) SGB V vorgesehen ist, vermag nicht von den unmittelbar geltenden Anforderungen der DSGVO zu befreien.

Soweit Sie daher lediglich die Vorgaben des nationalen Rechts zur ePA im SGB V umsetzen, ohne ein durchgehend feingranulares Zugriffsmanagement vorzusehen, verstoßen Sie gegen unmittelbar auf Sie als Verantwortliche treffende Pflichten nach der DSGVO. Dementsprechend bleibt die Ihnen obliegende Umsetzung von Einführung und Betrieb der ePA hinter den datenschutzrechtlichen Anforderungen zurück.

2.3. Nähere Ausführungen zur Begründung eines Verstoßes gegen die DSGVO

Jede Verarbeitung personenbezogener Daten muss den Grundsätzen des Art. 5 DSGVO entsprechen. Dies umfasst insbesondere die Grundsätze der Rechtmäßigkeit der Verarbeitung (Art. 5 Abs. 1 lit. a) DSGVO), der Erforderlichkeit und Zweckbindung (Art. 5 Abs. 1 lit. b) DSGVO), der Datenminimierung (Art. 5 Abs. 1 lit. c) DSGVO) sowie der Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f) DSGVO).

Besonders streng sind die Anforderungen bei besonderen Kategorien personenbezogener Daten, deren Verarbeitung gemäß Art. 9 Abs. 1 DSGVO grundsätzlich untersagt ist. Das Verarbeitungsverbot gilt nur ausnahmsweise in den Fällen des Art. 9 Abs. 2 DSGVO nicht.

In der ePA werden Gesundheitsdaten verarbeitet, welche auch zu den besonderen Kategorien personenbezogener Daten zählen. Somit gelten vorliegend auch die Vorgaben des Art. 9 DSGVO.

Der Verantwortliche hat gemäß Art. 24 Abs. 1 S. 1 DSGVO geeignete technische und organisatorische Maßnahmen umzusetzen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der DSGVO erfolgt. Darüber hinaus hat er gemäß Art. 25 Abs. 1 DSGVO geeignete technische und organisatorische Maßnahmen zu treffen, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen. Die technischen und organisatorischen Maßnahmen sind „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen“ zu treffen (vgl. Art. 25 Abs. 1 S. 1 DSGVO).

2.3.1. Rechtmäßigkeit der Verarbeitung (Rechtsgrundlage)

Die Verarbeitung der Gesundheitsdaten erfolgt nicht ausschließlich auf Grundlage einer Einwilligung gemäß Art. 6 Abs. 1 S. 1 lit. a), 9 Abs. 2 lit. a) DSGVO. Hier ist davon auszugehen, dass die Verarbeitung auf der Grundlage der Regelungen des SGB V als Recht eines Mitgliedsstaats im Gesundheitsbereich im Sinne des Art. 9 Abs. 2 lit. h) DSGVO und für die dort genannten Zwecke – insbesondere Versorgung oder Behandlung im Gesundheitsbereich erfolgt. Die Konzeption, dass die Einwilligung als

Tatbestandsmerkmal in der Norm enthalten ist („Mischtatbestand“), findet sich im SGB V an verschiedenen Stellen. Eigentliche Rechtsgrundlage für die Datenverarbeitung ist demnach das Gesetz, nicht die Einwilligung als solche.

Auch vorliegend gehen die einschlägigen Gesetzgebungsmaterialien ausdrücklich hiervon aus:

- „Die Legitimation der Datenverarbeitung ergibt sich aus der Einwilligung der Versicherten und der gesetzlichen Grundlage (vgl. § 339 Absatz 1)“ [vgl. BT-Drs. 19/18793, zu § 352 (S. 122)].
- „Dabei ergibt sich die Legitimation der Datenverarbeitung aus einem Zusammenspiel der informierten Einwilligung des Versicherten und der gesetzlichen Befugnisnorm zum konkreten Umfang der Datenverarbeitung (vgl. § 339 Absatz 1)“ [vgl. BT-Drs. 19/18793, zu § 359 Abs. 1 (S. 127)].

