Zeitschrift für Datenrecht und Informationssicherheit

digma

www.digma.info 16. Jahrgang, Heft 2, Juni 2016

Schwerpunkt:

Quantified Self

fokus: Selbstvermessung oder Selbstüberwachung?
fokus: Lifestyle- oder Medizinalprodukt?
report: Erinnern und Vergessen im digitalen Zeitalter

Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth
David Vasella

Schulthess §

inhalt

fokus

Schwerpunkt:
Quantified Self

auftakt

Selbstvermessung oder Selbstüberwachung?

Die Gefahr von Quantified-Self-Diensten liegt in der Komplexität und Intransparenz der QS-Wertschöpfungskette und in der Sensitivität der aus den Grunddaten ableitbaren persönlichen Details. Was droht uns aus dem Trend zur Selbstoptimierung?

Das vermessene Selbst

Sensortechnologien, GPS-gestützte Lokalisierungen, intelligente Messverfahren und automatische Identifikationsverfahren bringen neue Praktiken der digitalen Selbstvermessung hervor und konfrontieren uns mit neuen Formen gesellschaftlichen Steuerungs- und Kontrollwissens.

Lifestyle- oder Medizinprodukt?

Webbasierte und mobile Fitness-, Wellness- und Lifestyle-Dienste zur digitalen Vermessung des eigenen Körpers kommen mit der gesundheits- und heilmittelrechtlichen Regulierung in Berührung, wenn sie für medizinische Zwecke angepriesen oder eingesetzt werden. Was heisst das für die Anbieter?

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Prof. Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. (em.) Dr. iur. Rainer J. Schweizer, Prof. Dr. Günter Karjoth, Dr. iur. David Vasella

Redaktion: Dr. iur. Bruno Baeriswyl und Prof. Dr. iur. Beat Rudin

Rubrikenredaktorin: Dr. iur. Barbara Widmer

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Inland: CHF 168.00, Jahresabo Ausland: CHF 195.00, Einzelheft: CHF 44.00
PrintPlus: Jahresabo Inland: CHF 189.00, Jahresabo Ausland CHF 216.00

PrintPlus: Das PrintPlu§-Abonnement bietet die Möglichkeit, bequem und zeitgleich zur Printausgabe jeweils das PDF der ganzen Ausgabe herunterzuladen. Detaillierte Informationen finden Sie unter www.schulthess.com/printplus.

Anzeigenmarketing: Zürichsee Werbe AG, Herr Pietro Stuck, Seestrasse 86, 8712 Stäfa
Tel. +41 (0)44 928 56 11, pietro.stuck@zs-werbeag.ch

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich
Tel. +41 (0)44 200 29 29, Fax +41 (0)44 200 29 28, www.schulthess.com, zs.verlag@schulthess.com

Whistleblowing-Systeme im Konzern

«Whistleblowing» war das Schwerpunktthema in digma 2016.1. Dieser Beitrag fokussiert sich nun auf besondere Fragen im internationalen Konzern. Die stellen sich insbesondere bei grenzüberschreitenden Bekanntgaben. Was muss ein internationaler Konzern beachten, wenn er ein Whistleblowing-System einrichtet?

Erinnern und Vergessen im digitalen Zeitalter

Das Urteil des Europäischen Gerichtshofs zum sog. Recht auf Vergessenwerden vom 13. Mai 2014 stärkt den Nutzer in der Durchsetzung dieser Rechte gegenüber den Suchmaschinenbetreibern und begründet einen Anspruch auf Löschung der Links. Wie ist das Urteil umzusetzen?

Datenaufbewahrung und -verwendung

Im Kontext der Datenaufbewahrung und -verwendung steht in der Rechtsprechung des EGMR die Auslegung des Verhältnismässigkeits- und Zweckbindungsprinzips im Vordergrund. Unter welchen Voraussetzungen lässt sich ein Datensammeln im öffentlichen und im privaten Bereich rechtfertigen?

Quantified Self

Quantified-Self-Anwendungen zeigen uns, wie fit wir sind. Und wenn wir krank sind?

report

forum

Daten aus Selbstvermessung

Eine Analyse der datenschutzrechtlichen Rahmenbedingungen von Quantified Self in der Schweiz

Clara-Ann Gordon, Rechtsanwältin, LL.M., Partner, Pestalozzi Rechtsanwälte AG, Zürich clara-ann.gordon@pestalozzilaw.com

Für Quantified Self gelten die herkömmlichen Datenschutz- und Informationssicherheitsnormen. Was bedeutet das für Hersteller und Anbieter?

