4/2016
73 – 96

KURZMELDUNG
Dash-Cam-Aufnahme zugelassen
Viktoria Haidinger

DATENSCHUTZ KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Online und Datenschutz

Praxisprojekt Onlinekommunikation zwischen Ärzten und Patienten

Felix Stonek, Christoph Berdenich, Rainer Knyrim, Christian Kern

mHealth – meine Organe gehen online

Siegfried Gruber, Markus Oman

Marketing-Unternehmen sind keine Datenkraken

Interview mit Markus Deutsch, WKÖ

Datenschutz online: Analytics & Tracking-Cookies

Christoph Berdenich

Checkliste Webauftritt

Hans-Jürgen Pollirer

Privacy Shield: Politisch gewollte Totgeburt mit Anlauf? (Teil 2)

Maximilian Schrems

Datenschutz bei Patientendaten

Viktoria Haidinger

ISSN 2313-5409

dako.manz.at

MANZ

P.b.b. Verlag Manz 1230 Wien, Gutheil Schoder Gasse 17

Siegfried Gruber/Markus Oman
Senior Berater O.P.P. – Beratungs GmbH/geschäftsführender Gesellschafter O.P.P. – Beratungsgruppe

mHealth – meine Organe gehen online

Patienten messen Gesundheitsdaten selbst und übertragen die Ergebnisse elektronisch, teilweise über weltweite Clouds, an ihre Ärzte. Für alle Beteiligten stellen sich dabei Fragen: Der Arzt verlässt sich darauf, dass richtig und beim richtigen Patienten gemessen wurde sowie dass die Übertragung fehlerfrei ist. Vom Patienten wird eine hohe Selbstverantwortung verlangt. Arzt und Patient verlassen sich auf eine hohe Sicherheit der Übertragung.

Messungen als Teil der medizinischen Diagnose

„Spätestens seit der Einführung des Fieberthermometers wird in der Medizin mittels Technik leidenschaftlich gemessen und vermessen. Das Messen bietet dabei in der Medizin den Mehrwert, dass Patientendaten vergleichbar, standardisierbar und auch transportabel wurden. Das Messen der Ärzte hat sich dabei scheinbar verselbständigt. Schon seit langem messen Patienten selbst mit Begeisterung ihr Gewicht, ihre Temperatur oder zählen die Bakterien in ihrem Sputum."[1]

Mobile Gesundheit

Nachdem die Verwendung des Internets und von mobilen Endgeräte schon in vielen Bereichen des beruflichen und privaten Lebens Einzug gehalten hat, dringen diese Technologien nun in den Bereich der Gesundheit vor.

Die mobile Gesundheit, englisch **„mobile Health"** oder „mHealth", ist ein neues, dynamisches und expandierendes Feld der Gesundheitsversorgung. „mHealth" ist mit den Bereichen „Telemedizin" und „eHealth" verbunden. **Telemedizin** als Oberbegriff beschreibt die Verwendung (meist audiovisueller) Kommunikationstechnologien, der Begriff **„eHealth"** umfasst zusätzliche Gesundheitsdienstleistungen, die mit Mitteln

[1] *Martin*, Bedeutung und Funktion des medizinischen Messens in geschlossenen Patienten-Kollektiven. Das Beispiel der Lungensanatorien, in *Hess* (Hrsg), Normierung der Gesundheit. Messende Verfahren der Medizin als kulturelle Praktik um 1900 (1997).

der Informations- und Kommunikationstechnologien erbracht werden. Im Rahmen von „mHealth" wird die Verwendung mobiler Komponenten hinzugefügt, von Mobiltelefonen über Smartphones, Tablets und anderen tragbaren und im Gesundheitskontext nutzbaren Geräten.[2]

APPs und Wearables übernehmen die Selbstmessung

Eine Vielzahl von APPs dient dazu, um mittels Sensoren des Geräts (überwiegend Bewegungssensoren) oder am Körper angebrachten Sensoren (sog **„wearables"**) gemessener Werte oder durch manuelle Eingabe von Puls, Blutdruck, Kalorienzahl, Gewicht, etc Informationen zu sammeln. Die App selbst dient dazu, die Daten zu speichern, zu visualisieren und (mehr oder weniger valide) Aussagen über den körperlichen Zustand des Betroffenen zu treffen.

Das Angebot an gesundheitsbezogenen Apps umfasst aber nicht nur den vergleichsweise einfachen Bereich der Fitness- und Wellnessanwendungen, sondern erreicht auch Bereiche der **medizinisch-professionellen Benutzergruppen**, bei denen diese Apps die Daten von Patienten manuell (zB durch Eingabe über die Tastatur oder Anfertigen von Fotos) oder über entsprechende Sensoren automatisiert erfasst und dem behandelnden Arzt zur Analyse übermittelt werden. Auf Basis dieser Daten werden in weiterer Folge Entscheidungen iZm der spezifischen Heilbehandlung getroffen.

