Bundesministerium
für Gesundheit

Bundesministerium für Gesundheit, 53107 Bonn

[redacted]

REFERAT Z 15 „Justiziariat, Europarechtliche Angelegenheiten"
BEARBEITET VON [redacted]
ORR
HAUSANSCHRIFT Rochusstraße 1, 53123 Bonn
POSTANSCHRIFT 53107 Bonn
TEL +49 (0)228 99 441-0
FAX +49 (0)228 99 441-4894
E-MAIL [redacted]
INTERNET www.bundesgesundheitsministerium.de

Bonn, 26. November 2018

AZ [redacted]

Ihr Antrag nach dem Informationsfreiheitsgesetz (IFG) vom 6. Oktober 2018

Sehr geehrter Herr [redacted]

mit oben genanntem Antrag erbitten Sie Zusendung

a) einer Stellungnahme des Bundesamts für Sicherheit in der Informationstechnik (BSI) zum „Entwurf eines Gesetzes zur Ausstattung der elektronischen Gesundheitskarte mit kontaktloser Schnittstelle (15. SGB V-Änderungsgesetz)" soweit diese Stellungnahme die Sicherheit der Telematikinfrastruktur betrifft,
b) weiterer Stellungnahmen anderer Stellen, z.B. Universitäten oder Unternehmen, zum selben Gegenstand.

Ferner stellen Sie eine Reihe von Fragen, die nicht auf Zugang zu amtlichen Informationen gerichtet und daher nicht Gegenstand des Antrags nach dem IFG sind. Zu diesen Fragen sind Auskünfte am Ende dieses Bescheids enthalten.

Ihr Antrag wird gemäß § 3 Nummer 3 Buchstabe b) IFG abgelehnt, da durch den Informationszugang die Beratungen von Behörden beeinträchtigt würden.

Der Entwurf des 15. SGB V-Änderungsgesetzes ist noch nicht vom Bundeskabinett beschlossen worden. Der Entwurf liegt gegenwärtig der EU-Kommission im Notifizierungsverfahren nach der Binnenmarkt-Transparenzrichtlinie [Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft] vor. Im

Rahmen dieses Verfahrens können die EU-Kommission und andere EU-Mitgliedstaaten Stellungnahmen zum dem Gesetzentwurf abgeben. Daraufhin könnten weitere Beratungen der Bundesregierung zum Gesetzentwurf erforderlich werden. Diese Beratungen würden beeinträchtigt, wenn die Stellungnahmen Dritter bereits in der Öffentlichkeit bekannt wären und diskutiert würden. Auch die Stellungnahmen, die im Rahmen des Notifizierungsverfahrens abgegeben werden sind nicht öffentlich.

Rechtsbehelfsbelehrung:

Gegen diesen Bescheid kann innerhalb eines Monats nach Bekanntgabe Widerspruch eingelegt werden beim Bundesministerium für Gesundheit, Rochusstraße 1, 53123 Bonn. Dafür stehen mehrere Möglichkeiten zur Verfügung:

1. Der Widerspruch kann schriftlich oder zur Niederschrift erhoben werden.
2. Der Widerspruch kann auch auf elektronischem Weg erhoben werden. Dafür stehen folgende Möglichkeiten zur Verfügung: Der Widerspruch kann mit qualifizierter elektronischer Signatur per E-Mail erhoben werden. Die E-Mail-Adresse lautet: Poststelle_BMG@bmg.bund.de .
   Der Widerspruch kann auch durch De-Mail in der Sendevariante mit bestätigter sicherer Anmeldung nach dem De-Mail-Gesetz erhoben werden. Die De-Mail-Adresse lautet poststelle@bundesgesundheitsministerium.de-mail.de .

Auskünfte zu Ihren weiteren Fragen

Wurde das Bundesamt für Sicherheit in der Informationstechnik (BSI) bereits um eine Stellungnahme gebeten, welche Auswirkungen die beabsichtigte Maßnahme auf die Sicherheit der Telematikinfrastruktur gem. § 291a ff SGB V haben kann? Wenn Ja, bitte ich um Zusendung dieser Stellungnahme. Wenn Nein: Warum wurde eine solche Stellungnahme nicht angefordert? Wurde ggf. eine andere Stelle (Universität, Unternehmen etc.) um eine entsprechende Stellungnahme gebeten? Wenn Ja, welche? Wenn Ja, bitte ich um Zusendung dieser Stellungnahme.

