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 (0228) 997799-[redacted]
E-MAIL Referat21@bfdi.bund.de
BEARBEITET VON [redacted]
INTERNET www.bfdi.bund.de
DATUM Bonn, 05.09.2022
GESCHÄFTSZ. 21-400-5/003#0003

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

gematik GmbH
z. Hd. Dr. Florian Hartge
Friedrichstraße
10117 Berlin

ausschließlich per Mail an
[redacted]

nachrichtlich an:
Bundesministerium der Gesundheit
Referat 522
Rochusstraße 1
53123 Bonn

ausschließlich per Mail an
522@bmg.bund.de

BETREFF **Feature-Spezifikation "Abruf der E-Rezepte in der Apotheke nach Autorisierung" (ursprüngliche Bezeichnung: "Abruf der E-Rezepte in der Apotheke mit personenbezogenem Identitätsnachweis")**

Sehr geehrter Herr [redacted],

bezugnehmend auf meine E-Mail vom 1. September 2022 teile ich Ihnen mit, dass das BfDI zu den von Ihnen am 29. August 2022 versandten Festlegungen der Feature-Spezifikation „Abruf der E-Rezepte in der Apotheke nach Autorisierung“ das nach § 311 Abs. 2 Satz 1 Fünftes Buch Sozialgesetzbuch (SGB V) i. V. m. Abs. 1 S. 1 e) bb), 334 Abs. 1 Nr. 6 SGB V zu prüfende Einvernehmen nicht erteilen kann.

Die Feature-Spezifikation sieht vor, dass ein Abruf von E-Rezepten aus dem E-Rezept-Fachdienst unter Nutzung der Krankenversichertennummer (KVNR) und eines unsignierten Prüfungsnachweises des Versichertenstammdatenmanagement (VSDM)-Dienstes ermöglicht werden soll. Der unsignierte Prüfungsnachweis ist prinzipiell manipulierbar und könnte Angreifern den unberechtigten Zugang zum E-Rezept-Fachdienst mit den dort gespeicherten E-Rezepten ermöglichen.



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

Den Prüfungsnachweis nicht zu signieren, entspricht nicht dem durch Art. 32 Abs. 1 b., Abs. 2 Datenschutz-Grundverordnung (DSGVO) gesetzlich zu beachtenden Stand der Technik für den Schutz personenbezogener Daten. Diese Sicherheitsschwachstelle erachte ich angesichts der damit drohenden erheblichen Risiken für der besonders schutzwürdigen Gesundheitsdaten der Bürgerinnen und Bürger für so gravierend, dass ich insoweit derzeit keine Freigabe erteilen kann.

Das BSI hält den genannten Mangel ebenfalls für so gravierend, dass es kein Einvernehmen erteilen wird.

Als Lösung schlage ich vor, zeitnah ein Verfahren zu spezifizieren, dass das Signieren des Prüfungsnachweises vorsieht.

Begründung:

Ich begrüße prinzipiell eine barrierearme Möglichkeit, E-Rezepte in den Apotheken einzulösen, die die bestehenden Möglichkeiten (Zuweisung per App und Vorzeigen des E-Rezept-Tokens in einem 2D-Code oder Papierausdruck) ergänzt. Ein Medienbruch durch einen Ausdruck oder das Installieren einer App auf dem Smartphone wären so nicht nötig. Über die Telematikinfrastruktur (TI) könnten die Rezepte auch sicher zur Apotheke gelangen.

Die im vorliegenden Dokument vorgeschlagene technische Lösung gefährdet aber den für die bundesweite Nutzung zentralisiert ausgestalteten E-Rezept-Speicher. In diesem sog. E-Rezept-Fachdienst sind sämtliche nicht eingelösten ärztliche Verordnungen aller Versicherten zentral gespeichert. Damit ergibt sich ein hohes Risiko des missbräuchlichen Zugriffs auf besonders sensitive Gesundheitsdaten für grundsätzlich alle Versicherten in Deutschland. Denn zukünftig muss jeder gesetzlich Krankenversicherte in Deutschland am E-Rezept-System teilnehmen, wenn er eine ärztliche Verordnung erhält.

Dem vorliegenden Konzept nach würde der E-Rezept-Fachdienst so geöffnet, dass Apotheken dort alle Rezepte zu einer bekannten Krankenversichertennummer (KVNR) herunterladen können. Dazu muss die Apotheke einen Nachweis mitliefern, dass die elektronische Gesundheitskarte zu dieser KVNR in ihrem Kartenleser steckt. Diesen Nachweis soll das VSDM-System der Telematik-Infrastruktur ausstellen. Doch dieser Nachweis soll nicht signiert sein und wäre somit ohne weiteres fälschbar: Dass diese Form des unsignierten Nachweises nicht sicher ist, stellen Sie im Kapitel 5 „Datenschutz und Sicherheit“ des vorliegenden Spezifikationsdokuments selber fest: „Prüfungsnachweise sind aus Gründen des

