Bundesamt
für Soziale Sicherung

Bundesamt für Soziale Sicherung, Friedrich-Ebert-Allee 38, 53113 Bonn

An alle
bundesunmittelbaren
Krankenkassen

- per E-Mail -

HAUSANSCHRIFT
Friedrich-Ebert-Allee 38
53113 Bonn

TEL +49 228 619 2116
FAX +49 228 619 1872

gruppe11@bas.bund.de
www.bundesamtsozialesicherung.de

BEARBEITER(IN) THORSTEN SCHLOTTER

19. November 2020

AZ 116 – 830 – 2633/2020
(bei Antwort bitte angeben)

nachrichtlich:

Bundesministerium für Gesundheit
Aufsichtsbehörden der Länder
GKV-Spitzenverband
Verband der Ersatzkassen

**Stellungnahme des Bundesamts für Soziale Sicherung zum Einsatz der elektronischen Patientenakte nach den Vorgaben des Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (kurz: PDSG)**

**Warnung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach Artikel 58 Abs. 2 Bst. a DSGVO mit Schreiben vom 6. November 2020**

Sehr geehrte Damen und Herren,

die o. a. Warnung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) und die weiteren angedrohten Sanktionen haben bei vielen Krankenkassen für erhebliche Verunsicherung gesorgt. Daher möchten wir Sie über die Rechtslage und weitere mögliche rechtliche Konsequenzen aufklären.

Der BfDI warnt in seinem o. a. Schreiben davor, bei der Einführung der elektronischen Patientenakte (ePA) auf ein feingranulares Berechtigungsmanagement zu verzichten und lediglich die im Patientendaten-Schutz-Gesetz (PDSG) enthaltenen Vorgaben zur technischen Ausgestaltung der ePA einzuhalten. Dies würde seiner Auffassung nach gegen Artikel 25 und 32 DSGVO verstoßen.

Seitens des Bundesamtes für Soziale Sicherung (BAS) werden die Bedenken des BfDI nicht geteilt. Der Entwurf des PDSG wurde im Rahmen des Gesetzgebungsverfahrens von den Verfassungsressorts rechtlich umfassend, insbesondere auch auf die Vereinbarkeit mit übergeordnetem Recht, geprüft. Die Regelungen zur ePA sind gemessen an den Anforderungen der Datenschutzgrundverordnung (DSGVO) bereits mit ihrem Start ab dem 1. Januar 2021 auch ohne ein differenziertes, sog. feingranulares Rollen- und Rechtemanagement datenschutzkonform.

Ein wichtiges Kriterium hierfür ist die Ausgestaltung der ePA als freiwillige Anwendung, über deren Funktionsweise die Krankenkassen die Versicherten umfassend informieren müssen. Insbesondere sind damit die wesentlichen Anforderungen an eine wirksame Einwilligung der Versicherten nach Artikel 4 Nr. 11 DSGVO (freiwillige, in informierter Weise abgegebene Willenserklärung) erfüllt. Der Freiwilligkeit steht nicht entgegen, dass die Versicherten auf der ersten Umsetzungsstufe keine fein- oder mittelgranulare (dokumenten- oder kategorienbezogene) Einwilligung erteilen können. Die DSGVO fordert für eine wirksame Einwilligung keine Granularität hinsichtlich Daten in bestimmten Dokumenten. Das ausdrücklich normierte Diskriminierungsverbot in § 335 SGB V in der Fassung des PDSG gewährleistet zudem eine echte Wahlfreiheit.

Das Berechtigungsmanagement der ePA nach den §§ 339 Abs. 1, 353, 342 Abs. 2 Nr. 1 Buchstabe c SGB V genügt darüber hinaus den Datenschutzgrundsätzen der Datenminimierung (Erforderlichkeit), der Zweckbindung und der Vertraulichkeit nach Artikel 5 DSGVO. Die Frage der Einhaltung dieser Datenschutzgrundsätze nach Artikel 5 DSGVO ist letztlich ebenfalls eine Frage der Wirksamkeit der Einwilligung als Rechtsgrundlage für die Datenverarbeitung. Artikel 25 DSGVO ist eine spezielle Ausprägung dieser Datenschutzgrundsätze. Explizit verweist er auf den Grundsatz der Datenminimierung (Absatz 1) und nimmt die Erforderlichkeit in Bezug (Absatz 2). Der Norm kommt hinsichtlich der Datenschutzgrundsätze in Artikel 5 DSGVO eine ausschließlich konkretisierende Funktion zu. Vor dem Hintergrund einer freiwilligen und informierten Einwilligung und des mangelnden Verstoßes gegen die Datenschutzgrundsätze des Artikel 5 DSGVO, kann nach unserer Auffassung kein Verstoß gegen die Artikel 25 und 32 DSGVO begründet werden.

