DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

Zusammenfassung der Stellungnahme des Europäischen Datenschutzbeauftragten zu „Mobile-Health-Dienste: Lassen sich technologische Innovation und Datenschutz miteinander vereinbaren?“

(Der vollständige Text dieser Stellungnahme ist in englischer, französischer und deutscher Sprache auf der Internetpräsenz des EDSB unter www.edps.europa.eu erhältlich)

(2015/C 232/06)

Zusammenfassung

Mobile Health („mHealth“) ist ein rasch wachsender Sektor, der am Schnittpunkt von Gesundheitsfürsorge und IKT liegt. Er umfasst mobile Anwendungen, die auf intelligenten Endgeräten gesundheitsbezogene Dienste bieten sollen, wobei häufig personenbezogene Daten über Gesundheit verarbeitet werden. mHealth-Apps verarbeiten ferner große Datenmengen in den Bereichen Lifestyle und Wohlbefinden.

Der mHealth-Markt ist undurchsichtig, weil dort viele öffentliche und private Akteure gleichzeitig tätig sind, beispielsweise App-Entwickler, App-Stores, Endgerätehersteller und Werbetreibende, und ihre Geschäftsmodelle verschieben sich ständig und passen sich an sich schnell ändernde Bedingungen an. Falls sie jedoch personenbezogene Informationen verarbeiten, müssen sie dessen ungeachtet die Datenschutzvorschriften einhalten und über die von ihnen vorgenommenen Verarbeitungen Rechenschaft ablegen. Gesundheitsbezogene Informationen genießen darüber hinaus nach diesen Vorschriften besonderen Schutz.

Die Entwicklung von mHealth birgt ein großes Potenzial für die Verbesserung der Gesundheitsvorsorge und des Lebens des Einzelnen. Des Weiteren dürfte aufgrund des Volumens verfügbarer Daten und der Qualität der Schlüsse aus diesen Informationen die Massendatenverarbeitung (Big Data) zusammen mit dem Internet der Dinge erhebliche Auswirkungen auf mHealth haben. Es wird erwartet, dass sich neue Erkenntnisse für die medizinische Forschung ergeben, dass die Gesundheitskosten sinken und die Inanspruchnahme der Gesundheitsfürsorge für den Patienten einfacher wird.

Gleichzeitig gilt es aber auch, die Würde des Menschen und seine Grundrechte zu schützen, insbesondere das Recht auf Schutz der Privatsphäre und auf Datenschutz. Je mehr Big Data genutzt wird, desto weniger Kontrolle hat der Einzelne über seine personenbezogenen Daten. Dies ist teilweise zurückzuführen auf das enorme Ungleichgewicht zwischen den begrenzten Informationen, die den Menschen zur Verfügung stehen, und den umfangreichen Informationen, über die Unternehmen verfügen, die Produkte anbieten, die auch die Verarbeitung personenbezogener Daten umfassen.

Wir sind der Auffassung, dass die nachstehend beschriebenen Maßnahmen im Bereich mHealth für den Datenschutz erhebliche Vorteile brächten:

— Bei künftigen Entscheidungen über die politische Gestaltung von mHealth sollte der EU-Gesetzgeber die Rechenschaftspflicht derjenigen, die mit dem Design, der Bereitstellung und der Funktionsweise von Apps zu tun haben (einschließlich Designer und Gerätehersteller), in den Mittelpunkt rücken und ihnen mehr Verantwortung übertragen;

— App-Designer und -Publisher sollten Geräte und Apps mit dem Ziel konzipieren, für den Einzelnen mehr Transparenz und mehr Informationen bezüglich der Verarbeitung seiner personenbezogenen Daten zu erreichen und zu verhindern, dass mehr Daten erhoben werden, als es für die angestrebte Funktion erforderlich ist. Zu diesem Zweck sollten sie Schutz der Privatsphäre und Datenschutz schon in der Entwurfsphase berücksichtigen und sie zu Standardeinstellungen für den Fall machen, dass Benutzer beispielsweise bei der Installation von Apps auf ihren intelligenten Endgeräten nicht aufgefordert werden, datenschutzfreundliche Einstellungen vorzunehmen;

— die Industrie sollte Big Data im Bereich mHealth für Zwecke einsetzen, die für den Menschen von Vorteil sind, und sollte es vermeiden, sie für Praktiken zu nutzen, die dem Menschen schaden könnten, wie beispielsweise diskriminierende Profilerstellung; und

— der Gesetzgeber sollte sich für mehr Datensicherheit einsetzen und die Anwendung des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen mithilfe von Privacy Engineering und der Entwicklung von Bausteinen und Tools fördern.

