Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Deutscher Bundestag

Ausschuss für Gesundheit

Ausschussdrucksache
20(14)236

08.11.2024

Bonn, 08.11.2024

Stellungnahme

der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zum Entwurf eines Gesetzes zur Schaffung einer Digitalagentur für Gesundheit (GDAG)

(BT-Drs. 20/13249)

Mit dem Entwurf eines Gesetzes zur Schaffung einer Digitalagentur für Gesundheit (GDAG) wird die Gesellschaft für Telematik (gematik) zur Digitalagentur Gesundheit umgewandelt und ihr werden erweiterte Befugnisse für die Telematikinfrastruktur (TI) und für die Digitalisierung im Gesundheitsbereich als Ganzes übertragen.

So identifiziert der Entwurf zutreffend das Problem der fehlenden Zuständigkeit der gematik für die Primärsysteme der Leistungserbringerinstitutionen. Deshalb werden der Digitalagentur Gesundheit in § 329 Abs. 1 – 3a SGB V im Störungsfall gewisse Befugnisse gegen Anbieter und Hersteller eingeräumt. Diese Befugnisse beschränken sich aber auf die Reaktion nach bereits aufgetretenen Störungen. Ich rate dazu, der Digitalagentur Gesundheit präventiv die Kompetenz zu geben, verbindliche Vorgaben für alle Produktteile von Primärsystemen zu erlassen, die mit der TI interagieren.

Wegen der beabsichtigten zentraleren Rolle der Digitalagentur Gesundheit rege ich außerdem eine verbindliche Beteiligung des BSI bei den Vorgaben zur Sicherheitszertifizierung für Zulassungs- und Vergabeverfahren in der TI in § 335 Abs. 3 SGB V an.

Im Einzelnen:

Zu Art. 1 Nr. 4 Buchst. b Doppelbuchst. cc; § 291a Absatz 3 SGB V – Verarbeitung der Krankenversichertennummer (KVNR) im TI-Messenger

Die vorgeschlagene neue Nummer 6 in § 291a Absatz 3 SGB V n.F. erlaubt die Speicherung des eindeutigen Identifikators (technisch: Matrix-ID) zur Nutzung des

Haus- und Lieferanschrift
Graurheindorfer Straße 153
53117 Bonn

ÖPNV-Anbindung
Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Internet www.bfdi.bund.de
Kontakt www.bfdi.bund.de/kontakt

Datenschutzerklärung
www.bfdi.bund.de/datenschutz

Sofortnachrichtendiensts der TI (TI-Messenger) auf der elektronischen Gesundheitskarte (eGK). Ausweislich der Begründung soll diese Regelung in Verbindung mit den Bestimmungen zum Versichertenstammdatenmanagement dazu führen, dass Primärsysteme aus den Stammdaten der Krankenkassen ebenfalls den Identifikator erhalten. Diese technische Maßnahme soll die Fehleranfälligkeit der Implementierung der Bildungsregel des Identifikators in Primärsystemen verschiedener Hersteller verringern. Diesem Prozess kann zugestimmt werden. Er könnte in der Tat dazu dienen, fehlerhafter Implementierungen vorzubeugen, weil der Identifikator vor Ort nicht gebildet werden muss, sondern aus den Stammdaten abgerufen werden kann.

Die Begründung legt aber zusätzlich die Bildungsregel des hier Matrix-ID bezeichneten Identifikators fest: Die Adresse soll sich demnach aus der Krankenversichertennummer (KVNR) im Klartext und einem Kennzeichen für die Krankenkasse zusammen setzen. § 290 Absatz 4 SGB V erlaubt ihre Verwendung im Rahmen der TI zur eindeutigen Identifikation des Versicherten, soweit dies für die eindeutige Zuordnung von Daten und Diensten bei der Nutzung dieser Anwendungen und Dienste erforderlich ist. Wegen ihre Schutzbedarfs, rege ich an, technische Maßnahmen zum Schutz der KVNR vorzusehen. Als geeignet sehe ich eine Pseudonymisierung mittels eines Hash-Verfahrens an, die einen gewissen Schutz gegen das Bekanntwerden der KVNR gegenüber Dritten bietet.

