Bundesversicherungsamt

Bundesversicherungsamt, Friedrich-Ebert-Allee 38, 53113 Bonn

An alle
bundesunmittelbaren
Sozialversicherungsträger

- nur per E-Mail -

HAUSANSCHRIFT
Friedrich-Ebert-Allee 38
53113 Bonn

TEL +49 228 619 2116
FAX +49 228 619 1872

thorsten.schlotter@bvamt.bund.de
www.bundesversicherungsamt.de

BEARBEITER(IN) Hr. Schlotter

20. Januar 2017

AZ: 116 - 8240 - 527/2016
(bei Antwort bitte angeben)

Arbeitspapier zur datenschutzrechtlichen Beurteilung des Einsatzes von mobilen Applikationen im Bereich der gesetzlichen Krankenversicherung

Sehr geehrte Damen und Herren,

die Entwicklung und der Einsatz mobiler Applikationen (im Folgenden kurz: Apps) ist Gegenstand der sog. Digitalen Transformation und damit auch Bestandteil der Veränderungsprozesse in der gesetzlichen Sozialversicherung. Vor diesem Hintergrund und auf Grundlage unserer bisherigen Beratungen haben wir einen datenschutzrechtlichen Systematisierungsansatz herausgearbeitet, der Sie bei der Frage unterstützen kann, ob ein konkreter Einsatz von Apps datenschutzrechtlich zulässig ist.

Die datenschutzrechtliche Herangehensweise zur Beurteilung des rechtmäßigen Einsatzes von Apps kann anhand eines Struktogramms verdeutlicht werden (siehe Abbildung auf der nächsten Seite, Quelle: Eigene Darstellung). Die Eingangsfrage lautet aus datenschutzrechtlicher Sicht, wer verantwortlicher Anbieter der jeweiligen App sein soll (Frage 1). Ist die Kasse Anbieter der App, ist sie auch als Adressat der datenschutzrechtlichen Vorgaben anzusehen und muss für sich auch die weiteren Fragen beantworten. Als nächstes ist dann zu fragen, ob die Kasse für das Anbieten bzw. Entwickeln einer solchen App eine Ermächtigungsgrundlage im Leistungsrecht hat (Frage 2). Wird diese Frage ebenfalls bejaht, ist weiter fraglich, ob überhaupt Sozialdaten durch die App verarbeitet werden sollen (Frage 3). Wenn Sozialdaten betroffen sind, steht weiter die leistungsrechtliche Frage im Raum, ob die Daten,

die erhoben und verarbeitet werden, für die Aufgabe der Kasse - was Art und Umfang anbelangt - erforderlich sind (Frage 4). Ist auch das der Fall, steht abschließend die Frage im Raum, ob besonders schutzbedürftige Daten betroffen sind (Frage 5). Diese Frage zielt auf das Schutzniveau und den daraus resultierenden Aufwand für die Sicherheitsmaßnahmen.

