Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

BfDI

Datenschutz kompakt

9. Dezember 2016

diesmal:
Gesundheits-Apps

Was sind Gesundheits-Apps?

Der Markt für Apps im Gesundheitsbereich boomt. Das Angebot umfasst rund eine Million Apps mit gesundheitlichem Bezug (Fitness-, Gesundheits-, Lifestyle-Apps, Sport- und medizinische Apps) – eine einheitliche Definition existiert nicht. Gemeinsam ist ihnen, dass sie die Körperdaten ihrer Nutzer elektronisch erfassen. Während einige Apps diese Daten lediglich im Gerät selbst speichern, etwa im Smartphone, Tablet, einer Smartwatch oder einem Tracker, übermitteln andere Apps diese etwa über die Telefonfunktion des datenerfassenden Geräts an Dritte. Gesundheits-Apps dienen vor allem der Selbstvermessung und Selbstoptimierung ihrer Nutzer. Aber auch zahlreiche weitere Anwendungsszenarien sind denkbar: Medizinische Apps können beispielsweise als Helfer bei Anamnese und Therapie eingesetzt werden. Denkbar ist auch ein Einsatz in der Gesundheitsversorgung, zur Prävention und Gesundheitsförderung, im Rahmen von Bonusprogrammen, als Grundlage der Prämienkalkulation von Versicherungen oder in der Forschung.

Welche datenschutzrechtlichen Risiken bestehen?

Der Einsatz solcher Gesundheits-Apps birgt erhebliche datenschutzrechtliche Risiken. Zumeist unzureichende oder unverständliche Datenschutzerklärungen verursachen mangelnde Transparenz; die Nutzer wissen nicht, was mit ihren sensiblen Daten geschieht und worin sie einwilligen. Mängel in der technischen Datensicherheit können Unbefugten Datenzugriff ermöglichen: Das Auslesen von Login-Daten, die Weitergabe sensibler Gesundheitsdaten an Dritte oder die Einspeisung von Schadsoftware in das Gerät sind mögliche Konsequenzen. Mangelhafte oder fehlerhafte Verschlüsselung und dadurch ungeschützte Kommunikationswege erhöhen die Wahrscheinlichkeit unbefugter Zugriffe. Ein erhebliches Risiko für die Nutzer birgt auch die unberechtigte und unkontrollierte Zusammenführung sowie Auswertung der Daten. Selbst wenn personenbezogene Daten aus Apps anonymisiert verwendet würden, können die erfassten Körperdaten mit Daten kombiniert werden, die an anderer Stelle über die Nutzer frei verfügbar sind, und so zu einer Re-Identifizierung der Nutzer führen. Dadurch ließen sich umfassende Gesundheitsprofile einzelner Menschen erstellen und im Geschäftsverkehr, im Versicherungswesen oder in anderen Zusammenhängen ohne Wissen der Nutzer gegen diese verwenden.

Wie sind Gesundheitsdaten datenschutzrechtlich nach geltender Rechtslage zu bewerten?

Gesundheitsdaten gehören zu den sensibelsten aller personenbezogenen Daten. Sie sind vom Bundesdatenschutzgesetz und speziellen Regelungen zu Gesundheitsdaten in besonderer Weise geschützt. Die Erhebung, Verarbeitung und Nutzung dieser Daten bedarf einer Rechtsgrundlage und ist nur unter strengen Anforderungen zulässig. Die Einwilligung der Nutzer, die im Regelfall die Rechtsgrundlage darstellt, muss freiwillig, informiert, widerruflich und in den meisten Fällen schriftlich erfolgen. App-Nutzer sind umfassend über