«Quantified Self» wurde in San Francisco gegründet und basiert auf der Idee, dass man mit den Daten, die man selbst oder andere über einen sammeln, ein statistisches Bild des Gesundheits- und Leistungszustands machen kann. In Meetups und grossen Konferenzen teilen die Anhänger dieser Bewegung Erkenntnisse aus ihren Statistiken, Erfahrungen mit Geräten und Software und geben der rasch wachsenden Zahl an Herstellern Inputs für neue Erfassungsmethoden[1].

Gesundheits-Apps

Es ist zwischen Gesundheits-Apps, die keiner Regulierung unterliegen, und Medical Apps, die unter das Medizinproduktegesetz fallen, zu unterscheiden. Gesundheits-Apps vermessen die körperliche Fitness, geben Tipps zur gesunden Lebensführung, informieren über Krankheiten oder machen andere Angebote für körperliches, seelisches und soziales Wohlbefinden. Medical Apps hingegen verbinden medizinisches Wissen und individuelle Patientendaten und werden direkt zum Erkennen und Behandeln von Krankheiten eingesetzt[2]. Im Folgenden wird der Begriff «Apps» in erster Linie für Gesundheits-Apps verwendet, die keiner Regulation im Gesundheitsbereich unterliegen, sowie für Apps betreffend Aktivitäten im Sport- und Lifestylebereich.

Wearables – Kleinstcomputer befestigt am menschlichen Körper

Der Trend zur Selbstvermessung des eigenen Körpers mittels Sensoren dient dem Erkenntnisgewinn zu persönlichen, sportlichen, gesundheitlichen und gewohnheitsspezifischen Fragestellungen[3]. Wearables sind Kleinstcomputer, die am Körper des Menschen befestigt werden. Sie sind eingenäht in Kleidern, eingebaut in Uhren oder Armbändern, in Brillen usw.[4]. Es gibt hier diverse Untergruppen wie Smartwatches, Fitnesstrackers, Wrist Sport Computers oder HF-Geräte (Health und Fitness Trackers). Gemäss einer Studie von Garnter wird der Verkauf von Wearables im Jahre 2016 weltweit um 18,4% zunehmen und auf 274,59 Millionen Geräte ansteigen[5]. Unabhängig vom benutzten Gerät handelt es sich bei der Selbstvermessung zu Gesundheitszwecken um einen ernst zu nehmenden Trend. Davon zeugen auch die über 100 000 Apps, die bei iTunes und Google Play zum Download angeboten werden[6]. Das Einsatzgebiet der Wearables in der Schweiz ist primär im Bereich Lifestyle und Sport anzusiedeln. Wearables und damit einhergehende neue Angebote diverser Dienstleister sind nicht nur aus technischer Sicht interessant, sondern es stellen sich in diesem Zusammenhang auch neue rechtliche Fragen[7]. Im Folgenden wird der Begriff «Wearables» allgemein für die verschiedenen Self-Tracking-Geräte verwendet.

Akteure und ihre gesammelten gesundheits- und aktivitätsbezogenen Daten

Die Akteure in der Quantified-Self-Welt sind in erster Linie die Träger der Wearables, die selber die Daten generieren und die Aufschluss über den Gesundheitszustand oder allfällige Krankheiten geben. Die App-Hersteller geben jedoch vor, welche Daten aufgezeichnet und gesammelt werden können. Sie führen diese Daten in der Regel auf einer externen Serverplattform (Cloud) zusammen und bearbeiten diese dort. Daneben haben Unternehmen im Gesundheitsbereich und auch in anderen Wirtschaftszweigen ein grosses Interesse an solchen Daten. Wearables und damit verbundene Apps sammeln diverse Daten, unter anderem auch solche, die sich einer bestimmten Person zuordnen lassen (z.B. Name, E-Mail-Adressen, usw.). Insbesondere Wearables aus dem Fitness- und Gesundheitsbereich sammeln Daten, die gesundheitsbezogen sind, wie Bodymass-

indexe, Schlaf- und Blutzuckerwerte, Herz- und Atemfrequenz, und die Rückschlüsse auf den Gesundheitszustand und allfällige Krankheiten einer Person zulassen. Die Offenlegung dieser Daten könnte der betroffenen Person zum Nachteil werden, sei es bei der Stellensuche oder beim Versicherungsabschluss[8].

