Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Gesundheits-Apps

Inhalt

Einführung

Mobile Technologien bestimmen unser Alltagsleben immer mehr. Insbesondere die Nutzung von Smartphones steigt stetig an. Damit verbunden ist auch die stark wachsende Nutzung von Applikationen, den sogenannten Apps. Die Anbieter von Apps haben bereits den Gesundheitssektor für sich entdeckt. Entsprechende Apps sind zum Teil bereits beim Kauf auf den Geräten vorinstalliert. Zudem wächst die Zahl der Anwender von Gesundheits-Apps rasant. Dieser Info-Flyer soll daher Gesundheits-Apps aus Sicht des Datenschutzes näher beleuchten.

Wearables und Gesundheits-Apps: Werkzeuge der digitalen Selbstvermessung

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). Oft benötigen die Gesundheits-Apps sogenannte Wearables.

Aber was sind Wearables?

Das englische Wort „wearable“ heißt übersetzt „tragbar“. Dementsprechend versteht man unter **„Wearables“** am Körper getragene technische Geräte. Hierunter fallen **Fitness-Armbänder, Smartwatches, Smartphones** oder **Tracker.** Gemeinsam ist diesen Geräten, dass sie **Körperdaten der Nutzer elektronisch erfassen.** So zählen sie etwa die Anzahl der Schritte oder messen zurückgelegte Distanzen. Auch das Schlafverhalten kann von ihnen überwacht werden. Während einige Wearables die gesammelten Körperdaten im Gerät selbst

speichern, übermitteln andere diese Daten mit Hilfe von Gesundheits-Apps über die Telefonfunktion an Dritte.

Was sind nun Gesundheits-Apps?

Leider existiert keine einheitliche Definition von Gesundheits-Apps. Im Allgemeinen sind Gesundheits-Apps auf mobilen Endgeräten installierte Anwendungsprogramme, die die Körperdaten – sowohl Gesundheitsdaten als auch Verhaltensweisen – ihrer Nutzer elektronisch erfassen und auswerten. **Sie 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, als Marketing- und Serviceinstrument, zur Prävention und Gesundheitsförderung, im Rahmen von Bonusprogrammen, als Grundlage der Prämienkalkulation von Versicherungen oder in der Forschung. Dementsprechend bieten sowohl gesetzliche als auch private Krankenkassen Gesundheits-Apps für ihre Versicherten an.

Rechtliche Rahmenbedingungen für die Nutzung von Wearables und Gesundheits-Apps

Bei den **Gesundheitsdaten**, die von Wearables und Gesundheits-Apps verarbeitet werden, handelt es sich um **personenbezogene Daten mit besonderer Sensibilität**. Sie unterliegen dem Schutz der EU-Datenschutz-Grundverordnung und des Bundesdatenschutzgesetzes. Ihre Erhebung, Verarbeitung oder Nutzung ist nur unter erhöhten Anforderungen auf Basis einer Rechtsgrundlage oder einer Einwilligung der Betroffenen zulässig. Dabei muss die **Einwilligung freiwillig**, **informiert**, **ausdrücklich und nachweislich** abgegeben werden. Zur Informiertheit gehört auch die **Transparenz**. Dies bedeutet, dass Betroffene umfassend die Zwecke kennen müssen, für die ihre Daten verwendet werden. Sie sind über die möglichen Risiken aufzuklären. Die Betroffenen haben jederzeit das Recht, über ihre **gespeicherten Daten Auskunft** zu erhalten. Die Anbieter von Gesundheits-Apps müssen durch geeignete technische und organisatorische Maßnahmen gewährleisten, dass keine Unbefugten Zugriff auf die Gesundheitsdaten haben.

Für die datenschutzrechtliche Einschätzung ist auch der jeweilige Einsatzbereich einer Gesundheits-App wichtig. Werden **Gesundheits-Apps** bei Anamnese und **Therapie** eingesetzt, ist entscheidend, ob sie als Medizinprodukte gelten und **die nationalen sowie europäischen rechtlichen Vorgaben für Medizinprodukte erfüllen**. Werden Gesundheits-Apps im Arzt-Patienten-Verhältnis – etwa bei der Behandlung chronisch Kranker – verwendet, muss die ärztliche Schweigepflicht gewahrt werden. Sozialversicherungsträger dürfen die Gesundheitsdaten der Apps nur dann verarbeiten, wenn dies nach dem Sozialgesetzbuch rechtlich zulässig ist. Eine Legitimation per Einwilligung des Betroffenen ist hier nicht möglich. Dies gilt insbesondere für die gesetzlichen Krankenkassen.

