EUROPEAN DATA PROTECTION SUPERVISOR

Stellungnahme 1/2015

Mobile-Health-Dienste

Wie lassen sich technologische Innovation und Datenschutz miteinander vereinbaren?

21. Mai 2015

INHALTSVERZEICHNIS

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 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.

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE,

gestützt auf die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, insbesondere auf Artikel 41 Absatz 2 und Artikel 46 Buchstabe d,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

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 mit Hilfe 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 so genannte *quantifizierte Selbst*)[3].

[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.

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.

II. DATENSCHUTZIMPLIKATIONEN VON mHEALTH

II.1 Vorgaben aus den EU-Vorschriften

8. Der Schutz der Privatsphäre und der Schutz personenbezogener Daten sind Grundrechte, die in den Artikeln 7 und 8 der Charta der Grundrechte der EU verankert sind[5]. Darüber hinaus bestehen spezifische Vorschriften, die derzeit auch auf mHealth anzuwenden und in der Datenschutzrichtlinie[6] und in der Datenschutzrichtlinie für elektronische Kommunikation[7] niedergelegt sind. Sie besagen, dass bei jeglicher Verarbeitung personenbezogener Daten bestimmte Garantien einzuhalten sind; so dürfen beispielsweise personenbezogene Daten nur für bestimmte Zwecke verarbeitet werden (Zweckbindung) und sollten nicht an einen Bestimmungsort außerhalb der EU übermittelt werden, der kein angemessenes Schutzniveau bietet (internationale Übermittlungen). Insbesondere

[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 .

[5] Zum Unterschied zwischen den beiden in Artikel 7 bzw. 8 geregelten Grundrechten siehe die Leitlinien des EDSB zum Datenschutz in der Regulierung von Finanzdienstleistungen auf EU-Eben, abrufbar unter https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Thematic%20Guidelines/14-11-25_Financial_Guidelines_DE.pdf.

[6] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995, S. 31.

[7] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.7.2002, S. 37.

gesundheitsbezogene Daten genießen einen größeren Schutz und dürfen nur verarbeitet werden, wenn bestimmte Voraussetzungen erfüllt sind; so bedarf es vor allem der Einwilligung des Nutzers für den konkreten Fall und in Kenntnis der Sachlage[8].

II.2 Definition der Arten von Daten, die im Zusammenhang mit mHealth verarbeitet werden

9. Die erste zu klärende Frage lautet, ob die im Rahmen von mHealth verarbeiteten Daten personenbezogene Daten über bestimmte oder bestimmbare natürliche Personen sind und damit unter den Rechtsrahmen für den Datenschutz fallen. Wenn diese Frage bejaht wird, muss bestimmt werden, ob, und wenn ja, welche dieser Daten als gesundheitsbezogene Daten einer Person zu gelten haben und damit den für besondere Datenkategorien geltenden strengeren Datenschutzvorschriften unterliegen. Von Belang ist diese Frage vor allem im Hinblick auf die großen Mengen an Informationen über Lifestyle und Wohlbefinden, die häufig über intelligente Endgeräte und soziale Apps weitergegeben werden[9].

Im Zusammenhang mit mHealth verarbeitete Daten sind personenbezogene Daten

10. Zur ersten oben gestellten Frage sei angemerkt, dass **im Zusammenhang mit mHealth verarbeitete Daten grundsätzlich personenbezogene Daten sind**, da sie bestimmte oder bestimmbare natürliche Personen betreffen (Artikel 2 Buchstabe a der Richtlinie 95/46/EG, nachstehend „die Richtlinie“).

11. Pseudonymisierung und selbst Anonymisierung[10] ändern grundsätzlich nichts daran, dass die Datenschutzgarantien auf mHealth-Daten anzuwenden sind. **Pseudonyme Daten sind und bleiben personenbezogene Daten, da nicht nur der für die Verarbeitung Verantwortliche, sondern auch Dritte durch Kombination mit externen Informationen aus anderen Quellen die Person erneut bestimmen können[11].**

Sind alle im Zusammenhang mit mHealth verarbeiteten Daten als sensible Gesundheitsdaten zu behandeln?

12. Zur zweiten Frage sei gesagt, dass in vielen Fällen im Zusammenhang mit mHealth verarbeitete Daten sich auf den körperlichen (oder seelischen) Gesundheitszustand der

---

[8] Artikel 8 der Richtlinie verbietet die Verarbeitung besonderer (also „schutzbedürftiger“) Kategorien von Daten, darunter Gesundheitsdaten, wobei eine Reihe von Ausnahmen vorgesehen ist, die aber eng auszulegen sind.

[9] Im Grünbuch der Kommission heißt es: Unter mHealth versteht man *„medizinische Verfahren und Praktiken der öffentlichen Gesundheitsfürsorge, die durch Mobilgeräte wie Mobiltelefone, Patientenüberwachungsgeräte, persönliche digitale Assistenten (PDA) und andere drahtlos angebundene Geräte unterstützt werden“*. Dazu gehören *„Lifestyle- und Gesundheits-Apps, die mit medizinischen Geräten oder mit Sensoren (z. B. in Armbändern und Uhren) vernetzt werden können, wie auch persönliche Hinweis- bzw. Begleitsysteme, per SMS übermittelte Gesundheitsinformationen und Erinnerungen an die Medikamenteneinnahme sowie drahtlos bereitgestellte Telemedizindienste“*.

[10] Selbst als anonymisiert geltende Daten können immanente Merkmale aufweisen, die zur Bestimmung einer konkreten natürlichen Person führen (wenn z. B. es um eine seltene Krankheit geht, unter der weltweit nur wenige Menschen leiden, dann besteht die Gefahr, dass diese Menschen leicht zu bestimmen sind).

[11] Siehe Artikel 29-Datenschutzgruppe, Stellungnahme 4/2007 vom 20. Juni 2007 zum Begriff „personenbezogene Daten“ (WP 136), abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf, und Stellungnahme 5/2014 vom 10. April 2014 zu Anonymisierungstechniken (WP 216), abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf.

Personen beziehen oder darüber Auskunft geben, die die Geräte oder Apps nutzen[12], und somit den für besondere Datenkategorien (Artikel 8 der Richtlinie) geltenden strengeren Datenschutzvorschriften unterliegen. Es gibt allerdings auf diese Frage keine einfache endgültige Antwort: Eine Beurteilung der Frage, welche im mHealth-Bereich verarbeiteten Daten sensible Gesundheitsdaten sind, kann nur fallweise erfolgen. **Daten über Lifestyle und Wohlbefinden dürften generell als Gesundheitsdaten gelten, wenn sie in einem medizinischen Kontext verarbeitet werden (wenn z. B. der Patient die App auf Rat des Arztes nutzt), oder wenn Informationen über den Gesundheitszustand einer Person vernünftigerweise aus den Daten (allein oder in Kombination mit anderen Informationen) abgeleitet werden können, insbesondere dann, wenn der Zweck der App darin besteht, die Gesundheit oder das Wohlbefinden der Person zu überwachen (in einem medizinischen oder einem anderen Kontext).**

13. Der bestehende EU-Rechtsrahmen für den Datenschutz enthält zwar Vorschriften für die Verarbeitung sensibler Daten (einschließlich Gesundheitsdaten), doch bietet er keine Definition des Begriffs „Gesundheitsdaten“ (auf der Ebene der einzelnen Mitgliedstaaten stellt sich die Lage anders dar)[13].