Wo fallen die Daten an und wem gehören sie?

Es gibt Apps, die vorsehen, dass die Daten nur lokal auf den Wearables selbst gesammelt werden. Hier findet keine Übermittlung via Bluetooth in eine Cloud statt. Andere Apps bzw. Wearables senden die gesammelten Daten täglich an das Smartphone und damit an einen Server in der Cloud, der sich meistens im Ausland befindet. Im Austausch erhält der Träger eine grafische Auswertung über Qualität und Dauer der körperlichen Aktivitäten oder über seinen Gesundheitszustand[9]. Zudem nutzen Apps alle dem Smartphone zur Verfügung stehenden Kommunikations- und Speichermöglichkeiten wie der Datenexport über E-Mail oder auf einen externen Speicherort (wie Dropbox) sowie die Synchronisierung mit externen Servern. Sie bieten aber auch Benachrichtigungsmöglichkeiten per SMS[10]. Es werden daher Unmengen von Daten gesammelt, weshalb auch im Gesundheitswesen Big Data zu einem grossen Thema und Treiber der Entwicklung geworden ist. Bei der Quantified-Self-Szene geht es, wie bei allen Social Media, ums Teilen. Dasselbe gilt für Gesundheitsforen im Internet, wie beim bekannten Webportal patienslikeme.com, dessen 250 000 Nutzer an chronischen Krankheiten leiden. Man muss nur eine E-Mail-Adresse, Benutzername und Passwort sowie einige persönliche Angaben eintippen, schon ist man dabei[11]. All diese Datensätze haben für die App-Hersteller bzw. Plattformbetreiber einen enormen Wert, da sie diese z.B. an Pharmaunternehmen weiterverkaufen können, welche diese Daten für die Erforschung von neuen Medikamenten verwenden können. Die Betreiber sichern sich daher meistens in den allgemeinen Geschäftsbedingungen alle Rechte an den Daten. Der Nutzer ist nicht mehr Eigentümer seiner eigenen Gesundheitsdaten. Dies ist aus (datenschutz-)rechtlicher Sicht heikel, da der Nutzer damit auch sein Selbstbestimmungsrecht (die digitale Souveränität) über die weitere Verwendung aus sachenrechtlicher Sicht wohl aufgibt. Neben der Frage, ob an solchen Gesundheits- und auch an anderen Daten überhaupt Eigentumsrechte erworben und übertragen werden können, gibt es diverse andere, offene Rechtsfragen, für welche es in der Schweiz heute noch keine gesetzlichen Regelungen oder offiziellen Weisungen gibt. Es gelten auch hier bis auf Weiteres die einschlägigen DSG-Bestimmungen.

Primäre- und sekundäre Nutzung von Daten

Primärnutzung bezeichnet die Generierung von Daten und die damit verbundene Nutzung. Die Primärnutzung von Daten basiert in der Regel auf einem Vertragsverhältnis zwischen zwei Parteien: dem Träger des Wearable und dem App-Provider. Die Primärnutzung ist unbestritten und nicht problematisch, da der Nutzer der Datenlieferant selber ist und dies freiwillig tut.

Ob an Gesundheits- und anderen Daten überhaupt Eigentumsrechte erworben und übertragen werden können, ist in der Schweiz eine offene Rechtsfrage.

Die Sekundärnutzung betrifft die Wiederverwendung von Daten für einen anderen Zweck[12]. Hier steht das Thema der Kontrolle über persönliche Gesundheitsdaten im Vordergrund. Leider ist den Nutzern nicht immer klar, was bei den Web-basierten App-Diensten mit den Daten geschieht, die sie sammeln. Viele Apps, die man sich aufs Handy herunterlädt, offenbaren überhaupt nicht oder nur in schlecht auffindbaren Nutzerbedingungen, dass sie ebenfalls Daten sammeln, auswerten und weiterleiten[13]. Zudem sind sich viele Nutzer nicht bewusst, dass eine stetig wachsende Industrie mit ihren persönlichen Daten Geld verdient. Und weil viele Anbieter ihren Hauptsitz nicht in der Schweiz haben, gilt, was die Weitergabe von Daten angeht, längst nicht immer nur das DSG[14]. Auch der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) hat Vorbehalte: «Die Apps und Wearables, die diese Vermessung möglich machen, funktionieren immer nach demselben Konzept. Sie schöpfen Daten ab – und übermitteln sie dann irgendwohin, in der Regel zum Anbieter dieser Produkte. Dann muss ich mir als Nutzer die Frage stellen: Interessiert es mich, was derjenige mit meinen Gesundheitsinformationen anstellt, der mir das Gerät verkauft hat? Verkauft er sie beispielsweise weiter?»[15]

Datenschutzrechtlicher Rahmen

Hinter der guten Absicht, Verantwortung für den eigenen Körper zu übernehmen und gesünder zu leben, lauern aus datenschutzrechtlicher

Sicht diverse Gefahren. Der vorliegende Beitrag untersucht die datenschutzrechtlichen Rahmenbedingungen für Apps und Wearables.