Auch wenn mHealth ein neuer und sich entwickelnder Sektor ist, bieten die derzeit geltenden und mit der Reform weiter gestärkten Datenschutzvorschriften der EU Garantien für den Schutz der Daten natürlicher Personen. Wir werden dessen ungeachtet das Internet Privacy Engineering Network (IPEN) auffordern, neue vorbildliche Verfahrensweisen und innovative Lösungen für mHealth zu testen. Eine zentrale Rolle kommt in Anbetracht der globalen Dimension der Datenverarbeitung bei mHealth auch einer engeren Zusammenarbeit zwischen den Datenschutzbehörden weltweit zu.

I. **Einleitung und Hintergrund**

I.1 *Hintergrundinformationen zu mHealth — Gesellschaftliche Vorteile und Big Data*

1. Anfang der 2000er-Jahre kam es zu ersten Berührungen zwischen den Medien, der IT-Industrie und der Branche der elektronischen Kommunikation, durch die sowohl neue unternehmerische Rahmenbedingungen entstanden als auch neue regulatorische Fragen auftraten. In ähnlicher Weise hat heute die Gesundheitsindustrie neue Möglichkeiten für Entwicklung und Wachstum im Zusammengehen mit neuen Technologien (intelligente Endgeräte und entsprechende mobile Apps) gefunden. Ziel dieser Kombination ist es letztendlich, den Nutzern mithilfe intelligenter Endgeräte Gesundheitsversorgung zukommen zu lassen, und sie gilt als ein *„neuer, sich rasch entwickelnder Bereich, der das Potenzial hat, den Umbau der Gesundheitsfürsorgesysteme mitzubestimmen und deren Qualität und Effizienz zu steigern“* ([1]).

2. Es wird davon ausgegangen, dass die Konvergenz von Technologie und Gesundheitsfürsorge Folgendes bewirkt: i) bessere Gesundheitsfürsorge zu geringeren Kosten, ii) aufgeklärte Mitwirkung der Patienten (d. h. bessere Kontrolle über ihre eigene Gesundheitsversorgung) ([2]) und iii) leichterer und unmittelbarerer Zugang zu medizinischer Versorgung und Online-Informationen (z. B. durch die Möglichkeit für Ärzte, aus der Ferne Patienten zu überwachen und häufiger mit ihnen per E-Mail Kontakt zu halten).

3. Erreicht werden können solche Ziele durch Konzeption und Verteilung mobiler Endgeräte (z. B. am Körper tragbare Computer) und Apps für intelligente Endgeräte der Nutzer. Sie können immer größere Mengen personenbezogener Daten von zahlreichen „Datensensoren“ aufnehmen (die Speicher- und Rechenkapazität wächst exponentiell in dem Maße, in dem ihr Preis sinkt), die dann in den Datenzentren des Anbieters weiter verarbeitet werden, die über Rechenkapazitäten in bisher ungekanntem Ausmaß verfügen. Diese Kombination von allgegenwärtiger Nutzung und Konnektivität, auf Gewinnerzielung abhebenden Diensten, die den Nutzern kostenlos angeboten werden (vor allem kostenlose Apps für mobile Geräte), sowie Big Data und Data Mining spielen im Bereich mHealth eine entscheidende Rolle, denn sie schaffen ein digitales Abbild eines jeden von uns (das sogenannte *quantifizierte Selbst*) ([3]).