Mobile Anwendungen ermöglichen neue Arten der medizinischen Versorgung.

Diese mobilen Anwendungen ermöglichen Anbietern von Gesundheitsdiensten neue Arten der Versorgung, indem sie aktuelle Informationen über ihre Patienten erhalten. Aus der Sicht der Gesundheitsdienstleister ist es beim Einsatz telemedizinischer Versorgungskonzepte wichtig, die **Validität** der jeweiligen **Daten** bzw der daraus aufbereiteten Informationen zu beachten.[3] Der Einsatz von nicht explizit für den medizinischen Einsatz vorgesehenen Produkten liegt in der Verantwortung des Behandlers bzw des Vertragspartners.[4] Ergibt sich aus der Produktbeschreibung und aus Werbematerialien eine medizinische Zweckbestimmung, so handelt es sich in der Regel um ein **Medizinprodukt**.[5] Für das Inverkehrbringen und die Inbetriebnahme eines derartigen Produkts ist Voraussetzung, dass dieses rechtmäßig mit einer CE-Kennzeichnung versehen wird.[6]

Selbstverantwortung des Patienten

Aber auch die Benutzer sind hier gefordert, denn vielfach sind mitverantwortlich für die Bereitstellung der Daten in der erforderlichen Qualität.

Im Rahmen der folgenden Überlegungen soll va der Einsatz derartiger Produkte iZm einer Heilbehandlung durch Anbieter von Gesundheitsdiensten aus datenschutzrechtlicher Perspektive analysiert werden.

Schon heute finden sich viele derartige Angebote, bei denen entweder der Auftraggeber selbst oder aber allenfalls Dienstleister ihren Sitz außerhalb Österreichs (vielfach in den USA) haben, daher stellt sich die Frage der **Anwendbarkeit** des **DSG 2000**. Bis zum Inkrafttreten der DSGVO (am 25. 5. 2018) ist das österr Datenschutzgesetz nur auf die Verwendung personenbezogener Daten in Österreich bzw bei Verwendung in anderen Mitgliedstaaten der EU für Zwecke einer in Österreich gelegenen Haupt- oder Zweigniederlassung eines Auftraggebers anzuwenden. Die nachfolgenden Erläuterungen nehmen Bezug auf jene Fälle, in denen das DSG 2000 räumlich anwendbar ist. **Nach** dem **Inkrafttreten der DSGVO** wird der räumliche Anwendungsbereich auf die Verarbeitung personenbezogener Daten durch einen Verantwortlichen[7] oder Auftragsverarbeiter,[8] der seinen Sitz in der Union hat, ausgedehnt, unabhängig davon, ob die Verarbeitung in der Union stattfindet. Zudem ist die DSGVO auch anzuwenden auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht, der betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten. Das wird bei der Bereitstellung von mHealth-Leistungen wohl häufig der Fall sein.

Damit derartige Anwendungen überhaupt unter den Regelungsbereich der datenschutzrechtlichen Bestimmungen fallen, ist es erforderlich, dass hierbei **Informationen** verwendet werden, die **iZm** einer identifizierten bzw **identifizierbaren Person** stehen. Primär erfassen derartige Anwendungen die Messdaten des jeweiligen Benutzers lokal auf dem jeweiligen Endgerät (Smartphone, Wearable etc). In der Regel werden derartige Anwendungen nicht direkt von den jeweils mit der Heilbehandlung befassten Gesundheitsdienstleister angeboten, sondern durch Betreiberdienste. Diese Betreiber stellen einerseits die Anwendung am jeweiligen Endgerät zur Verfügung, aber auch die zentralen Dienste zur Datenspeicherung und zum Datenaustausch mit Gesundheitsdiensteanbietern (GDA). Vielfach handelt es sich bei diesen Betreibern um die Hersteller von einschlägigen Medizinprodukten oder Arzneimitteln bzw von ihnen beauftragte Dienstleister.

Mit einer Registrierung ist eine Zuordnung von Daten zu einer Person möglich!

Zur Verwendung iZm einer Heilbehandlung ist eine **Zuordnung** dieser **Daten zu einer Person** erforderlich, damit für den GDA eine Zuordnung der Daten zum Patienten möglich ist. Dies erfolgt in der Regel im Zusammenhang mit der Anmeldung **(Registrierung)** zu einem Dienst. In der Praxis hat sich gezeigt, dass im Rahmen der Registrierung zu derartigen Diensten der Name, die Adresse und diverse Kontaktdaten des Patienten gegenüber dem Diensteanbieter bekannt zu geben sind. Soweit eine namentliche Registrierung erforderlich ist, liegen die Daten nicht nur für den GDA, sondern auch für den Dienstebetreiber in personenbezogener Form vor.