14. In der Datenschutz-Grundverordnung[14], deren Annahme noch aussteht, findet sich eine Definition von *„Gesundheitsdaten“*, die besagt: *„Informationen, die sich auf den körperlichen oder geistigen Gesundheitszustand einer Person oder auf die Erbringung von Gesundheitsleistungen für die betreffende Person beziehen“*[15]. Interessanter ist die umfassende, aber nicht erschöpfende Auflistung in Erwägungsgrund 26 der Datenschutz-Grundverordnung[16], die jedoch nicht konkret auf die Frage eingeht, ob, und wenn ja, in welchem Umfang Informationen über Lifestyle und Wohlbefinden in die Kategorie Gesundheitsdaten fallen.

[12] Zu Gesundheitsdaten zählen auch Verwaltungsunterlagen, die personenbezogene Daten in Zusammenhang mit dem Gesundheitszustand einer Person enthalten. Zu diesen Dokumenten gehören ärztliche Atteste (z. B. Bescheinigungen der Arbeitsunfähigkeit), Formulare in Zusammenhang mit Krankenurlaub oder der Erstattung medizinischer Ausgaben. Siehe die Leitlinien des EDSB für die Verarbeitung von Gesundheitsdaten am Arbeitsplatz durch Organe und Einrichtungen der Gemeinschaft, September 2009, S. 2.

[13] Nähere Einzelheiten sind dem ersten Bericht der Europäischen Kommission über die Umsetzung der Datenschutzrichtlinie zu entnehmen, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0265:de:NOT.

[14] COM(2012) 11 final.

[15] Datenschutz-Grundverordnung, Artikel 4 Absatz 12.

[16] Erwägungsgrund 26 lautet: *„Zu den personenbezogenen Gesundheitsdaten sollten alle Daten gezählt werden, die sich auf den Gesundheitszustand eines von der Verarbeitung Betroffenen beziehen, außerdem Informationen über die Vormerkung der betreffenden Person zur Erbringung medizinischer Leistungen, Nummern, Symbole oder Kennzeichen, die einer bestimmten Person zugeteilt wurden, um diese für medizinische Zwecke eindeutig zu identifizieren, jede Art von Informationen über die betreffende Person, die im Rahmen der Erbringung von medizinischen Dienstleistungen erhoben wurden, Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz, darunter biologischer Proben, abgeleitet wurden, die Identifizierung einer Person als Erbringer einer Gesundheitsleistung für die betroffene Person sowie Informationen etwa über Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Behandlungen oder den physiologischen oder biomedizinischen Zustand der betroffenen Person unabhängig von der Herkunft der Daten, gleich, ob sie von einem Arzt oder sonstigem medizinischen Personal, einem Krankenhaus, einem medizinischen Gerät oder einem In-Vitro-Diagnose-Test stammen“.*

15. Im erläuternden Bericht zum Übereinkommen Nr. 108 des Europarates[17] heißt es, dass der Begriff „gesundheitsbezogene personenbezogene Daten“ auch *„Informationen über den vergangenen, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand einer Person* [umfasst]. *Diese Informationen können sich auf eine Person beziehen, die krank, gesund oder verstorben ist“*. Es sei in diesem Zusammenhang unterstrichen, dass der Begriff sich auch auf gesunde Personen beziehen kann (was dafür sprechen würde, dass Informationen über Lifestyle und Wohlbefinden ebenfalls aufgenommen werden sollten, da diese Informationen in der Lage sind, die künftige Gesundheit eines gesunden Menschen zu berühren).

16. **In Ermangelung einer klaren Definition sollte der Begriff Gesundheitsdaten nach einer Prüfung der jeweiligen Umstände eines Falls weit gefasst werden,** damit er alle Informationen über die körperliche und geistige Gesundheit eines Menschen umfasst[18]. Angemessen zu berücksichtigen ist ferner, dass nicht nur das Wesen der Informationen sie zu Gesundheitsdaten macht. Auch die näheren Umstände der Erhebung und Verarbeitung solcher Informationen spielen eine Rolle. Nach Auffassung einer nationalen Datenschutzbehörde[19] kann nicht immer klar zwischen dem Begriff Gesundheitsdaten und Informationen über Wohlbefinden unterschieden werden. Vielmehr sind die Grenzen fließend zwischen Fällen, in denen Informationen über Wohlbefinden nur wenig oder gar nichts mit der Gesundheit einer Person zu tun haben, und Fällen, in denen – je nach den Umständen der Erhebung und Verarbeitung der Daten einschließlich des Umfangs und der Zweckbestimmungen der Verarbeitung – die Informationen eindeutig Gesundheitsdaten sind und vielleicht sogar in einem medizinischen Kontext verwendet werden.

17. Das bedeutet im Ergebnis, dass eine zu enge Auslegung des Begriffs Gesundheitsdaten die Menschen eines angemessenen Schutzes ihrer Informationen über Lifestyle und Wohlbefinden berauben würde, die ja sehr intime Informationen über sie enthalten können, sie so ihr Vertrauen verlieren würden und damit die möglichen wirtschaftlichen und sozialen Vorteile von mHealth gefährdet wären[20].

18. Die Verantwortung liegt auf jeden Fall bei den für die Verarbeitung der personenbezogenen Daten Verantwortlichen, die Rechenschaft darüber ablegen sollten, wie sie rechtlich die von ihnen verarbeiteten Lifestyle-Informationen definieren. In den meisten Fällen liegen ihnen Anhaltspunkte vor, die eine Einstufung solcher Informationen als Gesundheitsdaten erforderlich machen. Wie die Artikel 29-Datenschutzgruppe bereits festgestellt hat, **können Lifestyle-Daten in manchen Fällen *„Informationen über die Gesundheit einer Person liefern, da die Daten zeitgebunden erfasst werden und daher***

[17] Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, 28. Januar 1981, Nr. 108.

[18] Bei beiden Datenkategorien (Daten über Lifestyle und Wohlbefinden) können gesundheitsbezogene Daten verarbeitet werden und kann somit das in Artikel 8 der Richtlinie vorgesehene höhere Schutzniveau ausgelöst werden. Siehe die Stellungnahme des EDSB vom 27. März 2013 zu der Mitteilung der Kommission über den „*Aktionsplan für elektronische Gesundheitsdienste 2012-2020 – innovative Gesundheitsfürsorge im 21. Jahrhundert*“, Punkte 10-11.

[19] Commission Nationale de l´Informatique et des Libertés (CNIL), *Le Corps, Nouvel Object Connecté`*, Cahiers IP no. 2.

[20] In Rahmen einer Initiative des Global Privacy Enforcement Network (GPEN) haben sich Datenschutzbehörden intensiv mit mHealth-Apps befasst. Siehe ferner die Artikel 29-Datenschutzgruppe in ihrem Schreiben an die Kommission vom 5. Februar 2015, abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_en.pdf .

die Möglichkeit bieten, im Zeitverlauf aus ihren Veränderungen Schlüsse zu ziehen. ***Die für die Verarbeitung Verantwortlichen sollten diesen Wandel vorhersehen und entsprechend angemessene Maßnahmen ergreifen"*[21]. Eine solche Vorschrift verlagert den Aufwand für die Beurteilung der Art der verarbeiteten Daten (und damit letztendlich der Einhaltung des Gesetzes) wirksam auf den für die Verarbeitung Verantwortlichen, also die Stelle, die am besten Bescheid weiß[22].

Welche Auswirkungen hat es, wenn personenbezogene und sensible Daten in mHealth nicht erkannt und nicht angemessen geschützt werden?