Diese Einschätzung ist das Ergebnis einer Prüfung zur Bildungsregel der Matrix-ID im Rahmen der Beratung der gematik, bei der Art. 25. Abs. 1 DSGVO maßstäblich war, sowie der Gesetzesbegründung des DVPMG. In der Abwägung überwog der Schutzbedarf der KVNR gegenüber den technischen und organisatorischen Argumenten. Für die KVNR ist ein hoher Schutzbedarf anzunehmen, da sie der eindeutigen Zuordnung und Verknüpfung vor allem besonderer Kategorien personenbezogener Daten dient. Der KVNR kommt die Rolle eines bereichsspezifischen Personenkennzeichens für die TI zu. Die Implementierungskosten für ein Pseudonymisierung können als gering abgeschätzt werden, da entsprechende Hash-Funktionen in allen gängigen Bibliotheken bereits vorhanden sind. Als technisch-organisatorisches Argument wurde dargelegt, dass Anpassungen in den Primärsystemen in der Vergangenheit unerwartete Herausforderungen gebracht hätten. Allerdings wurde genauso abgeschätzt, dass vor dem Hintergrund der in jedem Fall bestehenden Notwendigkeit der Integration des TI-Messenger in die Primärsysteme der zusätzliche Aufwand für die Nutzung der pseudonymen Matrix-ID vernachlässigbar sei.
Die Pseudonymisierung wird in BT-Drs. 19/27652, S. 117 zu Doppelbuchstabe cc ausdrücklich als mögliches Beispiel einer Lösung angegeben.

Jedenfalls rege ich an, § 291a Absatz 3 Nummer 6 wie folgt zu fassen:

„den eindeutigen Identifikator zur Nutzung des Sofortnachrichtendienstes der Telematikinfrastruktur nach § 363a Absatz 1 Nummer 1. Der Identifikator wird mittels eines Pseudonyms der Krankenversichertennummer gebildet.“

Zu Art. 1 Nr. 7 Buchst. b; § 307 Absatz 5 SGB V – Auskunftsrechte zu E-Rezept
Die Aufgaben der koordinierenden Stelle nach § 307 Absatz 5 SGB V sollen erweitert werden. Sie erteilt Betroffenen dann Auskunft über Protokolldaten aus der Anwendung E-Rezept. Diese neue Möglichkeit der Betroffenen zur Wahrnehmung ihrer Auskunftsrechte begrüße ich. Allerdings fehlt weiterhin eine Möglichkeit für die mutmaßlich nach wie vor große Gruppe von Versicherten, die kein Frontend nutzen, Einblick in die für sie gespeicherten E-Rezepte zu erhalten. So könnten sie ihr Auskunftsrecht nach Art. 15 Abs. 1 DSGVO ausüben. und damit ihr Recht auf Auskunft nach Art. 15 Abs. 1 DSGVO ausüben zu können. Die Betroffenenrechte der DSGVO und insbesondere das Recht auf Auskunft nach Art. 15 Abs. 1 gelten grundsätzlich für alle Betroffenen. Diese Rechte werden allerdings durch § 308 Abs. 1 SGB V beschränkt. Dort ist in Satz 1 festgelegt, dass die Betroffenenrechte nach Art. 12 – 22 DSGVO ausgeschlossen sind, wenn Verantwortliche und Auftragsverarbeiter diese nicht oder nur unter Umgehung von Schutzmechanismen befriedigen können. Die Einrichtung einer Möglichkeit zur Einsichtnahme in Daten in der Anwendung E-Rezept könnte als Umgehung von Schutzmaßnahmen, beispielsweise dem Prinzip „Zugriff nur nach Authentisierung des Betroffenen“, dargestellt werden. Demgegenüber steht aber die Tatsache, dass bereits jetzt Zugriffe auf Anwendungen der TI ohne vorherige Authentisierung und Autorisierung eines Versicherten erfolgen. Die weitestgehende Gewährleistung der Beteiligtenrechte, darunter das Auskunftsrecht der Betroffenen, zählt zum Kernbestand datenschutzrechtlicher Vorgaben und bildet insoweit bislang auch datenschutzpolitisch eine rote Linie. Ich würde es begrüßen, wenn eine solche Möglichkeit geschaffen wird, da die Anwendung E-Rezept für alle Versicherte ohne Widerspruchmöglichkeit personenbezogene Gesundheitsdaten verarbeitet und alle Versicherten eine Kontrollmöglichkeit über die für sie gespeicherten Daten erhalten sollten.