die Erhebungs- und Verarbeitungszwecke sowie bestehende Risiken aufzuklären. Sie müssen jederzeit Auskunft darüber erhalten, welche Daten von ihnen gespeichert wurden. Auf Anfrage müssen diese Daten gelöscht werden. Technisch muss die App den Datenschutz gewährleisten: Einzurichten sind Zugangs-, Zugriffs- und Weitergabekontrollen, etwa durch entsprechende Verschlüsselungsverfahren. Werden Apps bei Anamnese und Therapie eingesetzt, ist zunächst entscheidend, ob sie als Medizinprodukte gelten und die rechtlichen Vorgaben des Medizinproduktegesetzes erfüllen. Werden Apps im Arzt-Patienten-Verhältnis – etwa bei der Behandlung chronisch Kranker - eingesetzt, muss die ärztliche Schweigepflicht gewahrt werden. Entweder müssen die zur Behandlung erhobenen Daten vertraulich behandelt werden oder die Patienten zuvor umfassend über die Datenflüsse und Risiken der App aufgeklärt werden, bevor sie wirksam einwilligen beziehungsweise die Entbindung von der Schweigepflicht erklären können.

Soweit gesetzliche Krankenkassen Apps anbieten, richtet sich die Zulässigkeit nach spezialrechtlichen Regelungen des Sozialgesetzbuches (SGB). Verarbeitungen von Sozialdaten, die nicht vom SGB gedeckt sind, sind unzulässig und lassen sich im Regelfall auch nicht durch eine Einwilligung des Betroffenen legitimieren. Im Gegensatz dazu besteht für den Einsatz von Apps in der privaten Krankenversicherung mehr Spielraum. Transparenz und Aufklärung der Nutzer sind hier besonders wichtig.

Die ab Mai 2018 geltende EU-Datenschutz-Grundverordnung beinhaltet keine speziellen Regelungen zum Einsatz von Gesundheits-Apps. Sie gewährt dem nationalen Gesetzgeber über ihren Artikel 9 Absatz 4 jedoch die Möglichkeit, ergänzende Regelungen im Umgang mit Gesundheitsdaten zu treffen. Entwickler und Anbieter von Gesundheits-Apps werden zudem künftig den auf europäischer Ebene erarbeiteten Code of Conduct on privacy for mHealth apps“ berücksichtigen müssen, der der Artikel 29-Gruppe derzeit zur Kommentierung vorliegt. Hersteller und Anbieter von Gesundheits-Apps müssen demnach etwa selbstverpflichtend Datenschutzfunktionen von Anfang an vorsehen („privacy by design“/„privacy by default“). Zu diesen Datenschutzfunktionen gehört insbesondere die transparente Darstellung, für welche Zwecke die Gesundheitsdaten gespeichert und an wen sie übermittelt werden.

Fazit

Der datenschutzkonforme Einsatz von Gesundheits-Apps erfordert:

- Bereits bei der Entwicklung von Gesundheits-Apps und entsprechenden Geräten (Wearables, Tracker) sind datenschutzrechtliche Vorgaben zu beachten („privacy by design“). Beim Verkauf der Geräte und der Software sind Datenschutzfunktionen vorab einzustellen („privacy by default“). Gesundheits-Apps dürfen sich nicht, wie derzeit regelmäßig der Fall, bei der erstmaligen Inbetriebnahme eines Smartphones ohne Zutun des Nutzers aktivieren.
- Nutzer von Gesundheits-Apps und entsprechenden Geräten (Wearables, Tracker) sind transparent, umfassend und verständlich über bestehende Risiken zu informieren, etwa zur Datenübermittlungen an Dritte.
- Nutzer müssen durch Aufklärung über Risiken und Gefahren bei der App-Anwendung sensibilisiert werden.
- Der Gesetzgeber sollte durch regulatorische Vorgaben für die Nutzung von Apps und dadurch erhobene Daten die Rechte der Verbraucher schützen, beispielsweise in der privaten Krankenversicherung. Dazu gehört auch das Verbot der Zusammenführung/Re-Identifizierung/Auswertung der Daten durch Dritte.

Eine stichprobenartige Überprüfung in Deutschland erhältlicher Wearables und Gesundheits-Apps durch die Datenschutzbehörden des Bundes und der Länder weist hier noch auf erhebliche Defizite hin. Ein Großteil der Anbieter informiert die Nutzer nicht ausreichend und bietet keine Löschfunktion für gesammelte Daten:

https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2016/19_Gesundheitsapps.html?nn=5217040