Fehlende spezifische Gesetzgebung für Wearables und Apps

Es gibt in der Schweiz keine spezifischen Gesetzesbestimmungen, die sich mit Wearables und den dazugehörigen Apps beschäftigen. Auch hat es keine datenschutzrechtlichen Vorgaben für die Hersteller und Anbieter von Wearables und Apps. Der EDÖB hat sich verschiedentlich zum Thema geäussert[16], aber bis dato kein Merkblatt oder Weisungen herausgegeben. Es finden daher die herkömmlichen datenschutzrechtlichen Bestimmungen Anwendung.

Hat sich der Träger von der Schweiz aus registriert und werden die Daten in der Schweiz gesammelt, kann angenommen werden, dass das DSG zur Anwendung kommt.

Übermittlung in eine ausländische Cloud: Anwendbarkeit des DSG?

Viele der heutigen Hersteller/Anbieter von Wearables und Apps sind im Ausland, insbesondere in den USA, ansässig. Es findet also eine grenzüberschreitende Datenübermittlung statt. Es stellt sich daher die Frage, ob das DSG überhaupt zur Anwendung kommt. Das DSG ist auf die Bearbeitung von Personendaten in der Schweiz anwendbar, es gilt das Territorialitätsprinzip. Die Erhebung von Daten in der Schweiz – auch nur für eine kurze Minute und auch wenn die Daten danach gleich ins Ausland übermittelt werden – genügt als Anknüpfungspunkt für die Anwendbarkeit des DSG[17]. Da sich der Träger von Wearables von der Schweiz aus registriert hat und die Daten in der Schweiz während der Aktivitäten gesammelt werden, kann angenommen werden, dass das DSG zur Anwendung kommt. Es gibt jedoch auch hier Gegenargumente: Der Nutzer loggt sich direkt in einer Maske auf einer .com-Website mit Servern im Ausland ein, die Aktivitäten finden nicht in der Schweiz statt und die Daten fallen gleich auf dem ausländischen Server an und werden dort bearbeitet. In einem solchen Fall ist es wohl fraglich, ob das DSG zur Anwendung kommt. Solche und ähnliche Fragen wird es in der Zukunft aus rechtlicher Sicht zu erörtern geben. Schliesslich sei am Rande darauf hingewiesen, dass auch Art. 6 DSG bei grenzüberschreitenden Übermittlungen von gesundheits- und aktivitätsbezogenen Daten in die Cloud Anwendung findet und die entsprechenden Massnahmen (vertragliche Garantien, Privacy Shield usw.) ergriffen werden müssen, um einen angemessenen Schutz im Ausland, insbesondere in den USA, zu gewährleisten.

Besonders schützenswerte Personendaten und Persönlichkeitsprofile

Die Träger von Wearables sammeln gesundheits- und aktivitätsbezogene Daten. Es stellt sich nun vorab die Frage, ob dies Personendaten gemäss Definition des DSG sind. Dies ist nur dann der Fall, wenn die mittels Wearables gesammelten Daten sich einer bestimmten oder bestimmbaren Person (mit zusätzlichen Identifikatoren wie IP- oder MAC-Adressen) zuordnen lassen[18]. Apps sind sehr gut geeignet, (Gesundheits-)Daten über einen längeren Zeitraum zu erfassen und zu überwachen. Apps leben gerade davon, dass sich die Nutzer registrieren müssen, ansonsten gar keine Statistiken und Auswertungen über den Gesundheitszustand des Trägers angefertigt werden können. Es ist daher davon auszugehen, dass die gesammelten Daten dem Träger zugeordnet werden können (müssen) und diese damit Personendaten gemäss DSG sind. Es stellt sich weiter die Frage, ob diese Daten besonders schützenswerte Personendaten sind. Bekanntermassen knüpft das DSG zahlreiche, z.T. recht einschneidende Rechtsfolgen an den Begriff der besonders schützenswerten Personendaten: erhöhte Anforderungen bei der Einwilligung, Informationspflichten bei der Beschaffung, Anmeldepflicht von solchen Datensammlungen, erhöhte technische und organisatorische Massnahmen bei der Bearbeitung sowie ein Rechtfertigungsgrund für eine Bekanntgabe an Dritte[19]. Angaben über die Gesundheit werden als besonders schützenswerte Personendaten angesehen. Darunter fallen alle Informationen, welche direkt oder indirekt Rückschlüsse über den physischen oder psychischen Gesundheitszustand einer Person geben. Es ist nicht erforderlich, dass es sich um eine den Ansprüchen der Medizin gerecht werdende Diagnose handelt. Im Lichte dieser Ausführungen gehen die meisten Schweizer Autoren davon aus, dass die mittels Wearables und der dazugehörigen Apps gesammelten Daten besonders schützenswerte Personendaten darstellen.