19. Das Grünbuch der Kommission zu mHealth bietet Belege für den Umfang des Risikos durch fehlenden Schutz natürlicher Personen. Neuere Schätzungen[23] beziffern die Zahl der derzeit auf zahlreichen Plattformen verfügbaren mHealth-Apps auf 97 000, von denen sich 70 % mit der Fitness und dem Wohlbefinden des Verbrauchers befassen und sich 30% an Angehörige von Gesundheitsberufen wenden[24]. Ferner wird erwartet, dass bis 2017 3,4 Mrd. Menschen weltweit ein Smartphone ihr Eigen nennen werden und die Hälfte von ihnen mHealth-Apps nutzen wird[25].

20. Im Gegensatz zu den oben genannten Zahlen, die auf einen tendenziellen Boom weisen, heißt es im Grünbuch, dass nur 23 % der Menschen irgendeine mHealth-Lösung genutzt haben. 67 % beabsichtigen nicht, ihr Mobiltelefon zur Förderung ihrer Gesundheit einzusetzen, und 77 % haben ihr Handy noch nie für gesundheitsbezogene Tätigkeiten genutzt[26]. 45 % der Menschen haben Bedenken ob der unerwünschten Verwendung ihrer Daten, wenn sie ihr Mobiltelefon für gesundheitsbezogene Tätigkeiten nutzen[27]. Diese Bedenken werden von dem Befund untermauert, dass neun der 20 beliebtesten gesundheitsbezogenen Apps nachweislich Daten an Unternehmen übermitteln, die Einzelheiten über die Handy-Nutzung durch die Menschen verfolgen[28].

21. Den oben genannten Zahlen ist zu entnehmen, dass die größte Gefahr mangelndes Vertrauen wegen unzureichenden Schutzes der Daten von mHealth-Nutzern ist. **Sollte es dem Gesetzgeber, den Regulierungsbehörden und den für die Verarbeitung Verantwortlichen nicht gelingen, genau festzulegen, was personenbezogene und sensible Daten sind (indem sie beispielsweise die Ansicht vertreten, dass Lifestyle-Informationen unter keinen Umständen als sensible Gesundheitsdaten betrachtet werden), würde dies die Nutzer von der Nutzung von mHealth abhalten.** Umgekehrt hingegen werden wirksame Datenschutzmechanismen die aufgeklärte Mitwirkung und das Engagement des Nutzers im Bereich mHealth steigern[29].

---

[21] Artikel 29-Datenschutzgruppe, Stellungnahme zum Internet der Dinge, S. 17.
[22] Einige Hinweise zur Definition von Gesundheitsdaten gab die Artikel 29-Datenschutzgruppe in ihrem Schreiben vom 5. Februar 2015, abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_en.pdf.
[23] Research2Guidance (2013), *„The mobile health global market report 2013-2017: the commercialisation of mHealth apps"*, Vol. 3.
[24] Deloitte Studie *„mHealth in a mWorld"*, 2012.
[25] Research2Guidance, *cit.*
[26] Bohem E., *Mobile Healthcare´s Slow Adoption Curve*, 2011, Forrester Research Inc.
[27] Blue Chip Patient Recruitment. *Leveraging Mobile Health Technology for Patient Recruitment*, October 2012.
[28] Financial Times, *Health apps run into privacy snags*, 1.9.2013.
[29] Stellungnahme des EDSB zum *Elektronische Gesundheitsdienste Aktionsplan 2012-2020*, Punkt 13.

II.3 Ein Markt mit vielen Akteuren: Zuweisung von Verantwortlichkeiten und Gewährleistung der aufgeklärten Mitwirkung der Nutzer

22. **Die verschiedenen Akteure der mHealth-Industrie, also App-Entwickler, Hersteller von Betriebssystemen und Geräten, App-Stores und Dritte (z. B. Werbetreibende), stützen sich auf Geschäftsmodelle, deren Grundlage, wenn auch in unterschiedlichem Ausmaß, die Monetarisierung der von Nutzern erzeugten (oder sie betreffenden) personenbezogenen Daten ist**.

23. Da die Geschäftsmodelle zu neuen Modalitäten der Monetarisierung personenbezogener Daten übergehen (z. B. *Plattformen* und so genannte *Coopetition*[30]), wird es für Nutzer immer schwieriger, nicht nur die *tatsächliche Nutzung* ihrer Daten, sondern auch die *Wiederverwendung* von Daten durch kommerzielle Partner des für die Verarbeitung Verantwortlichen und die *potenzielle Verwendung* zu kontrollieren, die erfolgen könnte, wenn sich aufgrund technologischer und wirtschaftlicher Entwicklungen neue Möglichkeiten der Monetarisierung auftun. So können beispielsweise personenbezogene Daten, die ursprünglich für einen Patientenverband als Information über eine bestimmte Krankheit gedacht waren, später von diesem Verband an ein pharmazeutisches Unternehmen weitergegeben werden, das ein Medikament gegen diese Krankheit vertreibt und die Daten für kommerzielle Zwecke nutzen wird. Wie es in der bereits erwähnten Stellungnahme des EDSB[31] heißt, ist die Monetarisierung ein äußerst dynamisches Phänomen und wirft eine Reihe schwerwiegender Datenschutzprobleme auf.

24. **Zunächst einmal kann es in Anbetracht der Vielzahl der Akteure in der mHealth-Industrie und der verschiedenen Rollen diese Akteure schwierig sein, alle für die Verarbeitung Verantwortlichen zu identifizieren und die Verantwortlichkeiten angemessen zuzuweisen.** Es ist aber unbedingt erforderlich, den/die für die über mobile Endgeräte und Apps durchgeführte Verarbeitung Verantwortlichen zu bestimmen, der/die für die Einhaltung des Datenschutzrechts verantwortlich ist/sind[32]. **Jede Stelle muss transparent und sichtbar sein und allein oder gemeinsam mit anderen Rechenschaft über ihren Umgang mit personenbezogenen Daten ablegen.**

25. Zweitens ist es für Personen schwierig, umfassend informiert zu sein und damit die Verwendung ihrer personenbezogenen Daten zu kontrollieren, die, insbesondere in plattformgestützten Unternehmen (z. B. sozialen Netzwerken), an verschiedene Stellen übermittelt und dort verarbeitet werden (Gerätehersteller, App-Publisher, Plattformbetreiber und andere für die Verarbeitung Verantwortliche oder Auftragsverarbeiter). Weil es an Transparenz mangelt und nur spärliche Informationen über die Art der Verarbeitung der personenbezogenen Daten vorliegen, sind Personen nicht in der Lage, ihre explizite Einwilligung zu geben[33].

---

[30] CNIL, *cit.*, S. 31. Zentrales Merkmal dieses Modells ist die Fähigkeit des Betreibers, tatsächliche oder potenzielle Wettbewerber zu kommerziellen Partnern zu machen und somit aus dem Wettbewerb zwischen Unternehmen die so genannte *Coopetition* zu machen.

[31] Stellungnahme des EDSB vom März 2014 zu *Privatsphäre und Wettbewerbsfähigkeit im Zeitalter von Big Data*: *das Zusammenspiel zwischen Datenschutz, Wettbewerbsrecht und Verbraucherschutz in der digitalen Wirtschaft.*

[32] Siehe Artikel 29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, WP 169, vom 16. Februar 2010.

[33] Artikel 29-Datenschutzgruppe, Stellungnahme zu Apps auf intelligenten Endgeräten, S. 5.