Gesundheitsdaten sind Daten besonderer Kategorien

Aus datenschutzrechtlicher Sicht handelt es sich bei den hierbei verwendeten Daten um **sensible Daten** gem § 4 Z 2 DSG 2000 in Form von „Gesundheitsdaten", somit um personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorge-

[2] *Kay/Santos/Takane,* mHealth: New horizons for health through mobile technologies, World Health Organization (2011) 66. [3] *Albrecht,* Kapitel Kurzfassung, in *Albrecht* (Hrsg), Chancen und Risiken von Gesundheits-Apps (CHARISMHA) 22. [4] *Pramann,* Gesundheits-Apps und Datenschutz, in *Albrecht* (Hrsg), Chancen und Risiken von Gesundheits-Apps (CHARISMHA) 236. [5] EuGH 22. 11. 2012, C-219/11, *Brain Products.* [6] *Pramann,* Gesundheits-Apps und Datenschutz 230. [7] Auftraggeber iSd § 4 Z 4 DSG 2000. [8] Dienstleister iSd § 4 Z 5 DSG 2000.

hen.[9] Eine Verwendung dieser Daten ist nur unter den Voraussetzungen der Regelungen des § 9 DSG 2000[10] zulässig.

Soweit die Daten durch den GDA im Rahmen einer konkreten Heilbehandlung verwendet werden, ergibt sich die **Zulässigkeit** in der Regel aus § 9 Z 12 DSG 2000 iVm der jeweiligen Rechtsgrundlage zur Ausübung seines Berufs, wenn die Verwendung dieser Daten durch ärztliches Personal oder sonstige Personen erfolgt, die einer Geheimhaltungspflicht unterliegen.

Freiwilligkeit ist nur bei ausreichender Information gegeben.

Erfolgt die Datenverwendung zu anderen Zwecken (entweder durch den GDA, den Dienstebetreiber oder sonstige Dritte), so ist für diese Fälle eine **ausdrückliche Zustimmung** des Betroffenen gem § 9 Z 6 leg cit erforderlich. Wenn bspw Gesundheits-Apps über den Verkauf von Nutzungsdaten mit Personenbezug finanziert werden, wäre dies ohne umfangreiche Aufklärung und Einwilligung nicht zulässig.[11]

Die Wirksamkeit einer diesbezüglichen Einwilligung ist nur dann gegeben, wenn diese auf der **freien Entscheidung** des Betroffenen beruht und dieser über den vorgesehenen Zweck der Verwendung, die konkreten Datenarten sowie über Dritte, an die Daten weitergegeben werden, informiert ist. Zudem ist darauf hinzuweisen, dass eine einmal erteilte Zustimmung jederzeit widerrufen werden kann. Durch Einhaltung der Schriftform kann das Erfordernis der Nachweislichkeit jedenfalls erfüllt werden. Inwieweit die Erteilung einer Zustimmung durch Aktivieren einer „Checkbox" (Häkchen) in elektronischen Prozessen das Erfordernis der Nachweislichkeit erfüllt, muss im Einzelfall geprüft werden.

PRAXISTIPP FÜR BETROFFENE

AGB können Gerichtsstände in Übersee festlegen: Es ist schwer, in New York zu klagen, wenn man aus der österr Provinz kommt.

Neben der datenschutzrechtlichen Zustimmungserklärung unterliegt die Verwendung derartiger Anwendung vielfach auch der Einbeziehung **allgemeiner Geschäftsbedingungen**. Diese sollten, auch wenn sie umfangreich sind, vor ihrer Akzeptanz sorgfältig gelesen werden, denn auch sie werden Vertragsbestandteil.

Soweit die Daten in personenbezogener Form für Zwecke der **wissenschaftlichen Forschung** und Statistik verwendet werden sollen, so ist dies nur im Rahmen der Bestimmungen des § 9 Z 10 DSG 2000 zulässig. Wobei in diesen Fällen idR eine Verwendung der Daten in personenbezogener Form nicht erforderlich ist. Eine Datenverwendung in anonymisierter Form ist zur Zielerreichung meistens ausreichend.

