Landesbeauftragte für Datenschutz · Postfach 71 16 · 24171 Kiel

[redacted]

Landesbeauftragte für Datenschutz
Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223

Ansprechpartner/in:
Frau Hansen
Durchwahl: 988-1200

Aktenzeichen:
LD2-71.42/22.016

Kiel, 19.08.2022

Einschätzung zur Verarbeitung vertragsärztlicher elektronischer Verordnungen
Ihre Anfrage zu Lösungsansätzen in Bezug auf das E-Rezept

Sehr geehrte[redacted]

auf unsere Korrespondenz in obiger Angelegenheit komme ich zurück.

Unsere Rechercheergebnisse und Bewertungen habe ich in den folgenden Punkten zusammengefasst:

1. Nach dem Willen des Gesetzgebers ist für die elektronische Übermittlung und Verarbeitung vertragsärztlicher elektronischer Verordnungen von apothekenpflichtigen Arzneimitteln, einschließlich Betäubungsmitteln, sowie von sonstigen in der vertragsärztlichen Versorgung verordnungsfähigen Leistungen die Telematikinfrastruktur zu nutzen, sobald die hierfür erforderlichen Dienste und Komponenten flächendeckend zur Verfügung stehen, § 360 Abs. 1 SGB V. Die Authentifizierung durch Patientinnen und Patienten soll dabei gemäß Ihren Ausführungen entweder mit einer NFC-fähigen Gesundheitskarte, PIN und NFC-fähigem Smartphone oder teilweise mittels Anmeldung in der jeweiligen Krankenkassen-App erfolgen. Die versicherte Person kann so auf das ausgestellte E-Rezept zugreifen und dieses in einer selbst gewählten Apotheke elektronisch einlösen. Da nur sehr wenige versicherte Personen über die notwendige Technik verfügen, ist diese Art der Authentifizierung nicht kurzfristig flächendeckend umsetzbar.

2. Da nach § 360 Abs. 2 i.V.m. Abs. 1 SGB V für die Übermittlung der Verordnungen von verschreibungspflichtigen Arzneimitteln Dienste und Komponenten der Telematikinfrastruktur der Gematik zu nutzen sind, besteht keine gesetzliche Verpflichtung, auf andere (elektronische) Übertragungswege auszuweichen. Eine Übermittlung per E-Mail wird daher vom Gesetzgeber nicht gefordert.

Versicherte haben nach § 360 Abs. 9 Satz 1 SGB V gegenüber den in § 360 Abs. 2 Satz 1 SGB V genannten Leistungserbringern sowie den in § 360 Abs. 4 Satz 1 SGB V genannten

Psychotherapeuten ein Wahlrecht, ob ihnen die für den Zugriff auf ihre ärztliche oder psychotherapeutische Verordnung erforderlichen Zugangsdaten barrierefrei entweder durch einen Ausdruck in Papierform oder elektronisch bereitgestellt werden sollen. Auch hierbei hatte der Gesetzgeber die Nutzung der Telematikinfrastruktur der Gematik im Blick. Für eine geplante oder gesetzlich geforderte Versendung von QR-Codes per E-Mail an die versicherten Personen oder Apotheken bestehen keine Anhaltspunkte.

3. Mit der Versendung von QR-Codes an versicherte Personen oder Apotheken würden bereits Gesundheitsdaten nach Art. 4 Nr. 15 DSGVO i.V.m. Art. 9 Abs. 1 DSGVO übermittelt. Dabei ist zu berücksichtigen, dass auf dem Markt frei erhältliche Apps aus dem Apothekenumfeld jeder Person, die befugt oder unbefugt im Besitz des jeweiligen QR-Codes ist, die Kenntnisnahme von in der Telematikinfrastruktur der Gematik enthaltenen Daten einer Verordnung zu verschreibungspflichtigen Arzneimitteln ermöglicht: Beim Einlesen von QR-Codes in solche Apps werden die Verordnungsdaten ermittelt und den App-Nutzenden angezeigt. Die Versendung von QR-Codes per E-Mail ohne angemessene Verschlüsselung würde daher das Risiko erhöhen, dass die Gesundheitsdaten in unbefugte Hände geraten: Die frei erhältlichen Apps führen, soweit ersichtlich, keine Berechtigungsprüfung der Nutzenden durch, sodass der Name der versicherten Person, deren Geburtsdatum, Kontaktdaten des Arztes, Ausstellungsdatum der Verordnung sowie die verschreibungspflichtigen Arzneimittel mangels ausreichender technischer Sicherung von unbefugten Personen eingesehen werden könnten. Ähnliches wird wohl auch bei der Nutzung von Online-Apotheken ermöglicht.

Gesundheitsdaten weisen eine hohe Sensibilität auf. Deren Übermittlung per E-Mail ist an den Vorgaben von Art. 32 DSGVO zu messen. 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 des Risikos für die Rechte und Freiheiten natürlicher Personen müssen die Leistungserbringer geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen schließen auch die Wahl einer angemessenen Verschlüsselung ein, Art. 32 Abs. 1 Buchst. a DSGVO. Eine Transportverschlüsselung wäre für den Versand der E-Mails nicht ausreichend. Die Inhalte der E-Mails bedürfen eines zusätzlichen Schutzes. Denkbar erscheint es, der versicherten Person auf sicherem Weg getrennt ein Passwort zur Entschlüsselung der E-Mail oder eines E-Mail-Anhangs zu übermitteln, welche den QR-Code enthält. Diese zusätzliche Verschlüsselung wäre insbesondere unter Berücksichtigung des Stands der Technik und der Implementierungskosten vertretbar. Auch andere verschlüsselte und gegen unbefugte Zugriffe geschützte Kommunikationswege zwischen Leistungserbringern und versicherten Personen sind prinzipiell denkbar.

Eine Zustimmung von Versicherten in einen unverschlüsselten Versand ist hingegen rechtlich nicht möglich: Eine Einholung von Einwilligungen der versicherten Personen durch die Leistungserbringer hinsichtlich der Übermittlung der QR-Codes per E-Mail an die versicherte Person selbst oder an Apotheken unter Verzicht auf angemessene Verschlüsselung wäre unzulässig, denn die von den verantwortlichen Leistungserbringern vorzuhaltenden technischen und organisatorischen Maßnahmen beruhen auf objektiven Rechtspflichten, die nicht zur Disposition der Beteiligten stehen. Hierzu hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder in einem Beschluss vom 24.11.2021 Stellung genommen:

https://www.datenschutzkonferenz-online.de/media/dskb/20211124_TOP_7_Beschluss_Verzicht_auf_TOMs.pdf

4. In Betracht käme es auch, dass der Leistungserbringer nach Einholung einer Einwilligung der Patientin oder des Patienten nach deren bzw. dessen Wahl den QR-Code bzw. eine Verordnung zu verschreibungspflichtigen Arzneimitteln an eine bestimmte Apotheke versendet und hierzu die Telematikinfrastruktur der Gematik nutzt, beispielsweise das Verfahren KIM (Kommunikation im Medizinwesen), in dem die Kommunikation durch Ende-zu-Ende-Verschlüsselung abgesichert ist.

Für Rückfragen stehen mein Team und ich Ihnen gern zur Verfügung.

Mit freundlichen Grüßen

gez. Marit Hansen
Landesbeauftragte für Datenschutz Schleswig-Holstein