Antwort 1: Im Rahmen der Anhörungen zum Entwurf eines Gesetzes zur Ausstattung der elektronischen Gesundheitskarte mit kontaktloser Schnittstelle (15. SGB V-Änderungsgesetz) wurden unter anderem das BSI, das Bundesministerium des Innern (BMI), zu dessen Geschäftsbereich das BSI gehört sowie Verbände, deren Belange betroffen sind, beteiligt.

—

Welche Daten sollen durch die "elektronische Gesundheitskarte mit kontaktloser Schnittstelle" verschlüsselt übertragen werden?

Antwort 2: Die vorgesehene kontaktlose Schnittstelle der elektronischen Gesundheitskarte (eGK) ermöglicht die Übertragung aller Daten, auf die auch bislang über ein Kartenlesegerät zugegriffen werden kann. An dem bisherigen Umfang der Datenübermittlung ändert sich nichts.

—

In welchem Zeitraum soll auch der "Zugriff der Leistungserbringer auf Daten der elektronischen Gesundheitskarte" mittels der NFC-Schnittstelle realisiert werden?

Antwort 3: Hierzu liegen bisher keine konkreten Zeitpläne vor.

—

Sind neben den kontaktlos von der elektronischen Gesundheitskarte übertragenen Daten zur Authentifizierung gegenüber der TI weitere Authentifizierungsfaktoren (z.B. PIN-Eingabe) vorgesehen?

Antwort 4: Die bisher vorgesehene PIN-Eingabe bleibt auch mit Einführung der eGK mit kontaktloser Schnittstelle bestehen. Zusätzlich wird die Eingabe der auf der eGK aufgedruckten Card Access Number (CAN) bei Nutzung der eGK mit kontaktloser Schnittstelle notwendig.

—

Wie soll ausgeschlossen werden, dass Authentifizierungsvorgänge "belauscht" werden können (z.B. über Funkwanzen in Arztpraxen oder Trojaner auf dem Smartphone), um die gestohlenen Authentifizierungsdaten zum Zugriff auf die Gesundheitsdaten der Betroffenen in der TI benutzt werden? Wie soll sichergestellt werden, dass auf den Geräten keine Apps installiert sind, die Authentifizierungsdaten oder Gesundheitsdaten des Nutzers unbemerkt auslesen und weiterleiten?

Antwort 5: Die hier zum Einsatz kommende NFC-Technologie ist nur im unmittelbarsten Nahbereich (etwa beim direkten Auflegen auf das mobile Endgerät/weniger als 4 cm Abstand) wirksam. Zudem müssen die Versicherten bei jedem drahtlosen Einsatz der eGK die auf der eGK aufgedruckte sechststellige CAN eingeben. Anschließend wird eine verschlüsselte Verbindung zwischen eGK und mobilem Endgerät aufgebaut, sodass im Falle eines Mitlesens der Daten, diese dem Angreifer nur verschlüsselt vorliegen würden.

—

Müssen die mobilen Endgeräte, über die Zugriffe auf die Telematikinfrastruktur ermöglicht werden sollen, bestimmte Anforderungen erfüllen? Müssen sie vom BSI zertifiziert sein?

Antwort 6: Die notwendigen Sicherheitsanforderungen sind abhängig von der konkreten Anwendung und dessen Schutzbedarf. Der Gesetzentwurf trifft dazu keine Aussage.

—

Zum Hintergrund der vorstehenden Fragen: Für viele mobile Geräte gibt es ständig neue Nachfolgemodelle, mit der Folge, dass für "veraltete" Versionen meist schon zwei Jahre nach dem Kauf keine Sicherheitsupdates mehr erhältlich sind. Wie soll vermieden werden, dass Hacker dadurch entstehende Sicherheitslücken ausnutzen?

Antwort: Siehe Antworten 5 und 6.

Mit freundlichen Grüßen

Im Auftrag

[redacted]