26. Das Problem ist also die Asymmetrie im Wissensstand von Betreibern und Nutzern. Einerseits werden Marktteilnehmer, die in einer Reihe von Branchen tätig sind (Gesundheitswesen, Technologie, Werbung, Versicherung usw.), alle Möglichkeiten prüfen, um Daten im Rahmen neuer kommerzieller Initiativen zu verwerten und ihren Gewinn zu steigern. Andererseits wissen und verstehen die Nutzer praktisch nichts von der geschäftlichen Dynamik, die die Verarbeitung ihrer personenbezogenen Daten zur Folge hat. **Die immer größer werdenden Datenmengen, die als Folge der Tendenz, Big Data zu nutzen, verfügbar sind und verarbeitet werden, werden diese Asymmetrie im Wissensstand nur verstärken und die Kluft zwischen für die Verarbeitung Verantwortlichen und Nutzern vergrößern.**

II.4 Die Auswirkungen von Big Data auf mHealth

27. Aufgrund der Entwicklung von mHealth wird allenthalben erwartet, dass sich Big Data spürbar auf die Gesundheitsfürsorge auswirken wird. **Da Big Data die Möglichkeit bietet, Verknüpfungen zwischen bisher nicht miteinander verknüpften Datensätzen herzustellen – und damit weitere Schlüsse zu ziehen –, wird es der medizinischen Forschung neue Einblicke vermitteln, die zuvor nicht zu erhalten waren[34].** So wird es beispielsweise möglich sein, Erkrankungen wie Fettleibigkeit, Herz-Kreislauf-Erkrankungen oder Depression mit menschlichem Verhalten, Lifestyle oder anderen Ursachen zu verknüpfen, die für einen bestimmten geografischen Bereich oder eine Gruppe von Personen charakteristisch sind.

28. Big Data kann auch Entscheidungsprozesse oder die Sammlung relevanter Informationen auf der Nutzerseite erleichtern[35]. Dessen ungeachtet dürfte Big Data in der kommerziellen Ausbeutung der durch die Kombination von Daten gewonnenen Erkenntnisse die größten Auswirkungen auf die Privatsphäre des Einzelnen haben (und die größten Bedenken hervorrufen).

29. Die Wirtschaftstheorie besagt, dass ein Anbieter seinen Gewinn maximiert, wenn er in der Lage ist, Kunden zu identifizieren (und dann gegebenenfalls Preisdiskriminierung auszuüben). Bleiben alle Patienten unidentifiziert, gilt grundsätzlich, dass ein Pharmaunternehmen für ein Arzneimittel vermutlich von allen den gleichen Preis verlangen wird. Ist das gleiche Unternehmen hingegen in der Lage, zu ermitteln, welche seiner Kunden über größere finanzielle Mittel verfügen oder das Arzneimittel dringender benötigen, kann es von diesen Kunden einen höheren Preis verlangen (z. B im Wege einer „Premium"-Version des Arzneimittels, die angeblich besser wirkt). Big Data könnte eine solche Diskriminierung von Gruppen fördern. Es besteht daher eine direkte Beziehung zwischen der Verfügbarkeit großer Gesundheitsdatensätze und der potenziellen Rentabilität einer Reihe von im Gesundheitsbereich tätigen Branchen, da die Unternehmen ihre geschäftlichen Vorschläge gezielter anbringen und damit einen größeren Gewinn aus der Nutzung personenbezogener Daten erzielen können. **In einem sich selbst verstärkenden Trend werden größere Gewinnaussichten zu einer noch**

[34] danah boyd and Crowford, Kate, *Six Provocations for Big Data*, (2011), p.3. *„Big Data ist ein bemerkenswertes Phänomen, und dies nicht wegen seiner Größe, sondern wegen seiner Rationalität zu anderen Daten. Dank seiner Bemühungen, Daten zu fördern und zu aggregieren ist Big Data grundlegend vernetzt. Sein Wert geht zurück auf die Muster, die aus der Herstellung von Verbindungen zwischen einzelnen Daten über eine Person, über Personen in Bezug auf andere Personen, über Gruppen von Personen oder über die Struktur der Information an sich abgeleitet werden können"*.

[35] So kann beispielsweise ein Gesundheitsdienstleister direkten Zugriff auf Informationen über Verletzungen einer Freizeitsportlerin haben und ihr eine Liste von Ärzten geben, die ihr bei der Rehabilitation helfen können.

größeren Nachfrage nach Daten und einem noch größeren Bedarf an wirksamen Garantien gegen Missbrauch führen.

30. Eine der wirksamsten Garantien in diesem Zusammenhang besteht darin, Nutzer auf die Zweckbestimmungen der Verarbeitung ihrer personenbezogenen Daten hinzuweisen (*Zweckbindung*). Es ist zwar obligatorisch, die Zwecke anzugeben, zu denen Gesundheitsdaten verarbeitet werden, doch neigen Betreiber von mHealth-Lösungen dazu, sich der Verfolgung und der Begrenzung solcher Zweckbestimmungen zu widersetzen. Grund hierfür ist die rasche Entwicklung der Marktdynamik, mit der Unternehmen in Richtung von Möglichkeiten gelenkt werden, an die sie zuvor noch gar nicht gedacht hatten.

31. Die umfassende Verfügbarkeit von Daten und die Möglichkeit, diese für kommerzielle und wissenschaftliche Zwecke auf höchst unterschiedliche Arten zu verarbeiten, wird Datenduplikation und -maximierung begünstigen, die im Widerspruch zu dem in Artikel 6 der Richtlinie verankerten Grundsatz der Datenminimierung stehen. Vor diesem Hintergrund sind Zweckbindung und Datenminimierung nicht voneinander zu trennen. Je größer der Spielraum bei den Zweckbestimmungen der Verarbeitung ist, desto schwieriger ist es, die Datenmenge auf das erforderliche Minimum zu beschränken (das ungebremste Wachstum von Apps für mobile Geräte wird die Tendenz zur Datenmaximierung ebenfalls verstärken)[36].

32. Auch die Wechselwirkung zwischen dem Internet der Dinge[37] und Big Data in mHealth kann im Hinblick auf das massive Vordringen intelligenter Endgeräte und Apps im Bereich mHealth zu großen Risiken beim Datenschutz führen. Von besonderer Relevanz für mHealth sind *tragbare Rechengeräte* (*wearable computing devices*) mit einer Vielzahl von miteinander verbundenen Sensoren, die Informationen über Körperfunktionen und Lifestyle aufzeichnen können. Die Qualität der von solchen Geräten und Sensoren generierten Daten kann sich zwischen reinen Rohdaten und verfeinerten Datenkombinationen und Rückschlüssen bezüglich der betroffenen Person bewegen und Aufschluss über spezifische Aspekte der Gewohnheiten, Verhaltensweisen und Präferenzen einer Person geben[38] und auf diese Weise die Vorstellung der Person als einem *quantifizierten Ich* (also einer digitalen Projektion der Person) verstärken.

33. Das folgende Beispiel veranschaulicht, was unter Datenminimierung zu verstehen ist: Wenn Entwickler für mobile Endgeräte eine App zur Bekämpfung von Fettleibigkeit entwerfen, sollten sie dafür sorgen, dass nur die für diesen Zweck erforderlichen personenbezogenen Daten erhoben werden. Sie könnte in diesem Zusammenhang zwar mitunter das Erfassen von Kalorien erleichtern (indem sie z. B. den Nutzern ermöglicht, den Strichcode auf von ihnen gekauften Lebensmitteln zu scannen), doch würde eine

[36] Über Apps erhobene personenbezogene Daten können später an nicht bekannte Dritte für vage definierte Zwecke wie „Marktforschung“ weitergegeben werden. Neuere Untersuchungen zeigen, dass riesige Mengen personenbezogener Daten mit Hilfe von Smartphones ohne irgendeine sinnvolle Verknüpfung mit der augenscheinlichen Funktion der App erhoben werden. Siehe Wall Street Journal, *Your Apps Are Watching You*, http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html.