Private Krankenversicherungen haben beim Einsatz von Gesundheits-Apps rechtlich mehr Spielraum. Die Aufklärung der Nutzer ist in allen Fällen besonders wichtig.

Datenschutzrechtliche Risiken – die Nutzung von Wearables und Gesundheits-Apps ist nicht ohne Gefahren

Grundsätzlich spricht nichts gegen die datenschutzgerechte, transparente und anwenderfreundliche Nutzung von Wearables und Gesundheits-Apps. Leider hat sich aber gezeigt, dass **in der Praxis** viele **wichtige Aspekte noch nicht datenschutzkonform geklärt** wurden. Das beweist auch eine stichprobenartige Prüfung von Wearables und Gesundheits-Apps verschiedener Anbieter im Jahr 2016. Datenschutzbehörden aus Bund und Ländern wollten hierbei besser verstehen und nachvollziehen können, was mit den sensiblen Gesundheitsdaten geschieht. Dabei zeigte sich, dass **Hersteller, Betreiber** und **Verkäufer** der getesteten Wearables und Gesundheits-Apps die **Nutzer oft nicht ausreichend darüber informieren, was mit ihren Daten geschieht**. Stichpunktartige Anfragen nach Auskunft zu gespeicherten Daten wurden mit pauschalen Verweisen auf Datenschutzerklärungen beantwortet oder wegen Nicht-Zuständigkeit abgewiesen. Viele Hersteller

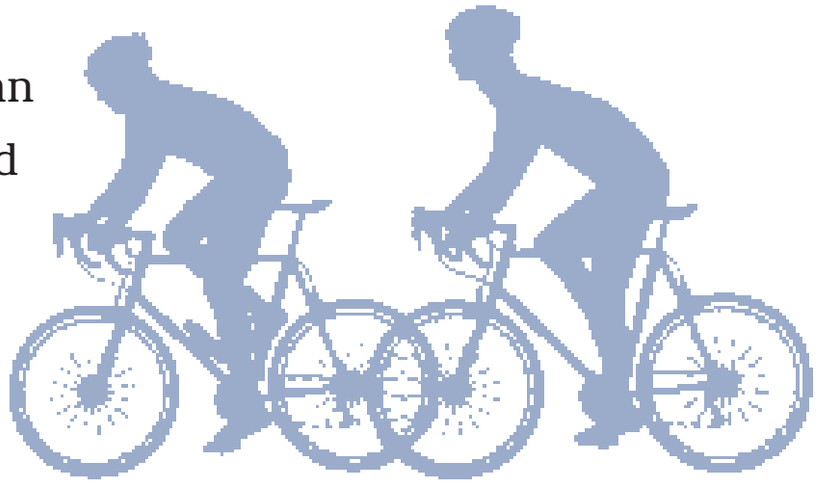
sind in Deutschland oder in anderen EU-Staaten nur mit Serviceniederlassungen präsent, während ihr Hauptsitz in anderen Nicht-EU-Staaten liegt. Mit der ab Mai 2018 EU-weit gültigen Datenschutzgrundverordnung können deutsche Aufsichtsbehörden Beschwerden deutscher Verbraucher zumindest EU-weit wirksam bearbeiten und nachverfolgen.

Derzeit erfüllen wenige Datenschutzerklärungen die gesetzlichen Anforderungen. Sie sind **zu lang** oder **schwer verständlich.** Zu essenziellen Datenschutzfragen enthalten sie nur **pauschale Hinweise.** Viele Erklärungen liegen nicht einmal in deutscher Sprache vor. Oft wird auch nur auf die **generelle Datenschutzerklärung** des Unternehmens verwiesen, die **kaum konkreten Bezug zu Wearables und den dort verarbeiteten sensiblen Gesundheitsdaten hat.**

Die durch die Wearables erhobenen Gesundheitsdaten werden oft durch externe Dritte verarbeitet. **Durch die unklaren Regelungen zur Datenverarbeitung entgleiten diese Daten dabei der**

Kontrolle durch die Nutzer. Zwar scheinen Einzelinformationen wie Körpergewicht, zurückgelegte Schritte, Dauer des Schlafes oder Herzfrequenz für sich betrachtet oftmals wenig aussagekräftig. In der Regel werden diese **Daten** jedoch **mit eindeutigen Personenkennungen oder** auch **Standortdaten verknüpft.** Bei einer dauerhaften Nutzung von Wearables fallen damit so viele Informationen an, dass sich ein **präzises Bild des Tagesablaufs und Gesundheitszustands der jeweiligen Nutzer ergibt.** Derartige Gesundheitsprofile lassen sich im Geschäftsverkehr oder Versicherungswesen **ohne Wissen der Nutzer gegen diese verwenden.** Vor allem, wenn durch unberechtigte und unkontrollierte Zusammenführung von Daten diese trotz vorheriger Anonymisierung bestimmten Nutzern zugeordnet werden können.