Der Wortlaut des Art. 9 Abs. 2 lit. h) DSGVO stellt klar, dass die Verarbeitung für die dort aufgeführten Zwecke „erforderlich“ sein muss. Die maßgebliche nationale Grundlage betont insoweit, dass mit der ePA „den Versicherten (…) Informationen (…) für Zwecke der Gesundheitsversorgung, insbesondere zur gezielten Unterstützung von Anamnese und Befunderhebung (…) bereitgestellt werden“. (§ 341 Abs. 1 Satz 3 SGB V). § 352 SGB V regelt weiterhin, dass die Zugriffsberechtigten nur insoweit auf die ePA zugreifen dürfen, wie es für die Versorgung der Versicherten notwendig ist. Der Zweck ist also bundesgesetzlich eindeutig umgrenzt. Es darf bei der Einholung der Einwilligung nicht über diesen Zweck hinausgegangen werden.

Das Fehlen einer ausreichend feinen Granularität verhindert die vom Gesetz vorgegebene zweckentsprechende Datenverarbeitung, weil für die jeweilige Behandlung nicht erforderliche Dokumente zwangsläufig (mit-) freigegeben werden müssen. Die Freigabe für eine „gezielte Unterstützung“ nicht notwendiger Dokumente geht über den gesetzlich festgeschriebenen Zweck der Einwilligung hinaus. Sie ist nach der Konzeption des Mischtatbestands nicht von ihrer gesetzlichen Grundlage gedeckt und damit unwirksam.

Eine gesetzliche, den Verarbeitungszweck begrenzende Regelung ist zudem nur dann tatsächlich wirksam, wenn eine entsprechende Kontrolle ausgeübt werden kann und der Betroffene das Recht und die Möglichkeit hat, ein Dokument – auch wenn es der Leistungserbringer für erforderlich hält – gerade nicht freigeben zu müssen.

Ergänzend und äußerst hilfsweise ist zu berücksichtigen, dass selbst dann, wenn man die Einwilligung selbst als Rechtsgrundlage der Verarbeitung ansehen wollte, die von der DSGVO aufgestellten Grundsätze der Verarbeitung personenbezogener Daten zu beachten wären.

Grundvoraussetzung einer wirksamen Einwilligung ist deren freiwillige Erteilung. Wichtiges Element des Freiwilligkeitsprinzips ist das in Art. 7 Abs. 4 DSGVO statuierte „Koppelungsverbot“. Eine der Freiwilligkeit entgegenstehende verbotene Koppelung liegt vor, wenn u. a. die Erbringung einer Leistung davon abhängig gemacht wird, dass der Betroffene in eine weitergehende Verarbeitung seiner personenbezogenen Daten einwilligt, welche nicht zur Erbringung der eigentlichen Leistung erforderlich ist.

Das Fehlen der Möglichkeit, dokumenten- und datensatzspezifische Zugriffsberechtigungen zu erteilen, zwingt die ePA-Nutzer, personenbezogene Daten freizugeben und damit einer weitergehenden Verarbeitung zuzuführen, ohne dass dies im Einzelfall für die eigentliche Leistungserbringung – Bereitstellung der ePA zur gezielten Unterstützung von Anamnese und Befunderteilung, § 341 Abs. 1 S. 3 SGB V – erforderlich ist. Damit ist die zweckentsprechende Leistungserbringung durch das Alles-oder-Nichts-Prinzip an eine weitergehende, nicht erforderliche Datenverarbeitung gekoppelt. Die zugrundeliegende Einwilligung wäre deshalb insgesamt nicht freiwillig und damit unwirksam.

Da die Datenverarbeitung nach dem Alles-oder-Nichts-Prinzip insgesamt weder von einer legitimen Rechtsgrundlage gedeckt ist, noch auf eine wirksame Einwilligung gestützt werden kann, liegt ein Verstoß gegen den Grundsatz der Rechtmäßigkeit der Verarbeitung, Art. 5 Abs. 1 lit. a) DSGVO vor.