Zu Art. 1 Nr. 10 Buchst. b Doppelbuchst. aa Dreifachbuchst. bbb u. Nr. 18 Buchst. a; § 311 u. § 325 SGB V – Sicherheitsnachweis
Die Digitalagentur Gesundheit soll zukünftig nicht nur Betriebsleistungen für die zentrale Infrastruktur sondern auch Entwicklung und Betrieb von Komponenten und Diensten ausschreiben können. Im bisherigen Zulassungsmodell wurde ein Anbietermarkt gesteuert. Begründet wird die geplante Veränderung durch gestiegene Komplexität, die dafür sorgt, dass die Anforderungen an Hochverfügbarkeit und Sicherheit nicht in ausreichendem Maße erfüllt werden.

Um das Ziel einer besseren Erfüllung dieser Anforderungen zu erreichen, ist es aber erforderlich, dass sich alle Anbieter weiterhin an die Festlegungen und Maßnahmen nach §

311 Absatz 1 Nummer 1 SGB V halten. Die erforderlichen Nachweise dazu müssen genauso wie im Zulassungsverfahren erbracht werden. Dazu sollte im Gesetzestext klargestellt werden, welche Gutachten beigebracht werden müssen.

Gerade wegen der beabsichtigten zentraleren Rolle der Digitalagentur Gesundheit muss die Beteiligung einer bislang von der gematik unabhängigen dritten Stelle, hier des BSI, deren Expertise auch für die datenschutzrechtliche Bewertung bedeutsam ist, beim Nachweis der Sicherheit wieder verbindlich werden. Dazu schlage ich die Streichung von Artikel 1 Nr. 18 Buchst. a und die Anfügung von folgenden Sätzen in § 335 Absatz 3 SGB V vor:

„Der Nachweis der Sicherheit erfolgt durch eine Sicherheitszertifizierung nach den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik sowohl für das Zulassungs- als auch das Vergabeverfahren. Abweichend von Satz 2 kann die Digitalagentur Gesundheit im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik eine andere Form des Nachweises der Sicherheit festlegen, wenn eine Sicherheitszertifizierung auf Grund des geringen Gefährdungspotentials der zu prüfenden Dienste und Komponenten nicht erforderlich ist oder der hierfür erforderliche Aufwand außer Verhältnis steht und die andere Form des Nachweises die Sicherheit gleichwertig gewährleistet.“

Zu Art. 1 Nr. 10 Buchst. j; § 311 Absatz 9 SGB V – Niedrigeres Schutzniveau für Protokolldaten

Im § 311 Absatz 9 SGB V n.F. sollen die Regelungsinhalte des durch Art. 1 Nr. 11 dieses Gesetzesentwurfs wegfallenden § 312 Absatz 6 SGB V a.F. aufgefangen werden.

Der Digitalagentur Gesundheit wird in § 311 Absatz 9 Satz 1 SGB V n.F. die Aufgabe zugewiesen, Maßnahmen durchzuführen, die erforderlich sind, damit das Auslesen der Protokolldaten, wie sie gemäß § 309 Absatz 1 zum Zweck der Datenschutzkontrolle von allen TI-Anwendungen anzulegen sind, und der Daten in den Anwendungen nach § 334 Absatz 1 Satz 2 Nummer 2, 3 und 6 (Hinweise auf Vorhandensein und den Aufbewahrungsort von Organspendehinweisen und Vorsorgevollmachten, sowie E-Rezept) mittels einer Benutzeroberfläche eines geeigneten Endgeräts erfolgen kann. Gemäß Satz 3 sollen Versicherte in ein von einem hohen Sicherheitsstandard abweichendes Authentisierungsverfahren einwilligen können. Eine solche Regelung lehne ich ab, da es sich bei den aus der Anwendung von Art. 32 Abs. 1 DSGVO ergebenden technisch-organisatorischen Maßnahmen grundsätzlich um objektive Rechtspflichten der Verantwortlichen und Auftragsverarbeiter handelt, die nicht zur Disposition der Betroffenen stehen. Das Grundrecht auf informationelle Selbstbestimmung ermöglicht es zwar Betroffenen im Einzelfall, bewusst auf die ihrem Schutz dienenden technisch-organisatorischen Maßnahmen im Bereich der besonders zu schützenden Gesundheitsdaten verzichten zu können. Dieses Recht gilt aber nach Auffassung der

Datenschutzaufsichtsbehörden als lediglich auf Einzelfälle wie z.B. Notfälle beschränkt. So sieht es auch ein auf die Frage der Einordnung des Art. 32 Abs. 1 DSGVO bezogener gemeinsamer Beschluss der Datenschutzkonferenz des Bundes und der Länder vom 24.11.2021 vor. Diese objektiven Rechtspflichten zielen auf die Sicherstellung eines durchgängigen Schutzniveaus im Sinne des allgemeinen Interesses an einer sicheren Gesundheitstelematikinfrastruktur.