[37] Stellungnahme der Artikel 29-Datenschutzgruppe zum Internet der Dinge („Stellungnahme 8/2014 über die neuesten Entwicklungen beim Internet der Dinge“). *„Das Konzept „Internet der Dinge“ bezeichnet eine Infrastruktur, in der Billionen von Sensoren, die in verbreiteten Geräten des Alltags eingebettet sind – in Dingen oder Dingen, die mit anderen Objekten oder Personen verbunden sind –, Daten erfassen, verarbeiten, speichern und übermitteln und, da sie mit eindeutigen Kennungen verknüpft sind, mit anderen Geräten oder Systemen durch Nutzung von Netzwerkfähigkeiten interagieren.“*

[38] Artikel 29-Datenschutzgruppe, Stellungnahme zum Internet der Dinge, S. 8.

weitere Nutzung der Informationen über die von den Nutzern präferierten Marken durch den Betreiber über den ursprünglichen Zweck der App hinausgehen und somit übertrieben sein.

34. **Die weit reichende Erfassung sensibler Gesundheitsdaten wird darüber hinaus der Profilerstellung und einer möglichen Negativauswahl Tür und Tor öffnen, beispielsweise in den Bereichen Beschäftigung und Versicherung.**

35. Zum Thema Profilerstellung sei angemerkt, dass Anbieter von Gesundheitsdiensten in den letzten Jahren Big Data (einschließlich der Erfassung genetischer Daten) und Algorithmen verwendet haben, um die so genannte „prädiktive Medizin“ zu entwickeln, eine Fachrichtung, die sich die Prävention künftiger Gesundheitsrisiken aufgrund der derzeitigen Lebensweise (wie sie aus Daten hervorgeht) zum Ziel gesetzt hat. Versicherungsgesellschaften könnten sich dem Trend anschließen und Programme zur Förderung der Verwendung von Überwachungsgeräten und genetischer Screenings auflegen[39].

36. Bezüglich der Negativauswahl besteht die Sorge, dass in dem Fall, dass alle Versicherungen und privaten Anbieter von Gesundheitsleistungen standardmäßig personenbezogene Gesundheitsdaten gründlich beobachten, um ihre kommerziellen Angebote auf den einzelnen Kunden zuschneiden zu können, sie möglicherweise automatisch die Betreuung derjenigen ablehnen, die einer Offenlegung oder Weitergabe von Daten widersprechen, und dies unabhängig von ihrem Gesundheitszustand oder ihren Risikofaktoren. Die Weitergabe von Daten wird also automatisch zur Folge haben, dass Menschen diskriminiert werden, die ihre Gesundheitsdaten lieber nicht offenlegen oder weitergeben.

37. Ausgeglichen werden können durch Big Data verursachte mögliche Verzerrungen – vor allem Datenmaximierung und Profiling – zumindest teilweise durch die korrekte Anwendung des Rechts der Nutzer auf Widerspruch[40], wie weiter unten in Abschnitt III dargelegt.

II.5 Gestaltung von mHealth-Apps: wesentliche Merkmale

Pflichten im Bereich Datensicherheit

38. Wie bereits erwähnt, wird das fehlende Vertrauen in mHealth Nutzer von der Inanspruchnahme innovativer Lösungen abhalten und die Gesellschaft um die Vorteile von mHealth bringen. **Es ist daher für alle Betreiber von äußerster Wichtigkeit, die Vertraulichkeit, Integrität und Verfügbarkeit der im Einklang mit den Datenschutzvorschriften[41], mit internationalen Standards und bewährten**

[39] Zum Profiling siehe auch Europarat, Empfehlung CM/Rec(2010)13 über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten im Zusammenhang mit Profiling, angenommen am 23. November 2010, abrufbar unter https://wcd.coe.int/ViewDoc.jsp?id=1710949.

[40] Dieses Recht ist in Artikel 14 der Richtlinie geregelt und ist im Zeitalter des Internets und im Bereich mHealth von besonderer Bedeutung. Die Richtlinie verlangt ferner, dass Daten auf dem neuesten Stand zu halten sind (Artikel 6), und sie räumt der betroffenen Person die Möglichkeit ein, der Verarbeitung von Daten zu widersprechen, die ihrer Auffassung nach unrichtig sind, oder die Daten sperren zu lassen (Artikel 12). Der Gesundheitszustand ändert sich im Zeitverlauf, und Personen sollten nicht mit überholten Daten verknüpft werden.

[41] Wie Artikel 17 der Richtlinie, der ein Informationsrisikomanagement für Datenverarbeitungen vorsieht.

Vorgehensweisen[42] verarbeiteten personenbezogenen Daten zu gewährleisten. Von allen denkbaren Optionen für Informationssicherheit dürfte ein kontinuierliches Risikomanagement das Kernelement aller Aktivitäten im Bereich Sicherheit sein.

39. Auch wenn am häufigsten das Erfordernis der Vertraulichkeit personenbezogener Daten genannt wird, spielen andere Sicherheitsbestandteile – Integrität und Verfügbarkeit – im Hinblick auf Gesundheitsdaten ebenfalls eine wichtige Rolle.

40. Der Mangel an geeigneten (*die Privatsphäre wahrenden*) Tools und Praktiken ist für alle an der Entwicklung von mHealth-Geräten und -Apps Beteiligten (z. B. App-Entwickler und Gerätehersteller) ein Problem. In einem sich rasch entwickelnden technologischen Umfeld müssen Entwickler ihre Produkte schnell liefern, damit sie nicht von Wettbewerbern überholt werden. Daher verwenden sie möglicherweise häufig erneut bereits bestehende Komponenten, und dies trotz bekannter Schwachstellen bezüglich des Datenschutzes. Dazu mögen leider nur wenige Bausteine für datenschutzfreundliche Anwendungen und Dienste gehören, was oft geringe Sicherheit bedeutet. **In einem solchen Zusammenhang müssen zur Lösung des Problems die Grundsätze des *Datenschutzes durch datenschutzfreundliche Voreinstellungen* und des *Datenschutzes durch Technik* in Kombination mit systematischen Bemühungen und Privacy Engineering angewandt werden. Das Internet Privacy Engineering Network (IPEN[43]) bietet einen Rahmen, in dem diese Fragen in Zusammenarbeit zwischen Ingenieuren und Experten für rechtliche und regulatorische Fragen behandelt werden können.**

Datenübermittlung ins Ausland

41. **Da Geräte und Apps weltweit von Gesundheits- und IT-Unternehmen mit Sitz außerhalb der Europäischen Union vertrieben werden, kann die Datenverarbeitung häufig jenseits der Grenzen der Union stattfinden.** Das wohl relevanteste (und typische) Szenario bei mHealth dürfte so aussehen, dass die Daten in einem globalen Cloud-Umfeld verarbeitet werden, wobei die Daten an Drittländer ohne Wissen des Nutzers und ohne Kontrollmöglichkeit für ihn übermittelt werden, häufig unter der Verantwortung eines für die Verarbeitung Verantwortlichen, der seinen Sitz außerhalb der EU und außerhalb von Ländern hat, für die es eine Angemessenheitsentscheidung der Kommission gibt.