Mit der Nutzung von Wearables und Apps gibt der Nutzer nicht nur vielfältige Informationen über seine Gesundheit preis, sondern kreiert auch ein aufschlussreiches Persönlichkeitsprofil. So ergeben sich beispielsweise anhand der Aufzeichnung der Schlafgewohnheiten Hinweise auf das psychische Befinden einer Person[20]. Gleich wie bei der Bearbeitung von

besonders schützenswerten Personendaten werden bei der Bearbeitung von Persönlichkeitsprofilen ebenfalls erhöhte Anforderungen gestellt.

Transparenz: erhöhte Informationspflicht

Gemäss Art. 7a DSG sind betroffene Personen bei der Beschaffung von besonders schützenswerten Personendaten sowie Persönlichkeitsprofilen aktiv darüber zu informieren, wer der Inhaber der Datensammlung ist, welches der Bearbeitungszweck und die Kategorien der Datenempfänger sind, falls eine Datenweitergabe an Dritte geplant ist. Die vorsätzliche Verletzung dieser Informationspflicht wird mit einer Busse von bis zu CHF 10 000 strafrechtlich sanktioniert. Es ist nicht relevant, ob es sich um Daten handelt, welche die betroffene Person selber veröffentlicht oder in Umlauf bringt[21]. Die Information muss aktiv und ausdrücklich erfolgen. Sie ist jedoch nicht an eine Formvorschrift gebunden. Die Hersteller/Anbieter von Wearables und Apps haben daher sicherzustellen, dass sie in ihren Nutzerbedingungen und Datenschutzerklärungen diesen Informationspflichten nachkommen, auch wenn in der Regel genau diese, dem Schutz der Privatsphäre und dem Recht auf informationelle Selbstbestimmung dienenden Dokumente von den Nutzern ungelesen akzeptiert werden[22]. In diesen Nutzerbedingungen sollte stehen, wer die Daten bearbeitet, wozu die Daten verwendet und ob sie an Dritte weitergegeben werden. Hat sich der Nutzer für eine Verwendung eines Wearables oder einer App entschieden, ist es ratsam, eine datenschutzfreundliche Einstellung zu wählen und der Anwendung nur Zugriff auf diejenigen Daten zu gewähren, die für die Zweckerbringung erforderlich sind. Somit entfallen etwa der Zugriff auf das Adressbuch, den Kalender oder Standortdaten[23]. Leider ist es in der Praxis jedoch so, dass die Hersteller/Anbieter von Wearables und Apps die Nutzer sehr intransparent und unvollständig darüber informieren, wo die gesammelten Daten gespeichert werden (Cloud) und inwiefern sie diese Dritten bekannt geben. Viele Hersteller/Anbieter bieten die Apps gratis an, verkaufen aber anschliessend die gesammelten Daten[24].

Zweckentfremdung

Nach dem Grundsatz der Zweckbindung dürfen Personendaten nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Art. 4 Abs. 3 DSG). Während die Primärnutzung (siehe vorne) unbestritten ist, ist bei Apps oft nicht klar, inwiefern die Anbieter die gesammelten Daten verknüpfen und auswerten und damit zweckentfremden dürfen. Ein zentrales Merkmal von Big Data Analytics, welche gerade bei der Quantified-Self-Bewegung interessant ist, liegt in der Kombination verschiedenartiger Daten und in deren Auswertung zur Gewinnung neuer Erkenntnisse. Diese neu gewonnen Erkenntnisse werden für die medizinische Produkteherstellung, eine gezielte Produktewerbung oder auch als Grundlage für die Berechnung von Versicherungsprämien genutzt[25].