2.3.2. Transparenz der Verarbeitung/Patientensouverenität

§ 341 Abs. 1 Satz 1 SGB V enthält zudem die 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 geeignetes Endgerät eigenständig auf ihre ePA zugreifen können. Dies ist der Anspruch, den das PDSG selbst in § 336 SGB V definiert. Demnach ist jeder Versicherte berechtigt, auf Daten in der

ePA, einer Anwendung gemäß § 334 Abs. 1 Satz 2 Nr. 1 SGB V, barrierefrei zuzugreifen, entweder mit der elektronischen Gesundheitskarte (§ 336 Abs. 1 SGB V) oder unter weiteren Maßgaben ohne Einsatz der elektronischen Gesundheitskarte (§ 336 Abs. 2 SGB V). Dieser im Fünften Buch Sozialgesetzbuch 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. Art. 5 Abs. 1 lit. a) DSGVO). Die geforderte Einblicksmöglichkeit 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.

Zwar kann die den Frontend-Nichtnutzern gesetzlich gewährte Möglichkeit, über eine Vollmachterteilung ihre Rechte wahrzunehmen („Vertreterlösung“), dazu dienen, die eingeschränkte Datensouveränität zu lindern, vollständig wiederherstellen vermag sie die eingeschränkte Souveränität jedoch nicht. Das Hinzuziehen eines Dritten ist an sich bereits mit einem Souveränitätsverlust behaftet. Zudem erhalten Versicherte, die sich aus IT-Sicherheitsgründen gegen das Verarbeiten von Gesundheitsdaten auf privaten Endgeräten (den eigenen und denen von Vertretern) entscheiden, dauerhaft keine Möglichkeit, ein feingranulares Zugriffsmanagement zu nutzen sowie in ihre ePA oder in Zugriffprotokolle Einsicht zu nehmen.

Damit entspricht die Datenverarbeitung nicht den von der DSGVO gestellten Anforderungen an eine nachvollziehbare, transparente Datenverarbeitung und stellt einen Verstoß gegen Art. 5 Abs. 1 lit. a) DSGVO dar.

2.3.3. Technische und organisatorische Maßnahmen entsprechend dem Stand der Technik

Die technischen und organisatorischen Maßnahmen müssen dafür ausgelegt sein, die Datenschutzgrundsätze wirksam umzusetzen. Außerdem muss es den Nutzern möglich sein, den Zugriff auf ihre personenbezogenen Daten so zu steuern, dass die Verarbeitung nicht über die gesetzlich gesetzte Zweckumschreibung und die darüber konkretisierten weiteren Datenschutzgrundsätze hinausgeht. Hierfür ist ein feingranulares Zugriffsmanagement unabdingbar.

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 und damit auch Stand der Technik. Wird eine Berechtigung nur nach dem „Alles-oder-Nichts-Prinzip“ umgesetzt, entspricht dies nicht dem Stand der Technik und stellt damit einen Verstoß gegen Art. 25 Abs. 1 DSGVO dar. Insbesondere in Bezug auf besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO sind fein granular aufgelöste Berechtigungskonzeptionen aufzustellen (so auch große Teile der Literatur, etwa Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, Kap. 1 Rn. 60 für den Konzerndatenschutz).

2.3.4. Zweckbindung

Die Zwecke der ePA sind gesetzlich umgrenzt. Die Zwecke der Verarbeitung dürfen somit von den Verantwortlichen nicht frei gesetzt werden. Maßgeblich für die gesetzliche Zweckbestimmung der ePA sind insbesondere § 341 SGB und § 352 SGB V sowie die in den Gesetzesmaterialien zum Ausdruck kommenden Zweckbestimmungen. § 341 Abs. 1 S. 1 SGB V enthält zunächst die Prämisse, dass die ePA vom Versicherten eigenständig geführt wird. § 341 Abs. 1 S. 3 SGB V bestimmt, dass mit der ePA den Versicherten Informationen, insbesondere zu Befunden, Diagnosen, durchgeführten und geplanten Therapiemaßnahmen sowie zu Behandlungsberichten, für eine einrichtungs-, fach- und sektorübergreifende Nutzung für Zwecke der Gesundheitsversorgung, insbesondere zur gezielten Unterstützung von Anamnese und Befunderhebung, barrierefrei elektronisch

bereitgestellt werden sollen. Dementsprechend steht also die Information des Versicherten im Fokus des Zwecks. Zusätzlich ist aus § 341 Abs. 1 S. 3 SGB V zu folgern, dass die Bereitstellung von Dokumenten und Datensätze aus der ePA zielgerichtet erfolgen muss. Präzisiert wird dies in § 352 SGB V, der regelt, dass die Zugriffsberechtigten nur insoweit auf die ePA zugreifen dürfen, wie es für die Versorgung der Versicherten notwendig ist.