42. Eine deutsche Versicherung, die Daten über ihr Kundenrisiko in der EU erhebt, kann beispielsweise diese Daten später an ein anderes Versicherungsunternehmen in Kanada weitergeben, und dies im Einklang mit Artikel 25 der Richtlinie, weil in einer Entscheidung der Kommission[44] Kanada als ein Land anerkannt wurde, das ein

[42] Artikel 29-Datenschutzgruppe, *cit.*, S. 14. Im Hinblick auf die zu ergreifenden Vorkehrungen können sich App-Entwickler auf öffentliche Sicherheitsleitlinien stützen, wie die „Smartphone Secure Development Guidelines“ der ENISA, abrufbar unter http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines/at_download/fullReport.

[43] Im Internet Privacy Engineering Network (IPEN) haben sich Entwickler und Datenschutzexperten von Regulierungsbehörden, Unternehmen, Zivilgesellschaft und Wissenschaft zusammengetan und arbeiten gemeinsam an die Privatsphäre respektierenden Lösungen für praktische Probleme (https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/IPEN). Wir werden IPEN ersuchen, mHealth zu testen und der Frage nachzugehen, welche bewährten Vorgehensweisen von seinen Ingenieuren und Experten ins Leben gerufen/bewertet/empfohlen werden können.

[44] Entscheidung 2002/2/EG der Kommission vom 20. Dezember 2001 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzes, den der kanadische

angemessenes Datenschutzniveau bietet[45]. In anderen Fällen hingegen dürfen Datenübermittlungen nur vorbehaltlich der in Artikel 25 und 26 der Richtlinie vorgesehenen Kriterien und Garantien erfolgen[46].

III. MÖGLICHKEITEN FÜR DIE INTEGRATION VON DATENSCHUTZANFORDERUNGEN IN DIE ENTWICKLUNG VON mHEALTH-APPS

III.1 Rechtsrahmen

43. Wie bereits ausgeführt, handelt es sich bei vielen der im Zusammenhang mit mHealth auf intelligenten mobilen Endgeräten verfügbaren Datenarten um personenbezogene Daten, die daher im Einklang mit den Datenschutzvorschriften verarbeitet werden müssen.

44. Darüber hinaus geben Gesundheitsdaten Auskunft über sehr persönliche Aspekte einer Person und können auch ein erhebliches Eindringen in ihre Privatsphäre bedeuten. Hier muss also das Recht auf Privatsphäre garantiert werden, indem übermäßig in die Privatsphäre eindringende Maßnahmen durch alternative, eingeschränkte Optionen ersetzt werden, die dem gleichen Zweck dienen.

Anwendung derzeit geltender Vorschriften auf den mHealth-Kontext

45. Die für die Verarbeitung durch Apps auf mobilen Geräten Verantwortlichen sowie die App-Designer müssen bei der Gestaltung ihrer Apps für mHealth die Datenschutzvorschriften beachten und insbesondere der Schutzwürdigkeit von Gesundheitsdaten Rechnung tragen.

46. **Von entscheidender Bedeutung ist vor allem, dass sich für die Verarbeitung Verantwortliche und Auftragsverarbeiter um mehr Transparenz bezüglich der Art und Weise, in der sie personenbezogene Daten verarbeiten, weitergeben und wiederverwenden, sowie bezüglich der Zwecke, die sie damit verfolgen, bemühen.** Die Tatsache, dass sich hinter der Verarbeitung personenbezogener Gesundheitsdaten eine breite Palette kommerzieller Zwecke verbirgt, befreit die für die Verarbeitung Verantwortlichen nicht von ihrer Verpflichtung zur umfassenden Information der Nutzer; ganz im Gegenteil: Es sollte ausreichende Aufklärung erfolgen, damit die Nutzer ausdrücklich in die Verarbeitung ihrer Gesundheitsdaten einwilligen können. Die Freiheit

---

Personal Information Protection and Electronic Documents Act bietet (notifiziert unter Dokumentennummer V(2001) 4539).

[45] In solchen Fällen würde der Begriff „Übermittlung" daher sowohl „beabsichtigte Übermittlungen" als auch den „zugelassenen Zugriff" auf die Daten durch den/die Empfänger abdecken. Rechtswidriger Zugriff und Hacking wären ausgeschlossen.

[46] Siehe Artikel 29-Datenschutzgruppe, Stellungnahme 3/2009 (WP 161) über den Entwurf einer Entscheidung der Kommission zu Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG (vom für die Verarbeitung Verantwortlichen zum Datenverarbeiter) und Häufig gestellte Fragen zu bestimmten Aspekten im Zusammenhang mit dem Inkrafttreten des Beschlusses 2010/87/EU der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EC (WP 176) vom 12. Juli 2010 sowie Stellungnahmen der Artikel 29-Datenschutzgruppe zu verbindlichen unternehmensinternen Datenschutzregelungen (BCR) und das Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995 (WP 114), abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

der Nutzer, in der Frage der Verarbeitung ihrer Gesundheitsdaten eine Wahl zu treffen und zu entscheiden, darf als Folge des Designs der App nicht eingeschränkt werden.

47. **Hier gehört die Möglichkeit für betroffene Personen, über eine lokale Einschränkung der Verarbeitung von mHealth-Daten – auf ihren intelligenten Endgeräten, weniger auf einem Remote-Server – zu entscheiden, zu den wichtigen Garantien, die bei mHealth-Apps und -Geräten umgesetzt werden sollten. Auch die Option für Personen, der Weitergabe/Übermittlung der personenbezogenen Daten durch den für die Verarbeitung Verantwortlichen an einen Dritten ohne Zwang zuzustimmen oder auch nicht, gehört zu den wichtigen Merkmalen, die alle mHealth-Apps und -Geräte aufweisen sollten. Alle diese Optionen sollten intelligent und auch von nicht fachkundigen Nutzern einfach und auf der Grundlage eines klaren und leicht verständlichen Datenschutzhinweises anzuwenden sein.**

48. **Designer und Hersteller sollten die Kreativität und Dynamik, die sie normalerweise bei der Einführung attraktiver Geräte und Apps an den Tag legen, in gleichem Maße auch darauf verwenden, den Nutzers wirksame und benutzerfreundliche Datenschutzhinweise und Einstellungsoptionen an die Hand zu geben. Im Ergebnis sollten Personen in der Lage sein, für ihre Privatsphäre und den Schutz ihrer Daten relevante Optionen in dem Bewusstsein einzustellen, dass dies eine für die Nutzung der Geräte und Apps wichtige Handlung ist und keine langweilige Formsache oder ein unnötiger Aufwand.**

49. Um den Nutzern die Kontrolle über ihre eigenen Daten zu erleichtern – wie dies mitunter mit Software auf PCs geschieht –, sollten die Nutzer bei der Aktivierung eines mHealth-Geräts oder einer entsprechenden App einfach darüber entscheiden können, ob sie ihre eigenen Datenschutzeinstellungen vornehmen oder eher die Standardeinstellungen übernehmen/ändern möchten, die einem höheren Standard für den Schutz von Privatsphäre und Daten entsprechen sollten (Anwendung von *Datenschutz durch datenschutzfreundliche Voreinstellungen*). App-Entwickler sollten die Datenschutzoptionen in der App nach Vorbildern in allgemein akzeptierten Datenschutzleitlinien (z. B. denen der ENISA[47]) gestalten.

