



## Pressemitteilung

12/2022

Berlin, den 07.11.2022

Pressestelle des Bundesbeauftragten für  
den Datenschutz und  
die Informationsfreiheit

+49 (0)228-997799-5100

pressestelle@bfdi.bund.de

Verantwortlich: Dirk Hensel

Redaktion: Christof Stein

## Abruf des E-Rezepts per eGK? Aber sicher!

**Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Professor Ulrich Kelber, erteilt der unsicheren Feature-Spezifikationsvariante „Abruf der E-Rezepte in der Apotheke nach Autorisierung“ kein Einvernehmen. Die geplante Schnittstelle ist nicht nach dem Stand der Technik abgesichert und verstößt damit gegen die Datenschutz-Grundverordnung (DSGVO). Er schlägt eine sichere, für die Versicherten, Ärzte und Apotheker vollkommen funktionsgleiche Alternative vor, bei der im Hintergrund andere Verfahren genutzt werden.**

Der BfDI ist enttäuscht über den Ausstieg der Kassenärztlichen Vereinigungen aus den Pilotprojekten zur Einführung des E-Rezeptes sowie der Meinungsäußerungen der beiden kassenärztlichen Vereinigungen und des Apothekerverbands zum Thema: „Das E-Rezept als solches und die drei ursprünglich vorgesehen Einlösungswege sind konsentiert und funktionsfähig. Auch die nun zusätzliche geplante Funktionalität der Einlösung durch Stecken der elektronischen Gesundheitskarte (eGK) ohne Eingabe einer PIN ist umsetzbar. Die geplante Datenverarbeitung mit der zunächst von der gematik vorgelegten Umsetzung verursacht allerdings ein großes Risiko für die Rechte und Freiheiten aller Nutzerinnen und Nutzer des E-Rezepts, bundesweit und bei allen Arztpraxen und Apotheken. Uns gegenüber gemachte Vorschläge zur Minderung des Problems abseits einer anderen Umsetzung verringern die Gefahren für die Versicherten nicht ausreichend. Unverständlich ist, dass Kassenärztliche Vereinigungen und Apothekerverband dieses Problem, dass ihnen seit Monaten und damit länger als dem BfDI selbst bekannt ist, nicht wahrnehmen wollen und stattdessen schon Basisabsicherungen von IT-Lösungen als überzogen diffamieren. Leidtragende sind die Patientinnen und Patienten, die gerne das E-Rezept auf einem der bereits funktionierenden Wege nutzen möchten.“

Falls es zu einem – wohl leicht umsetzbaren – Hack bei der unzureichend gesicherten, vom BfDI und auch dem Bundesamt für die Sicherheit in der Informationstechnik (BSI) nicht freigegebenen Umsetzungsvariante gekommen wäre, hätte das Vertrauen in das E-Rezept und andere Digitalisierungen des Gesundheitssystems enorm gelitten: „Ich erwarte von allen Beteiligten, dass bis zum Sommer 2023 eine sichere Lösung für das Abholen von E-Rezepten durch Stecken der eGK



zur Verfügung steht. Die kassenärztlichen Vereinigungen sollten ihren Ausstieg aus dem Pilotprojekt überdenken und nicht angeblich überzogene IT-Sicherheits- und Datenschutzanforderungen vorschieben. Schließlich stehen alle Möglichkeiten der Einreichung von E-Rezepten, die auch zum Start des Pilotprojektes vorhanden waren, weiter uneingeschränkt zur Verfügung. Neue Funktionalitäten müssen aber Standardanforderungen an IT-Sicherheit erfüllen und dürfen nicht dem unberechtigten Zugriff auf den gesamten Bestand der E-Rezepte Tür und Tor öffnen. Eine Umsetzungszeit von sechs Monaten ist dabei in der Softwareentwicklung durchaus üblich und notwendig. Unzureichend gesicherte Schnellschüsse kann der BfDI bei seinem gesetzlichen Auftrag nicht mittragen. Ich bedanke mich bei dem Teil der Berufsverbände im Gesundheitssektor, die uns in dieser Haltung klar und eindeutig unterstützen.“

Der BfDI fordert außerdem, dass das Bundesministerium für Gesundheit und der Deutsche Bundestag durchsetzen, dass vorhandene sichere und bequeme Authentisierungsmittel zum Standard werden, wie beispielsweise eine PIN für die Gesundheitskarte oder den elektronischen Personalausweis: „Es ist alles da, überprüft und könnte sofort eingesetzt werden, wenn beispielsweise die Krankenkassen endlich ihre Versicherten mit der PIN zur eGK versorgen würden. Digitalisierung im Gesundheitssektor muss richtig umgesetzt werden: Sicher, datenschutzkonform und bequem zu nutzen. Unzureichend gesicherten Lösungen werden wir auch weiter eine datenschutzrechtliche Absage erteilen.“