Viele der Wearables und Gesundheits-Apps bieten die Möglichkeit, aufgezeichnete Fitness-Daten mit Freunden zu teilen. Häufig fehlt dabei jedoch ein Warnhinweis, dass die Weitergabe der sensiblen Nutzerdaten nur dann geschehen darf, wenn der Nutzer dieses ausdrücklich wünscht und bewusst hierin einwilligt. Einige Hersteller geben zwar an, dass sie die Fitness-Daten der Nutzer für Forschungszwecke und Marketing verwenden und an verbundene



Unternehmen weitergeben. **Die Nutzer erfahren aber auch hier häufig nicht, um wen es sich dabei handelt. Auch können sie der Weitergabe ihrer Daten oft nicht widersprechen.**

Darüber hinaus bieten Geräte und Gesundheits-Apps und die damit verbundenen Nutzerkonten oft **keine Möglichkeit, Daten selbst vollständig zu löschen.** Will man etwa ein gebrauchtes Gerät weiterverkaufen, **so genügt es nicht, die App zu löschen, um bereits gesammelte Daten zu vernichten.**

Daneben können **Datensicherheitsmängel** (Auslesen von Login-Daten, Einspeisung von Schadsoftware in die Wearables, ungeschützte und unverschlüsselte Kommunikation) **oder Bedienfehler der Nutzer Unbefugten Zugriff auf die Gesundheitsdaten ermöglichen.**

Eine weitere Problematik, die sich aus der Nutzung von Wearables oder Gesundheits-Apps ergeben kann, ist der **fehlende Schutz Minderjähriger.** Eine Zustimmung der Erziehungsberechtigten wird in der Regel nicht verlangt. Aufgrund der Unerfahrenheit und unter Umständen wegen der noch fehlenden Einsichtsfähigkeit der Minderjährigen kann dies dazu führen, dass sie eine Vielzahl von Daten über sich preisgeben, ohne zu wissen, welche negativen Konsequenzen sich hieraus in ihrem weiteren Leben ergeben können (etwa beim Abschluss von Krankenversicherungen).

Datenschutzgerechter Umgang mit Wearables und Gesundheits-Apps

Der Einsatz von **Gesundheits-Apps** birgt – wie geschildert – erhebliche **Risiken für das Recht auf informationelle Selbstbestimmung.** Daher sollten die Nutzerinnen und Nutzer von Wearables und Gesundheits-Apps verantwortungsvoll und sensibel mit ihren persönlichen Daten sein. **Sie sollten beim Kauf und dem Einsatz von Wearables und Gesundheit-Apps genau auf den Schutz ihrer Daten achten und sich umfangreich und intensiv informieren.** Folgende Fragen sollten dabei beantwortet werden:

- Gibt es eine vollständige Datenschutzerklärung?
- Welche Funktionalitäten beinhaltet die Gesundheits-App?
- Welche Daten werden von mir erhoben?
- Wie werden meine Daten verarbeitet?

- Wo werden meine Daten gespeichert?
  Vorzuziehen ist eine lokale Speicherung im Gerät selbst.

- An wen werden meine Daten weitergegeben?
  Datenübermittlungen sollten weitestgehend reduziert sein.

- Welche Zugriffsrechte auf die Gesundheits-App werden gefordert
  und warum?

- Welche Löschungsmöglichkeiten habe ich selbst?
  Eine datenschutzgerechte Gesundheits-App sollte den Nutzern direkt eine Löschungsmöglichkeit einräumen.

- Wer ist für die Gesundheits-App verantwortlich?

Grundsätzlich sollten die Nutzer und Nutzerinnen keine Gesundheits-Apps verwenden, **die** eine eindeutige medizinische Zweckbestimmung haben, jedoch **nicht als Medizinprodukt gekennzeichnet sind.** Zudem sollten sie **auf vorhandene Qualitätssiegel achten** und die Bewertungen anderer Nutzer als eine erste Einschätzung heranziehen.

Herausgeber:

Der Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit
Husarenstraße 30
53117 Bonn

Tel. +49 (0) 228 99 77 99-0
Fax +49 (0) 228 99 77 99-5550
E-Mail: referat13@bfdi.bund.de
Internet: www.datenschutz.bund.de

Realisation: Appel & Klinger Druck und Medien GmbH
Bildnachweis: Adobe Stock

Stand: Januar 2019