50. Es sei darauf hingewiesen, dass in einigen Fällen die Verarbeitung personenbezogener Daten durch Apps auf mobilen Geräten auch durch private Nutzer erfolgt, die dann gemeinsam als für die Verarbeitung Verantwortliche für die von ihnen verarbeiteten Daten verantwortlich sind. Eine solche Verarbeitung fällt dann nicht unter die so genannte *Ausnahmeregelung für Privathaushalte*[48], wenn der Nutzer der App beispielsweise in größerem Umfang personenbezogene Daten im Internet verbreiten möchte (über ein soziales Netzwerk oder eine Mailing-Liste). Die Ausnahmeregelung für Privathaushalte sollte darüber hinaus auch insofern nur begrenzt angewandt werden[49], als – unabhängig davon, ob der Nutzer die Kriterien der Regelung erfüllt – die am Design, dem Angebot und der Funktionsweise der App beteiligten Organisationen (App-Designer, App-Store und Dritte) nach wie vor für die in Verfolgung ihrer eigenen Ziele vorgenommene Verarbeitung verantwortlich sind.

[47] Siehe weiter oben Fußnote 42.
[48] Artikel 3 Absatz 2 der Richtlinie.
[49] Rechtssache C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů*, Urteil des EuGH vom 11. Dezember 2014, Randnr. 29ff.

51. Da zu mHealth auch die Verarbeitung von Daten durch intelligente Endgeräte gehört, sollte darauf hingewiesen werden, dass eine gültige, in Kenntnis der Sachlage gegebene Einwilligung der betroffenen Person eine Bedingung für die Speicherung von oder den Zugriff auf Informationen ist, die auf dem Endgerät des Abonnenten oder Nutzers gespeichert sind[50].

Die Datenschutz-Grundverordnung: die Modernisierung des Datenschutzrahmens

52. Die Datenschutz-Grundverordnung, die sich derzeit noch im Vorschlagsstadium befindet, in der Diskussion jedoch schon recht weit fortgeschritten ist, wird erhebliche Änderungen im Online-Datenschutz mit sich bringen und auch Auswirkungen auf die Gesundheitsfürsorge haben.

53. **Generelles Ziel der Datenschutz-Grundverordnung ist die Stärkung der Rechte der betroffenen Person, insbesondere in Situationen, in denen ein Eingriff in ihr Recht auf Privatsphäre durch Online-Aktivitäten noch verstärkt wird[51]. Darüber hinaus führt die Datenschutz-Grundverordnung neue Leitgrundsätze und Vorschriften im Zusammenhang mit mHealth ein[52].** So werden mit der Datenschutz-Grundverordnung beispielsweise Datenschutz durch Technik und Datenschutz durch datenschutzfreundliche Voreinstellungen rechtliche Verpflichtungen (und sind nicht länger nur „vorbildliche Vorgehensweisen“)[53] und müssen daher bei der Konzeption neuer mHealth-Apps oder -Geräte in vollem Umfang berücksichtigt werden.

54. Im Hinblick auf die Wechselwirkung zwischen EU-Recht und einzelstaatlichem Recht lässt die Datenschutz-Grundverordnung offensichtlich dem nationalen Gesetzgeber viel Spielraum[54]. Sobald der Bereich der Gesundheitsfürsorge von der Nutzung dieses Spielraums betroffen ist, sind wir der Auffassung, dass **die Annahme einzelstaatlicher Rechtsvorschriften die kohärente Anwendung des EU-Datenschutzrechts nicht beeinträchtigen sollte, indem dadurch neue Abweichungen geschaffen statt bestehende beseitigt werden**.

III.2 Zusätzliche Maßnahmen zur Stärkung der Datenschutzgarantien in mHealth

Förderung der Rechenschaftspflicht

55. Ein systematisches Herangehen an die Herausforderungen von mHealth erfordert eine korrekte Identifizierung des/der für die Verarbeitung Verantwortlichen und eine effiziente

[50] Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation (Nr. 2002/58/EG), anwendbar auf alle Stellen, die Informationen auf intelligenten Endgeräten speichern oder aus ihnen auslesen, unabhängig von der Art (öffentlich oder privat, Person oder Unternehmen, für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter oder Dritter) einer solchen Stelle. Siehe ferner Artikel 29-Datenschutzgruppe, *cit.*, S. 7.
[51] Als Beispiele seien die Artikel 11, 12 und 14 genannt.
[52] Insbesondere: Artikel 4 Absatz 12 mit einer Definition des Begriffs „Gesundheitsdaten“; Artikel 20 über Profiling (einschließlich Gesundheitsprofiling und „prädiktives“ Profiling); Artikel 33 zur Datenschutzfolgenabschätzung (einschließlich Abschätzung konkreter Risiken bei Verarbeitungen wie der Verarbeitung von Gesundheitsdaten) und Artikel 81 zu Garantien bei der Verarbeitung von Gesundheitsdaten.
[53] Artikel 23 „Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen“.
[54] Stellungnahme des EDSB zum Datenschutzreformpaket, Punkt 50ff.

Organisation der Verantwortlichkeiten für den Fall, dass mehrere Marktteilnehmer an der Datenverarbeitung beteiligt sind[55] [56].

56. Wir haben hierzu bereits dargelegt, wie aufgrund der Marktdynamik ständig neue Geschäftsmodelle entstehen, an denen gelegentlich neue Unternehmen und Betreiber beteiligt sind. Um zu verhindern, dass das schnelle Wachstum eines gegliederten Marktumfelds ins Chaos mündet, sollte die Verantwortung für alle Datenverarbeitungen kohärent und systematisch zugeteilt werden. Wer auch immer ein Interesse an personenbezogenen Daten hat oder mit ihnen ein Ziel verfolgt und daher Daten verarbeitet, soll den Nutzern gegenüber, deren Daten er verarbeitet, Rechenschaft ablegen.

Gewährleistung der korrekten Anwendung der Datenschutzvorschriften

57. mHealth ist zwar ein weitgehend neues Phänomen, doch enthalten sowohl die Richtlinie als auch die Datenschutzrichtlinie für elektronische Kommunikation Bestimmungen, die durchaus in der Lage sind, die Rechte von Nutzern zu schützen. Es ist daher – von politischen Entscheidungsträgern, für die Verarbeitung Verantwortlichen und Datenschutzbehörden – dafür Sorge zu tragen, dass die Datenschutzvorschriften proaktiv und verantwortungsvoll umgesetzt werden.

58. Wie von der Artikel 29-Datenschutzgruppe betont, sind Zweckbindung und Datenminimierung eng miteinander verknüpft[57]. Beide tragen dazu bei, dass personenbezogene Daten nicht auf unrechtmäßige Weise wiederverwendet werden. Da die derzeitige Entwicklung der Wirtschaftslandschaft auf Wiederverwendung von Daten und eine intensive Nutzung von Daten für mehrere (mitunter sogar unvorhergesehene) Zwecke hinausläuft, ist es von entscheidender Bedeutung, dass der Zweck der Verarbeitung für die Nutzer klar erkennbar ist und dass für die Verarbeitung Verantwortliche angemessene Schutzvorkehrungen treffen, so dass die Weitergabe und Verarbeitung von Daten auf das unbedingt erforderliche Maß beschränkt bleiben.

59. Es liegt auf der Hand, dass den zuständigen Datenschutzbehörden der EU und der Mitgliedstaaten eine Hauptrolle bei der Überwachung der Anwendung dieser Vorschriften und gegebenenfalls bei Eingriffen zukommt. Aufgrund der globalen Dimension der Verarbeitung ist ferner eine engere Zusammenarbeit zwischen den Datenschutzbehörden weltweit im Rahmen einer kohärenten Strategie unbedingt erforderlich.

Förderung einer kohärenten Anwendung von Datenschutzvorschriften im Bereich mHealth

60. Angemessene Aufmerksamkeit sollten der EU-Gesetzgeber und die Akteure im Bereich mHealth auch Leitlinien mit Standards für die Verarbeitung von Gesundheitsdaten

[55] Siehe Artikel 29-Datenschutzgruppe, Stellungnahme 1/2010 vom 16. Februar 2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ (WP 169), abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf.