Die Verwendung von Daten zu Zwecken, die bei deren Beschaffung nicht vorgesehen und für die betroffenen Personen nicht erkennbar waren, ist für Big Data damit geradezu charakteristisch[26] und stellt streng genommen eine Verletzung von Art. 4 Abs. 3 DSG dar. Auf der anderen Seite bieten die neuen Informationen, die durch die Kombination und Zweckentfremdung entstanden sind, neue Chancen und Erkenntnisse. Die Analysen stehen daher in einem Spannungsverhältnis zum Grundsatz der Zweckbindung. Ein möglicher Lösungsansatz wäre, dass die Zweckbindung durch einen auf dem Grundsatz der umfassenden Transparenz der Datenbearbeitung und der jederzeitigen Widerrufbarkeit einer einmal erteilten Einwilligung beruht[27].

In der Praxis informieren die Hersteller/Anbieter die Nutzer sehr unvollständig darüber, wo die Daten gespeichert und inwiefern sie Dritten bekannt gegeben werden.

Anonymisierung und Verschlüsselung als Lösung des Zielkonflikts?

Aus Sicht des Datenschutzes wäre es wünschenswert, die Identifizierung von Nutzern von Apps zu verunmöglichen oder zu erschweren. Wie dargelegt, ist die Anwendbarkeit des DSG nur insoweit gegeben, wie Personendaten bearbeitet werden. Falls Personendaten anonymisiert oder verschlüsselt werden (Schlüssel nur beim Nutzer – so dass faktisch eine Anonymisierung vorliegt) kann ein Bezug zu einer Person verunmöglicht werden und damit sind die Daten nicht mehr datenschutzrelevant. Dies tönt an und für sich ideal. Der EDÖB äussert sich jedoch auch hier kritisch: «Die Schwierigkeit bei Big Data mit ‹Sachdaten› oder ‹anonymisierten› Daten besteht darin, dass nicht ausgeschlossen werden kann, dass bei der Zusammenführung von mehreren Datenbeständen eine De-Anonymisierung erfolgt. Die Anonymisierung einzelner eindeutiger Identifikatoren reicht in vielen Fällen nicht aus, um Re-Identifizierungen auszuschliessen. Auch mit

sogenannten Quasi-Identifikatoren – Kombinationen von Attributen wie Geburtsdatum, Geschlecht und Postleitzahl – muss vorsichtig umgegangen werden. So ermittelten US-Wissenschaftler, dass sich vier Fünftel der amerikanischen Bevölkerung allein anhand dieser drei Merkmale nachträglich identifizieren lassen[28].» Das anwendbare Recht verlangt keine Anonymisierung oder Verschlüsselung der Personendaten bei Apps und zudem sind anonymisierte/verschlüsselte Personendaten oft «wertlos» für eine Analyse. Es bleibt den Herstellern/Anbietern im Moment nichts anderes übrig, als sich möglichst nahe an die datenschutzrechtlichen Grundsätze der Transparenz und Zweckbindung zu halten. Wobei in der Praxis Entwicklungen zu beobachten sind, wonach Datenschutz nicht mehr reicht, sondern Big-Data-Projekte auch aus ethischer Sicht beurteilt werden müssen. Zu diesem Zweck hat beispielsweise die Swisscom einen Ethik-Ausschuss ins Leben gerufen[29].

Die zweckfremde Verwendung von Daten ist für Big Data damit geradezu charakteristisch und stellt streng genommen eine Verletzung des DSG dar.

Einwilligung

Werden besonders schützenswerte Personendaten an Dritte übermittelt, dann braucht es hierfür eine ausdrückliche Einwilligung. Gerade die Daten, die mittels Wearables und Apps gesammelt werden, werden an Dritte weiterverbreitet oder auch verkauft. Damit der Nutzer jedoch eine Einwilligung abgeben kann, muss er umfassend über die Nutzung seiner Daten informiert werden. Dies setzt voraus, dass die Anbieter/Hersteller transparent und vollständig über die Nutzung in ihren Geschäftsbedingungen berichten (siehe vorne), damit der Nutzer in der Lage ist, das Ausmass und den Inhalt der Datenbearbeitung abzuschätzen. Leider wird ein Nutzer in der Praxis jedoch kaum je in der Lage sein, eine angemessene Folgeabschätzung der Datenbearbeitung vorzunehmen. Die heutige Datenschutzgesetzgebung entspricht daher mit ihren strengen Regeln nicht den derzeitigen Realitäten[30].