VSDM-Designs nicht signiert. Der E-Rezept-Fachdienst kann daher weder die Integrität noch die Authentizität eines Prüfungsnachweise überprüfen.“

Im Ergebnis könnten Angreifer mit einem Apotheken-Zugang zur TI (Apotheken-TI-ID) somit alle offenen E-Rezepte jeder Person, deren KVNR ihnen bekannt ist, abrufen. Angreifer könnten böswillige Akteure innerhalb von Apotheken sein, Personen, die in die IT-Systeme von Apotheken eingedrungen sind oder auch Personen, die sich eine Apotheken-TI-ID erschlichen haben. Die Aussagekraft der den ärztlichen Verschreibungen zu entnehmenden Informationen ist erheblich. Sie reicht von für die Betroffenen womöglich lediglich peinlichen Verschreibungen bis hin zu Informationen zu schweren Erkrankungen mit womöglich gravierenden Folgen wie Bloßstellungen und Diskriminierung, Ausgrenzung und Jobverlust. Angriffsszenarien sind das wiederholte Abrufen von E-Rezepten z.B. zu Werbezwecken, das gezielte Abrufen von E-Rezepten Einzelner (z.B. Prominenter oder politischer Gegner) etwa zum Zweck des sog. Doxing oder die massenhafte Kopie der Rezepte einer Vielzahl von Betroffenen zu Betrugszwecken.

Der Missbrauchsanreiz ist vor dem Hintergrund eines zentralen E-Rezepte-Speichers für alle deutschen versicherten Personen sehr hoch. Das Eintrittsrisiko ist angesichts von über 18000 Apotheken in Deutschland mit unterschiedlich stark aufgestellter IT-Sicherheit ebenfalls sehr hoch.

Als mögliche Lösung schlage ich vor, ein Verfahren zu spezifizieren, dass das Signieren des Prüfungsnachweises vorsieht. Sollte dies aufgrund der vorliegenden IT-Architektur nicht mit vertretbarem Aufwand möglich sein, berate ich Sie gerne zu alternativen Ansätzen. Infrage käme bespielhaft das Ausstellen eines Zugangstokens durch den VSDM-Dienst nach der Prüfung, ob die gültige eGK steckt. Dieser Token könnte, um Aufwände zu sparen, über das Internet versendet werden. Apothekenverwaltungssysteme (AVS) sind so erweiterbar, dass sie TI-Token transportverschlüsselt über das Internet empfangen können. Das zeigt z.B. Ihre Spezifikation „Einlösen ohne Anmeldung am E-Rezept-Fachdienst im E-Rezept-FdV“. Dort wird die Möglichkeit geschaffen, E-Rezept-Tokens ohne Anmeldung der Versicherten (d.h. ohne TI-Zugang) verschlüsselt über das Internet an die Apotheken zu senden.

Auch die direkte Kommunikation zwischen dem VSDM-Dienst und dem E-Rezept-Fachdienst und die Zuordnung mittels einer Vorgangsnummer ist eine denkbare Alternative.

Für beide Beispiele wären zwar Änderungen am AVS und E-Rezept-Fachdienst nötig. Das wäre aber auch schon bei dem von Ihnen vorgeschlagenen, nicht dem Stand der Technik entsprechenden Ansatz nötig. Hinzu kämen bei diesen Beispielen lediglich Änderungen am VSDM-Dienst.

Sollten Sie darlegen, dass trotz intensiver Prüfung keine Alternative – bevorzugt innerhalb der TI oder ersatzweise unter Nutzung des Internets – möglich sei, ist es nach meinem Verständnis weiterhin umsetzbar, mit bestehenden Mitteln das Vorhandensein einer bestimmten eGK in einer Apotheke durch PIN-Eingabe sicher zu prüfen. Hierzu müssten die gesetzlichen Krankenkassen nur die für die Nutzung der elektronischen Gesundheitskarte entsprechend notwendige Herausgabe von PIN-Nummern verstärkt anbieten und vorantreiben.

Die im Entwurf des Krankenhauspflegeentlastungsgesetzes vorgesehene Ergänzung des § 397 Abs. 2 a SGB V durch einen Bußgeldtatbestand zum Schutz der Verordnungsdaten vor missbräuchlichen Zugriffen ist als Bestreben eines verbesserten Schutzes von E-Rezepten grundsätzlich anzuerkennen. Sie taugt als bloße nachlaufende, also repressiv wirkende Sanktionsnorm nicht, um missbräuchliche Zugriffe wirksam zu verhindern. Die im vorliegenden Fall zur Anwendung kommende Datenschutzbestimmung des § 32 DSGVO hingegen zielt auf einen präventiven Datenschutz. Durch technisch-organisatorische Maßnahmen sowie im Übrigen durch ein konsequentes Privacy by Design könnten die in der vorgelegten Feature-Spezifikation angelegten Schwachstellen zum Schutz der Daten und Rechte der Bürgerinnen und Bürger von vornherein und effektiv unterbunden werden.

Mit freundlichen Grüßen
Im Auftrag

[redacted]