Zu Art. 1 Nr. 11; § 312 SGB V – Aufträge an die Digitalagentur Gesundheit
Die neue Fassung von § 312 SGB V ersetzt die detaillierte Auflistung der Aufträge an die gematik durch den Auftrag an die Digitalagentur Gesundheit, jährlich eine Roadmap zu erstellen, die die Gesellschafterversammlung genehmigen muss.

Die Abkehr von gesetzlich festgelegten Fristen ist nachvollziehbar. Allerdings sollten Aufgaben weiter durch den parlamentarischen Gesetzgeber festgelegt werden. Die Digitalagentur Gesundheit kann zur Verwirklichung der Aufträge Abhängigkeiten zwischen den Aufträgen feststellen, Projekte priorisieren und in einer Roadmap festhalten.

Zu Art. 1 Nr. 20; § 329 SGB V – Zuständigkeit für Primärsysteme
Der neuen Regelungen geben der Digitalagentur Gesundheit mehr Kompetenz, im Störungsfall Informationen von Primärsystemanbietern und -herstellern zu verlangen und zur Störungsbeseitigung aufzufordern, soweit technische Schnittstellen und Module enthalten sind, die zur Nutzung der TI erforderlich sind.

Diese Ausweitung der Kompetenz gegenüber Primärsystemherstellern und -anbietern ist sinnvoll, da in der Vergangenheit Störungen und Datenschutzverletzungen durch Fehler in Produkten verursacht wurden. Allerdings sollte die Digitalagentur Gesundheit auch ermächtigt werden, verbindliche Vorgaben zu Primärsystemen zu machen, um Störungsfällen vorzubeugen, soweit diese technische Schnittstellen und Module enthalten, die zur Nutzung der TI erforderlich sind. Durch die Abkehr von Fachmodulen auf dem Konnektor werden Sicherheits- und Fachfunktionen in die Systeme der Krankenhäuser, Praxen und Apotheken verlagert (die Anwendung E-Rezept wurde von Beginn an ohne Fachlogik auf dem Konnektor geplant; bei der elektronischen Patientenakte (ePA) wird das Fachmodul mit der „ePA für Alle“ des DigiG abgeschafft). Gleichzeitig zeigt sich, dass Fehler in den Anwendungen häufig auf mangelhafte Primärsysteme zurückzuführen sind. Verbindliche Vorschriften konnte die gematik bislang aufgrund ihrer ausschließlichen Zuständigkeit für die TI, die „im Konnektor endet“, nicht erlassen. Dass keine verpflichtenden Sicherheitsanforderungen für die Entwicklung der Primärsysteme durch die gematik erlassen werden, benennt die kürzlich veröffentlichte Sicherheitsanalyse des Fraunhofer-Instituts für sichere Informationstechnologie als Schwachstelle im Gesamtsystems ePA („Sicherheitsanalyse des Gesamtsystems ePA für alle - Version 4.0“, Fraunhofer SIT, Seite 71).

Ich rate dazu, der Digitalagentur Gesundheit die Kompetenz zu geben, verbindliche Vorgaben für alle Produktteile von Primärsystemen zu erlassen, die mit der TI interagieren.

Zu Art. 1 Nr. 28 Buchst. f; § 342 Absatz 7 Satz 1 SGB V – Stationäre Endgeräte

Angesichts der Einführung der Opt-Out-ePA ab Januar 2025 ist es nicht nachvollziehbar, warum Komponenten zur Wahrnehmung von Rechten für Betroffene auf stationären Endgeräten (z.B. Desktops) erst ab Juli 2025 zur Verfügung gestellt werden müssen. Für die auf diese Geräte angewiesenen Nutzerinnen und Nutzer wird damit zumindest übergangsweise eine Verkürzung einiger ihnen nach DSGVO zustehenden Beteiligungsrechte, wie dem Recht auf Auskunft nach Art. 15 Abs. 1 DSGVO, einhergehen, da eine Einsicht in die Inhalte der ePA über die Krankenkasse oder die Ombudsstellen nach § 342a SGB V nicht möglich ist.