Datensicherheit

In der Schweiz gibt es keine sektorspezifischen Vorgaben für die Datensicherheit betreffend Wearables und Apps. Auch hier muss auf die allgemeinen Bestimmungen des DSG verwiesen werden. Bei der Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen sind erhöhte Datensicherheitsmassnahmen zu ergreifen (Art. 7 DSG und Art. 8–12 VDSG). Leider stellt bei vielen Herstellern und Anbietern von Wearables und Apps die IT-Sicherheit jedoch kein prioritäres Thema dar[31]. Zudem ist es aus technischer Sicht oft sehr schwierig, die technische Datensicherheit einzuhalten. Bei der Anwendung von Big Data (d.h. der aus den Wearables und Apps gewonnenen Erkenntnisse) müssen die folgenden Zielkonflikte abgewogen werden: Effizienz, Compliance und Kosten versus Schutz der Persönlichkeit und der informationellen Selbstbestimmung. Es liegt nun am Gesetzgeber, Möglichkeiten aufzuzeigen, wie Big Data gesetzeskonform eingesetzt werden kann[32]. Der EDÖB hat bis dato auch keine sektorspezifischen Weisungen für die Datensicherheit für Wearables und Apps herausgegeben. In diesem Zusammenhang sei auf die generellen Ausführungen zu Big Data verwiesen[33].

Empfehlungen im Umgang mit Apps

Es finden in der Schweiz und auch im Ausland diverse Aktivitäten betreffend Apps statt. Zudem haben sich Interessengruppen gebildet. So hat es sich die eHealth Suisse zum Ziel gesetzt, eine «mHealth Roadmap Schweiz» zu erarbeiten[34], und auch der Bundesrat hat das Nationale Forschungsprogramm NFP «Big Data» (CHF 25 Mio.) lanciert, um die Grundlagen für einen wirksamen und angemessenen Einsatz von Datenmengen in allen Gesellschaftsbereichen (einschliesslich des Gesundheitsbereichs) zu schaffen.

Diese Bewegungen und Berichte geben diverse Ratschläge im Umgang mit Apps. Nachfolgend eine Zusammenfassung einiger praktischer Empfehlungen[35]:

- Es sollten generell nur Informationen bekannt gegeben werden, bei deren Veröffentlichung man sich «wohl» fühlt und wo keine nachteiligen Auswirkungen zu befürchten sind.
- Man muss immer davon ausgehen, dass die angegebenen persönlichen Daten dem App-Entwickler und auch Drittparteien weitergegeben werden.
- Die Angabe von persönlichen Informationen sollte auf ein Minimum reduziert werden.
- Nur die absolut notwendigen Zustimmungen und Zugriffe sollten erteilt werden.
- Die Funktionen, die für die Nutzung der App nicht unbedingt notwendig sind, sollten ausgeschaltet werden.
- Soweit dies möglich ist, sollten Informationen über den App-Entwickler eingeholt werden: gibt es eine dazugehörige Website? Wie ist die Qualität des Inhaltes der Website? Gibt es eine

Datenschutzerklärung? Wurden Kontaktdaten angegeben?

- Kostenpflichtige Apps abonnieren: Diese sind in der Regel sicherer.

Fazit

Die im Rahmen der Quantified-Self-Bewegung gesammelten gesundheits- und aktivitätsbezogenen Daten können nicht nur Verhaltensänderungen fördern und Aufschluss über die Gesundheit geben, sondern mit Analysen können auch bevölkerungsbezogene Gesundheitsdaten gewonnen werden. Die Chancen und Vorteile von Big Data im Gesundheitswesen und Sport-/Lifestylebereich werden in der Schweiz noch nicht voll ausgeschöpft. Aber auch die Schweizer Gesetzgebung hinkt hinter der technologischen Entwicklung hinterher und es besteht dringender Handlungsbedarf, angemessene Rechtsbestimmungen einzuführen. Die heutigen Bestimmungen des DSG reichen nicht mehr aus, um diesen Entwicklungen, die massgeblich von Social Media geprägt werden, gerecht zu werden. ■

Leider stellt bei vielen Herstellern und Anbietern von Wearables und Apps die IT-Sicherheit kein prioritäres Thema dar.