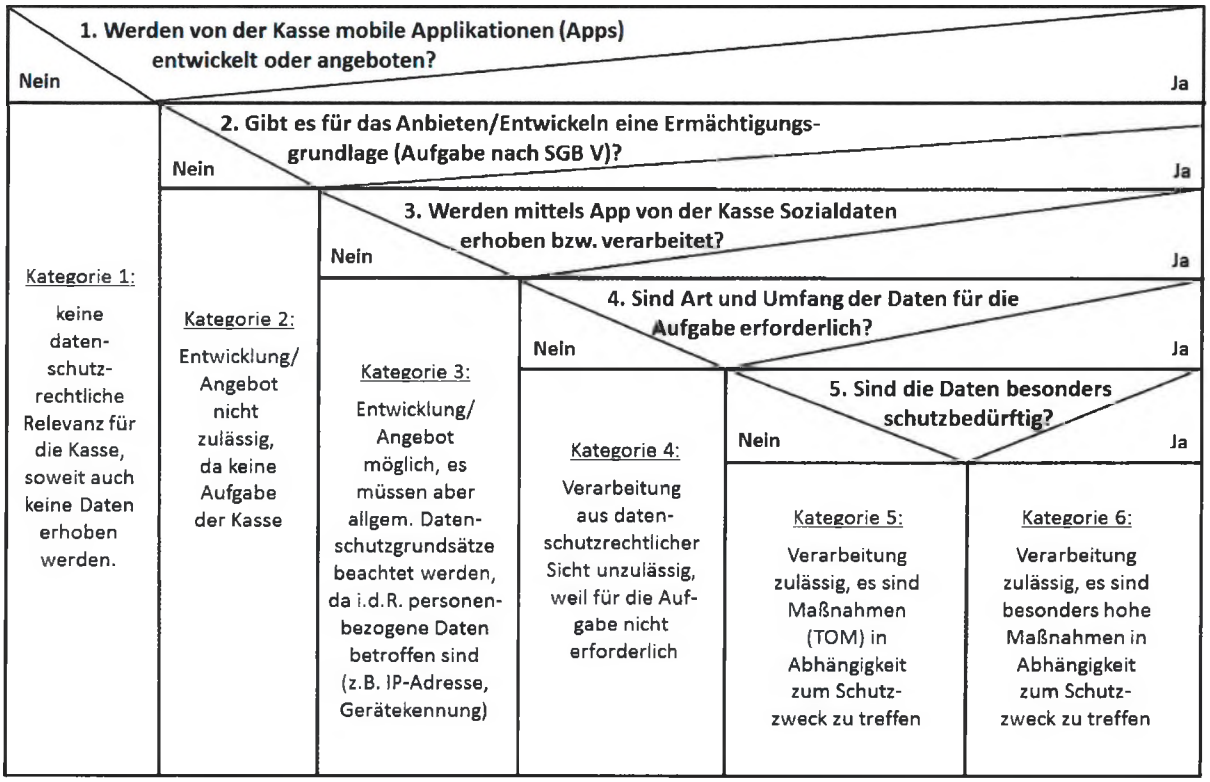

Abbildung: Einsatz von Apps im Bereich der gesetzlichen KV (Quelle: Eigene Darstellung)

Erläuterungen zu den Antwortkategorien:

In die Kategorie 1 fallen u. a. die Fitness-Apps bzw. Fitness-Tracker, deren Anschaffung von den Kassen unter bestimmten Voraussetzungen bezuschusst werden, bei denen die Kasse selbst aber nicht verantwortliche Stelle im Sinne des Datenschutzrechts ist. Adressat der datenschutzrechtlichen Vorgaben ist in diesem Fall der App-Anbieter.

Zu Kategorie 2 gehören Apps, für die es - jedenfalls bezogen auf die Kassen - keine sozialgesetzliche Ermächtigungsgrundlage gibt. Beispiele sind spezielle Gesundheits-Apps, durch die Behandlungs- und Diagnosedaten verarbeitet werden, für die eine Krankenkasse auch auf nicht-elektronischem Wege keine Erhebungsbefugnis hätte.

Zu der Kategorie 3 zählen Apps, durch die zwar keine Sozialdaten (§ 67 Abs. 1 SGB X) verarbeitet, durch die aber für die Funktionsfähigkeit andere personenbeziehbare Daten (§ 3 Abs. 1 BDSG) genutzt werden. Beispiele sind Auskunfts- und Informations-Apps, die z. B. die IP-Adresse des Nutzers (die notwendigerweise für die Internetkommunikation erforderlich ist) oder die Geräte- und Kartenkennung (die dauerhaft mit dem Gerät oder der Karte verbunden sind und folglich einem konkreten Nutzer zugeordnet werden können) verarbeiten. Die in diesem Kontext zu berücksichtigenden allgemeinen Datenschutzgrundsätze sind in der Orientierungshilfe zu den Datenschutzanforderungen an die App-Entwicklung und App-Anbieter des sog. Düsseldorfer Kreises aufgeführt (Quelle: https://datenschutz-berlin.de/attachments/ 1047/OH_Apps.pdf?1403260936, letzter Zugriff: 12.11.2016).

In die Kategorie 4 fallen Apps, die zwar von der Kasse vor dem Hintergrund bestimmter Unterstützungsleistungen angeboten werden können, durch die aber Daten verarbeitet werden, für die die Kasse keine Verarbeitungsbefugnis hat. Als Beispiel können Tagebücher (Fitness, Diabetes etc.) angeführt werden, die zwar als solche z. B. als Bestandteil einer Patientenschulungsmaßnahme rechtmäßig sein können, für die es aus datenschutzrechtlicher Sicht - jedenfalls was die Verarbeitung der Gesundheitsdaten durch die Kasse anbelangt - aber keine Verarbeitungsbefugnis gibt, sodass diese Daten auch nicht auf den Servern der Kasse verarbeitet werden dürfen (möglicherweise aber lokal in der App des Versicherten).

In die Kategorie 5 ist die große Gruppe der sog. Service-Apps einzusortieren, die zu einer „normalen", administrativen, elektronischen Kommunikation mit der Kasse dienen. Zur Gewährleistung insbesondere der Integrität, Vertraulichkeit, Verbindlichkeit und der Authentizität sind technische und organisatorische Maßnahmen (sog. TOMs) zu ergreifen, die in Abhängigkeit des jeweiligen Schutzbedarfs geeignet und verhältnismäßig sind (vgl. § 78a SGB X).

Zur Kategorie 6 zählen Apps, die besonders schützenswerte Daten gem. § 67 Abs. 12 SGB X verarbeiten. In erster Linie fallen hierunter Gesundheitsdaten, z. B. wenn die App als digitaler Zugang zur elektronischen Patientenquittung dienen soll. Eine solche Verarbeitung ist nur unter besonders hohen Sicherheitsvorkehrungen zulässig, die einen Missbrauch sehr unwahrscheinlich machen. Die technischen Hürden z. B. für die Authentisierung sind dabei regelmäßig sehr hoch anzulegen (vgl. hierzu unsere Rundschreiben vom 5. September 2014, Az. 715-8240-2028/2014 und vom 18. April 2016, Az. 116-820-981/2016; siehe auch Leitfaden Elektronische Kommunikation und Langzeitspeicherung elektronischer Daten - Version 4.1 vom 22. April 2016 der Prüfdienste nach § 274 SGB V).

Für Rückfragen stehen wir Ihnen gerne auf gewohntem Wege zur Verfügung.

Mit freundlichen Grüßen
Im Auftrag

(Thorsten Schlotter)