Auf der Grundlage dieser datenschutzrechtlichen Bewertung stellt sich für Krankenkassen nunmehr die Frage, ob und wie die Forderungen des BfDI rein faktisch umgesetzt werden können.

Die Regelungen des PDSG sehen vor, dass die Telematikinfrastruktur nur von solchen ePA verwendet werden darf, die durch die Gesellschaft für Telematik (gematik) zugelassen sind

(§ 341 Absatz 5 SGB V). Die Krankenkassen verfügen nach unserer Interpretation insoweit technisch über keine Möglichkeit, über die Spezifikationen der gematik hinaus eigene technische Vorgaben in der ePA zu realisieren. Die Umsetzung eines feingranularen Zugriffsmanagements unabhängig von den Spezifikationen der gematik ist somit objektiv unmöglich.

Dies führt zu einem rechtlichen Dilemma. Einerseits bewirken die Forderungen des BfDI und die angekündigten weiteren Maßnahmen, dass die Krankenkassen ihren Versicherten im Ergebnis keine ePA anbieten dürften, andererseits droht Krankenkassen die im PDSG verankerte Sanktionierung, wenn sie Ihrer gesetzlichen Verpflichtung nicht nachkommen. Soweit der GKV-Spitzenverband dies in einem entsprechenden bestandskräftigen Bescheid feststellt (§ 342 Abs. 5 S. 2 SGB V), müssen wir als Ausführungsbehörde die Höhe der Zuweisungen nach der Risikostruktur-Ausgleichverordnung entsprechend mindern (§ 270 Abs. 3 SGB V). Liegt uns ein Bescheid des GKV-Spitzenverbands vor, haben wir kein Ermessen und müssen die Sanktionierung vollziehen.

Da nicht auszuschließen ist, dass der BfDI weitere Aufsichtsmaßnahmen nach Artikel 58 Abs. 2 DSGVO prüfen und auch ergreifen wird, werden wir aber auch in unserer Rolle als Rechtsaufsichtsbehörde eingebunden. In § 16 Abs. 1 BDSG hat der Gesetzgeber Verfahrensregeln zu einem „rechtlichen Gehör“ definiert, die sicherstellen sollen, dass die Datenschutzaufsichtsbehörde vor Ausübung bestimmter Abhilfebefugnisse des Artikel 58 Abs. 2 DSGVO die zuständige Rechtaufsicht informieren und in einer angemessenen Frist die Gelegenheit einer Stellungnahme einräumen muss. Sollten die geplanten Verfügungen des BfDI der Auffassung der Rechtsaufsichtsbehörde widersprechen, kann diese die Sozialversicherungsträger zur gerichtlichen Klärung anweisen (vgl. BT-Drs. 18/11325, ab S. 88 und auch z. B. Kühling/Buchner/Wieczorek BDSG § 16 Rn. 5-9). Dies werden wir, soweit erforderlich, auch tun.

Die ausgesprochene Warnung des BfDI gehört nicht zu den Befugnissen nach Artikel 58 Absatz 2 DSGVO, die ein solches Verfahren auslösen. Hierbei handelt es sich nicht um einen Verwaltungsakt, weil die Warnung keine unmittelbaren Rechtspflichten auslöst. Bei den nächsten Schritten, die der BfDI in seinen diversen Presseberichten angedroht hat, ist aber eine Verfahrensbeteiligung durch die Rechtsaufsichtsbehörden sichergestellt.

Wir sind uns dessen bewusst, dass eine gerichtliche Klärung die Ultima Ratio sein sollte. Allen Beteiligten sollte allerdings klar sein, dass es hier nicht nur um abstrakte Rechtspositionen und deren Bestätigungen, sondern um die Weiterentwicklung der Digitalisierung im Gesundheitssystem geht. Der Datenschutz und die Sicherheit der Datenverarbeitung in der ePA sind mit Ihren Konzepten der Freiwilligkeit, der informierten Selbstbestimmung und des Diskriminierungsverbots Eckpfeiler der Digitalisierung, die für das Vertrauen und die Akzeptanz

digitaler Lösungen essentiell sind. Die neuen Regelungen des PDSG sind insoweit uneingeschränkt anzuwenden.

Mit freundlichen Grüßen
Im Auftrag

(Thorsten Schlotter)