Fussnoten

1 Quantified Self, Das Ich als Datenberg, in: TagesWoche vom 6. Juni 2013.
2 Hildegard Kaulen, An der Grenze zu Wellness, in: FAZ vom 27. Februar 2015.
3 datum, Newsletter des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten, Dezember 2014, 1.
4 Günter Karjoth, Der «betreute» Mensch, in: digma, 2014, 139.
5 Siehe <http://www.gartner.com/newsroom/id/3198018>.
6 Markus Städeli, Die Smarte Uhr wird überschätzt, das Handy unterschätzt, in: NZZ am Sonntag vom 22. März 2015.
7 Claudia Keller, Stategie & Praxis, Recht, Fitness-Apps als Datensammler: Was sagt das Recht?, 20.
8 datum (Fn. 3), 2.
9 Karjoth (Fn. 4), 141.
10 Konstantin Knorr, Datensicherheit bei mHealth-Apps, in: digma 2015, 162.
11 Irène Dietschi, Daten: Die vermessene Gesundheit, in: Beobachter vom 16. Mai 2014.
12 Big Data im Gesundheitswesen, White Paper, swiss academies communications, Vol. 10, Nr. 2, 2015, 15.
13 Hanspeter Thür, Die Privatsphäre im Zeitalter von Big Data, in Jusletter IT vom 21. Mai 2015.
14 Alexandra Bröhm, Zu viele Daten sind ungesund, in: Sonntags-Zeitung vom 25. Januar 2015.
15 Oliver Fuchs, Datenschutz ist kein Luxusgut, Interview mit Hanspeter Thür, in: NZZ vom 29. Januar 2015.
16 Siehe z.B. anlässlich der Datenschutztagung am 28. Januar 2015: GesundheitsApps und Wearables im Trend – Eine Bedrohung für die Privatsphäre?
17 BGE 138 II 346 ff. («Google Street View»).
18 Michael Isler, Mobile Medical Apps: Patient Datenschutz, in: digma 2013, 111.
19 Yvonne Jöhri, in: David Rosenthal/Yvonne Jöhri, Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 3 N 44.
20 datum (Fn. 3), 2 f.
21 David Rosenthal, in: Rosenthal/Jöhri (Fn. 19), Art. 7a N 7.
22 Claudia Keller, Stategie & Praxis, Recht, Fitness-Apps als Datensammler: Was sagt das Recht?, 22.
23 datum (Fn. 3), 3.
24 Barbara Widmer, mHealth – Health for me – or others?, in: digma 2015, S. 170 f.
25 Widmer (Fn. 24), 170.
26 Florent Thouvenin, Erkennbarkeit und Zweckbindung: Grundprinzipien des Datenschutzes auf dem Prüfstand von Big Data, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich 2014, 68.
27 Thouvenin (Fn. 26), 83.
28 Siehe <http://www.edoeb.admin.ch/datenschutz/00683/01169/index.html?lang=de>.
29 Matthias Sander, Ethik-Ausschuss für Big Data, Datenschutz allein reicht nicht aus, in: NZZ vom 21. April 2016.
30 Rolf Weber, Big Data: Rechtliche Perspektive, in: Weber/Thouvenin (Fn. 26), 25.
31 Widmer (Fn. 24), 171.
32 Nicole Beranek Zanon, Big Data und Datensicherheit, in: Weber/Thouvenin (Fn. 26), 114.
33 <http://www.edoeb.admin.ch/datenschutz/00683/01169/index.html?lang=de>.
34 Siehe <http://www.e-health-suisse.ch/umsetzung/00135/00218/00278/index.html?lang=de>.
35 Siehe z.B. Linda Ackerman, Mobile Health and Fitness Applications and Information Privacy, Report to California Consumer Protection Foundation, vom 15. Juli 2013, 23.

(Alle URL zuletzt besucht am 3.5.2016.)

Zeitschrift für Datenrecht und Informationssicherheit
digma
www.digma.info erscheint vierteljährlich

Meine Bestellung

❑ 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)
à **CHF 168.00** bzw. bei Zustellung ins Ausland **CHF 195.00** (inkl. Versandkosten)

❑ PrintPlus: Jahresabo Inland **CHF 189.00:** Jahresabo Ausland **CHF 214.00**

Name Vorname

Firma

Strasse

PLZ Ort Land

Datum Unterschrift

Bitte senden Sie Ihre Bestellung an:
Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8022 Zürich
Telefon +41 44 200 29 19
Telefax +41 44 200 29 29
E-Mail: zs.verlag@schulthess.com
Homepage: www.schulthess.com

Schulthess §