Für die Erreichung dieser Zwecke ist unabdingbar erforderlich, dass die Versicherten Einblick in ihre eigene ePA nehmen können. Für Frontend-Nichtnutzer ist dies sowohl 2021 als auch ab 2022 nicht gegeben.

2.3.5. Datenminimierung

Der Grundsatz der Datenminimierung besagt, dass personenbezogene Daten auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen. Der Zugriff auf personenbezogene Daten darf nur dann möglich sein, wenn keine alternative Methode zur Verfügung steht, um den mit der Verarbeitung angestrebten Zweck zu erreichen (Härting, DSGVO, Rn. 98).

Gemäß § 341 Abs. 1 Satz 3 SGB V sollen mit der ePA „den Versicherten (…) Informationen (…) für Zwecke der Gesundheitsversorgung, insbesondere zur gezielten Unterstützung von Anamnese und Befunderhebung (…) bereitgestellt werden“. Die Erteilung der Zugriffsberechtigung nach dem Alles-oder-Nichts-Prinzip hat zur Folge, dass auch Daten freigegeben werden, die zur gezielten Behandlungsunterstützung nicht erforderlich sind. So ist beispielsweise eine gynäkologische Anamnese in der Regel nicht erforderlich für eine internistische Behandlungsunterstützung. Mit der technisch vorhandenen Möglichkeit, den Zugriff auf spezifische, für die jeweilige Behandlung erforderliche Dokumente und Datensätze zu beschränken, steht auch eine Methode zur Verfügung, die den mit der Verarbeitung angestrebten Zweck unter Berücksichtigung des Grundsatzes der Datenminimierung erfüllen würde. Damit stellt das derzeitige Berechtigungskonzept einen Verstoß gegen Art. 5 Abs. 1 lit. c) DSGVO dar.

2.3.6. Integrität und Vertraulichkeit

Der Grundsatz der Integrität und Vertraulichkeit verlangt für die Datenverarbeitung eine angemessene Sicherheit der personenbezogenen Daten. Mit der Freigabe nicht erforderlicher Dokumente und Datensätze, wie es das Alles-oder-nichts-Prinzip mit sich bringt, steigt zwangsläufig das Risiko einer unbefugten und unrechtmäßigen Verarbeitung dieser Daten – zumal der Zugriff nicht leistungserbringerspezifisch, sondern nur der gesamten Leistungserbringerinstitution erteilt werden kann. Dieser Gefährdungslage würde mit der technisch möglichen feingranularen Zugriffsberechtigung entgegengewirkt, so dass das derzeitige Zugriffsmanagement gegen Art. 5 Abs. 1 lit. f) DSGVO verstößt.

2.3.7. Keine Absenkung des Datenschutzniveaus der DSGVO durch nationalen Gesetzgeber

Die Mitgliedstaaten können nach Art. 9 Abs. 4 DSGVO zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist. Erlaubt sind allerdings nur Vorschriften, die das Schutzniveau erhöhen. Eine Ausweitung der Ausnahmen vom Verbot des Art. 9 Abs.1 DSGVO ist den Mitgliedstaaten nicht gestattet (vgl. Petri, in: Simitis/ Hornung/ Spiecker gen. Döhmann, Datenschutzrecht, DSGVO mit BDSG, 1. Aufl. 2019, Art. 9 Rn. 101).

3. Behebbarkeit des Verstoßes

Eine Maßnahme gemäß Art. 58 Abs. 2 lit. d) DSGVO setzt voraus, dass behebbare Verstöße vorliegen (vgl. Polenz, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO mit BDSG, 1. Aufl. 2019, Art. 58 Rn. 33). Andernfalls käme nur die komplette Untersagung der datenschutzwidrigen Verarbeitungen in Betracht. Die ePA ist auf Dauer angelegt; der datenschutzrechtliche Verstoß ist durch Einführung eines feingranularen Zugriffsmanagements für die Zukunft behebbar.

4. Zur Verhältnismäßigkeit und Ermessensausübung

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.

4.1 Geeignetheit

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 gemäß 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.