I.2 *Ziel der Stellungnahme*

4. In Anbetracht der möglichen Auswirkungen der Entwicklung von Mobile Health („mHealth“) auf das Recht natürlicher Personen auf Schutz der Privatsphäre und auf den Schutz personenbezogener Daten haben wir beschlossen, diese Initiativstellungnahme zu veröffentlichen.

5. Sie soll auf die für mHealth relevantesten Datenschutzaspekte hinweisen, die möglicherweise derzeit übersehen oder unterschätzt werden, um die Einhaltung der bestehenden Datenschutzvorschriften zu verbessern und den Weg zu einer kohärenten Anwendung dieser Vorschriften zu ebnen. Dabei baut sie auf der Stellungnahme der Artikel-29-Datenschutzgruppe zu Apps auf intelligenten Endgeräten auf ([4]).

6. Sie betrachtet ferner die Implikationen dieses neuen, sich rasant verändernden Szenarios mit Blick auf die in der vorgeschlagenen Datenschutz-Grundverordnung erwogenen Änderungen.

7. Die vorliegende Stellungnahme umfasst zwei Abschnitte. In Abschnitt II wird auf die wichtigsten Datenschutzimplikationen von mHealth eingegangen. In Abschnitt III werden Möglichkeiten für die Integration von Datenschutzanforderungen in die Entwicklung von mHealth-Apps erörtert. Es wird dabei auf ein weiteres Tätigwerden des Gesetzgebers eingegangen, das gleichzeitig wünschenswert und erforderlich ist, damit die Probleme, die mHealth im Hinblick auf Würde, Privatsphäre, Datenschutz und Recht auf persönliche Identität aufwirft oder in Zukunft möglicherweise aufwerfen wird, wirksam beantwortet werden können.

IV. **Schlussfolgerung**

69. mHealth bietet eine Fülle neuer Möglichkeiten für eine bessere und bedarfsgerechtere Gesundheitsfürsorge, bessere Prävention von Krankheiten und niedrigere Gesundheitskosten für die Sozialsysteme sowie größere Chancen für Unternehmen. Um jedoch einen Zustand zu erreichen, in dem alle drei vorstehend genannten Kategorien von diesen Entwicklungen umfassend profitieren können, muss ein jeder die Verantwortlichkeiten akzeptieren, die mit den Chancen einhergehen.

70. Insbesondere unterstreichen wir die Verantwortung gegenüber den Menschen und das Erfordernis, deren Würde und ihr Recht auf Privatsphäre und Selbstbestimmung zu wahren. Vor dem Hintergrund sich rasch wandelnder wirtschaftlicher Gegebenheiten und der dynamischen Wechselwirkung zwischen verschiedenen privaten und öffentlichen Akteuren dürfen diese Kerngrundsätze nicht außer Acht gelassen werden und sollte privater Profit nicht zu Lasten der Gesellschaft gehen.

([1]) Europäische Kommission, Grünbuch über Mobile-Health-Dienste, 10. April 2014, COM(2014) 219 final, ergänzt durch eine Arbeitsunterlage der Kommissionsdienststellen (SWD(2014) 135 final).

([2]) Nathan Cortez, *The Mobile Health Revolution?*, University of California Davis Law Review, Vol. 47, S. 1173.

([3]) Kelvin Kelly, der Gründer von *Wired*, richtete die Plattform *quantifiedself.com* zusammen mit dem Journalisten Gary Wolf ein und machte das Konzept einer breiteren Öffentlichkeit bekannt.

([4]) Artikel-29-Datenschutzgruppe, Stellungnahme 2/2013 vom 27. Februar 2013 zu Apps auf intelligenten Endgeräten (WP 202), abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_de.pdf

71. Daher bieten Datenschutzgrundsätze und -vorschriften Hilfestellung in einem bisher weitgehend unregulierten Sektor. Die korrekte Einhaltung dieser Grundsätze und Vorschriften erhöht die Rechtssicherheit, steigert das Vertrauen in mHealth und trägt auf diese Weise zur vollen Entfaltung dieses Bereichs bei.

Brüssel, den 21. Mai 2015

Giovanni BUTTARELLI

Europäischer Datenschutzbeauftragter