[56] Stellungnahme des EDSB zum *Elektronische Gesundheitsdienste Aktionsplan 2012-2020*, Punkt 19. An dieser Stelle halten wir fest, dass die Datenschutz-Grundverordnung konkretere Vorschriften bezüglich der Rechenschaftspflicht enthält, damit Verantwortung effizient zugeteilt und die richtige(n) Stelle(n) rechenschaftspflichtig gemacht wird/werden.

[57] Artikel 29-Datenschutzgruppe, Stellungnahme zu Apps auf intelligenten Endgeräten, S. 17.

widmen, wie dem Arbeitspapier der Artikel 29-Datenschutzgruppe zur Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA)[58] und der Empfehlung des Europarates über den Schutz medizinischer Daten[59]. Auch ein von Akteuren im Bereich mHealth mit Unterstützung durch Datenschutzbehörden erarbeiteter Verhaltenskodex könnte auf eine kohärente Anwendung bestehender Datenschutzvorschriften im Bereich mHealth hinwirken.

Aufgeklärte Mitwirkung Betroffener

61. Eines der Ziele der Entwicklung von mHealth besteht darin, die aufgeklärte Mitwirkung der Patienten zu verstärken, damit diese mehr individuelle Kontrolle über ihre Gesundheitsversorgung haben.

62. Wir sind der Auffassung, dass eine verbesserte aufgeklärte Mitwirkung auch beim Datenschutz erreicht werden sollte, indem den Nutzern größere Kontrolle über ihre Daten eingeräumt wird. App-Entwickler und App-Stores sollten für mehr Transparenz für die Betroffenen sorgen. Die Nutzer sollten besser über die Verarbeitung ihrer Daten informiert werden und die Möglichkeit erhalten, rechtzeitig und wirksam ihre Einwilligung zu geben/zu widerrufen oder sich gegebenenfalls gegen die Verarbeitung zu entscheiden. Ein sehr wirksamer Weg, den Nutzern mehr Kontrolle zu ermöglichen, ist die Möglichkeit, ihre eigenen personenbezogenen Daten nur vor Ort und ohne Übermittlung an einen Betreiber zu verarbeiten.

63. Angesichts einer immer komplexeren Landschaft sprechen wir uns ferner für Datenübertragbarkeit (und Interoperabilität von Formaten und Technologien) als Lösung in Richtung Vereinfachung, Transparenz und Kontrolle durch Nutzer und gegen Datenduplikation aus.

Sicherung personenbezogener Daten und Verbesserung der Engineering-Anforderungen

64. Der Gesetzgeber sollte verlangen, dass alle Akteure die Vertraulichkeit, Integrität und Verfügbarkeit der im Einklang mit den Datenschutzvorschriften, mit internationalen Standards und bewährten Vorgehensweisen verarbeiteten personenbezogenen Daten gewährleisten. Von allen denkbaren Optionen für Informationssicherheit dürfte ein kontinuierliches Risikomanagement das Kernelement aller Aktivitäten im Bereich Sicherheit sein.

65. *Datenschutz durch datenschutzfreundliche Voreinstellungen* und *Datenschutz durch Technik* müssen in Kombination mit systematischen Bemühungen in Richtung Datenschutz-Engineering im gesamten mHealth-Ökosystem angewandt werden. Der Gesetzgeber sollte die Annahme von Tools für innovative datenschutzfreundliche Apps und Dienste fördern (Bibliotheken, Design-Muster, Snippets, Algorithmen, Methoden und Praktiken).

Garantien für die Verwendung von Big Data in mHealth

66. Big Data birgt zwar das Potenzial von Verbesserungen sowohl in der öffentlichen wie der privaten Gesundheitsfürsorge, doch kann es auch Datenschutzrechte einschränken, insbesondere durch übermäßiges Data Mining und Profiling. Der Gesetzgeber muss daher

[58] Artikel 29-Datenschutzgruppe, Arbeitspapier vom 15. Februar 2007, Nr. 00323/07/DE.
[59] Empfehlung Nr. R (97) 5 vom 13. Februar 1997.

Vorschriften erlassen, denen zufolge Data Mining im Zusammenhang mit mHealth nur unter bestimmten Umständen und unter der Voraussetzung akzeptabel ist, dass die Datenschutzvorschriften vollumfänglich angewandt werden.

67. In Anbetracht der Tatsache, dass eine wirksame Anonymisierung nur sehr schwer zu erreichen ist, und dass pseudonyme Daten noch immer personenbezogene Daten sind, muss jede Verarbeitung größerer Datenmengen zu Analysezwecken strengen Datenschutzgarantien unterliegen. Ferner ist ganz klar anzugeben, welche Personen zum Zugriff auf diese Daten befugt sind, und welche Modalitäten für einen solchen Zugriff gelten.

68. Die Kombination von Daten zum Zweck der Profilerstellung kann zwar in manchen Fällen und bei korrekter Anwendung (z. B. personalisierte Medizin) für den Einzelnen höchst vorteilhaft sein, doch kann sie auch erhebliche Datenschutzbedenken hervorrufen, vor allem, wenn sie dazu führt, dass andere Arten von Entscheidungen getroffen werden, die Personen berühren können (wenn z. B. eine Versicherung beschließt, eine Person nicht zu versichern, wenn sie Zugriff auf das Gesundheitsprofil der Person hat, das ihrer Auffassung nach mit einem hohen Krebserkrankungsrisiko behaftet ist)[60]. Daher sollte Profiling, wenn es insbesondere nicht nur zu Forschungszwecken und mit strenger funktionaler Trennung vorgenommen wird, sondern auch mit dem Ziel, die betreffenden Personen herauszusuchen und anders zu behandeln, nur unter ganz bestimmten Umständen mit einer ad hoc-Rechtsgrundlage und/oder mit der ausdrücklichen Einwilligung der betroffenen Person und unter der Voraussetzung erfolgen, dass strenge Datenschutzauflagen erfüllt werden (wie z. B. in Artikel 15 der Richtlinie und in Artikel 20 der vorgeschlagenen Datenschutz-Grundverordnung niedergelegt). Als zusätzliche Garantie gilt ferner nach wie vor das Recht der betroffenen Person auf Widerspruch gegen die Verarbeitung.

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.

71. Daher bieten Datenschutzgrundsätze und -vorschriften Hilfestellung in einem bisher weitgehend unregulierten Sektor. Die korrekte Einhaltung dieser Grundsätze und

[60] Siehe Artikel 29-Datenschutzgruppe, Stellungnahme zur Zweckbindung vom 2. April 2013, abrufbar unter http://idpc.gov.mt/dbfile.aspx/Opinion3_2013.pdf, *„Insbesondere kann ein Algorithmus eine Korrelation ausmachen und dann einen statistischen Schluss ziehen, der sich, wenn er in Marketing- oder andere Entscheidungen einfließt, als unfair und diskriminierend erweisen kann. Dies kann zur Verfestigung bestehender Vorurteile und Klischees führen und das Problem sozialer Ausgrenzung und Schichtung noch verstärken“.*

Vorschriften erhöht die Rechtssicherheit, steigert das Vertrauen in mHealth und trägt auf diese Weise zur vollen Entfaltung dieses Bereichs bei.

Brüssel, 21. Mai 2015

(gezeichnet)

Giovanni BUTTARELLI
Europäischer Datenschutzbeauftragter