4.2. Erforderlichkeit

Meine Möglichkeiten andere gleich geeignete, aber mildere Mittel zu ergreifen habe ich bereits ausgeschöpft.

Bereits vor Einführung der ePA habe ich eine ausdrückliche Warnung gemäß Art. 58 Abs. 2 Buchst. 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 gemäß 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. Eine

Verwarnung begründet keine Rechtspflicht, einen Verstoß abzustellen oder eine Verarbeitungstätigkeit zu ändern (Polenz, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO mit BDSG, 1. Aufl. 2019, Art. 58 Rn. 29).

- Die Verhängung von Beschränkungen oder Verboten für Verarbeitungen gemäß Art. 58 Abs. 2 lit. f) BDSG wäre kein milderes, sondern ein einschneidenderes Mittel, dessen Angemessenheit vor dem Hintergrund der grundsätzlichen Pflicht zur Einführung der ePA zweifelhaft wäre.

4.3. 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 gemäß § 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 gemäß § 342 Abs. 2 SGB V zusätzlich spätestens ab dem 1. Januar 2022 auch nach nationalem Recht erforderlich ist, ändert zum einen nichts an der bereits bestehenden europarechtlichen Verpflichtung aus der DSGVO, der Anwendungsvorrang zukommt, und macht meine konkret an Sie gerichtete, vollstreckbare Anweisung nicht unverhältnismäßig. Die Anweisung unter Ziffer 1 ordnet insoweit lediglich auf VA-Ebene das an, was Sie bis zum Ablauf der Frist auch bundesgesetzlich ohnehin umzusetzen haben.
Die europarechtliche Verpflichtung geht zudem über § 342 Abs. 2 Nr. 2 SGB V hinaus, indem sie alle Versicherten, also auch die Frontend-Nichtnutzer, 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, räume ich Umsetzungsfristen bis zum 31. Dezember 2021, spätestens jedoch innerhalb von einem Monat nach Rechtskraft eines etwaigen abschließenden Urteils für die Frontend-Nutzer bzw. binnen eines Jahres für die Frontend-Nichtnutzer ein. Diese Fristen sind 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 insgesamt als angemessen im engeren Sinne dar.

Mit freundlichen Grüßen

Ulrich Kelber

Rechtsbehelfsbelehrung
Gegen diesen Bescheid kann innerhalb eines Monats nach Bekanntgabe Klage beim

Sozialgericht Köln

schriftlich, in elektronischer Form oder zur Niederschrift der Urkundsbeamtin / des Urkundsbeamten der Geschäftsstelle Klage erhoben werden.

Die elektronische Form wird durch Übermittlung eines elektronischen Dokuments gewahrt, das für die Bearbeitung durch das Gericht geeignet ist und entweder von der verantwortenden Person qualifiziert elektronisch signiert ist oder von der verantwortenden Person signiert auf einem sicheren Übermittlungsweg gem. § 65a Abs. 4 Sozialgerichtsgesetz (SGG) eingereicht wird. Nähere Informationen ergeben sich aus der Verordnung über die technischen Rahmenbedingungen des elektronischen

Rechtsverkehrs und über das besondere elektronische Behördenpostfach (Elektronischer-Rechtsverkehr-Verordnung - ERVV). Über das Internetportal des Elektronischen Gerichts- und Verwaltungspostfachs (www.egvp.de) können weitere Informationen über die Rechtsgrundlagen, Bearbeitungsvoraussetzungen und das Verfahren des elektronischen Rechtsverkehrs abgerufen werden.

Die Klage muss gemäß § 92 des Sozialgerichtsgesetzes den Kläger, den Beklagten und den Gegenstand des Klagebegehrens bezeichnen. Zur Bezeichnung des Beklagten genügt die Angabe der Behörde. Die Klage soll einen bestimmten Antrag enthalten und von dem Kläger oder der zu seiner Vertretung befugten Person mit Orts- und Zeitangabe unterzeichnet sein. Die zur Begründung dienenden Tatsachen und Beweismittel sollen angegeben, der angefochtene Bescheid soll in Urschrift oder in Abschrift beigefügt werden. Der Klageschrift sind gemäß § 93 des Sozialgerichtsgesetzes nach Möglichkeit Abschriften für die Beteiligten beizufügen.