Häufig werden derartige Dienste unter Einbeziehung von **Dienstleistern im Ausland** erbracht. Soweit eine Übertragung personenbezogener Daten in Länder außerhalb des EWR oder Länder ohne (durch Verordnung festgestelltes) angemessenes Datenschutzniveau erfolgt, ist dafür eine gesonderte Zustimmung des Betroffenen erforderlich, soweit ein im Interesse des Betroffenen geschlossener Vertrag nicht ohne diese Datenübermittlung erfüllt werden kann. Ohne Zustimmung bzw Vertrag zugunsten des Betroffenen ist zur Rechtmäßigkeit der Datenübermittlung in diesen Fällen eine Genehmigung durch die Datenschutzbehörde erforderlich.

PRAXISTIPP FÜR GDA:

Wenn die Daten der App als Grundlage für Entscheidungen iZm einer Heilbehandlung verwendet werden, ist sicherzustellen, dass es sich bei der App um ein Medizinprodukt gem § 2 Abs 1 Medizinproduktegesetz handelt.

Zudem ist sicherzustellen, dass die Daten aus der App, soweit sie als Grundlage von Behandlungsentscheidungen verwendet wurde, auch Eingang in die **ärztliche Dokumentation** finden und auch für die gesetzliche Aufbewahrungsdauer verfügbar sind (im Zweifel Kopie „Bildschirmausdruck" anfertigen).

Datensicherheitsmaßnahmen

Neben den rechtlichen Überlegungen im Zusammenhang mit der Verwendung von mobilen Gesundheitsanwendungen, sollte das Thema des Schutzes der verwendeten Daten durch Ergreifen angemessener Datensicherheitsmaßnahmen noch Erwähnung finden. Für Auftraggeber und Dienstleister (somit GDA, Diensteanbieter und deren Dienstleister) ergibt sich die **Verpflichtung** zur Ergreifung entsprechender Datensicherheitsmaßnahmen aufgrund § 14 DSG 2000.

PRAXISTIPP FÜR GDA:

Soweit der GDA Gesundheitsdaten weitergibt, sind die Bestimmungen des Gesundheitstelematikgesetzes (GTelG) zu beachten.

§ 3 Abs 4 GTelG bestimmt, dass jedenfalls sicherzustellen ist, dass ein zulässiger Zweck gem § 9 Z 6 DSG 2000 vorliegt und die **Identität** des Betroffenen sowie die Identität und Rolle der an der Datenweitergabe beteiligten GDA nachgewiesen wurden. Zudem ist die **Vertraulichkeit** und die Integrität der weitergegebenen Gesundheitsdaten zu gewährleisten. IZm der Wahrung der Vertraulichkeit kommen hierbei Methoden der Kryptografie **(Verschlüsselung)** zur Verwendung, die Integrität der übermittelten Daten wird insb durch die Verwendung qualifizierter und fortgeschrittener elektronischer Signaturen (oder Siegel) gewährleistet.

„Privacy by design" kann helfen, die Vertraulichkeit von Daten zu gewährleisten.

In Anbetracht der Sensibilität der verwendeten Daten und der nicht unerheblichen Gefahren eines Missbrauchs, sollten im Zusammenhang mit der Produktentwicklung Überlegungen zu **„privacy by design"**und „privacy by default" mit einfließen und insb Mechanismen zur sicheren Identifizierung des Anwenders und Methoden der End-to-end-Verschlüsselung eingesetzt werden.

ISd DSGVO lautet der **Grundsatz** für privacy by design: So wenig personenbezogene Daten wie möglich erheben und verarbeiten. Diese Daten anonymisieren oder pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert. Das heißt: Bevor ein neues System zur Erfassung personenbezogener Daten eingeführt wird, sollen die verantwortlichen Stellen sicherstellen, dass Datenschutzlösungen von Anfang an fest eingebaut werden und nicht erst in einem späteren Stadium hinzugefügt werden müssen.

Zu beachten ist, dass aufgrund der ständig wachsenden Verarbeitung von Daten die Gefahr steigt, dass Daten, die ursprünglich ohne Personenbezug gespeichert wur-

[9] Art 4 Z 15 DSGVO. [10] Schutzwürdige Geheimhaltungsinteressen bei der Verwendung sensibler Daten. [11] *Pramann*, Gesundheits-Apps und Datenschutz 218.

den, durch neue Verarbeitungsmethoden (zB BigData) plötzlich Personenbezug erhalten (und somit neue Rechtsfolgen entstehen).

Ein nicht unwesentliches (Un-)Sicherheitselement stellt gerade bei Verwendung von mobilen Endgeräten in Form von Smartphones, Tablets uÄ der Benutzer dieser Endgeräte dar. Dieser übernimmt im konkreten Fall die Verantwortung für die Sicherheit der ihn betreffenden Daten auf seinem Endgerät. Durch Einrichtung eines entsprechenden **Zugriffsschutzes** und Verwendung eines aktuellen **Virenschutzes** sowie Schutzprogrammen gegen Schadsoftware sollte sichergestellt werden, dass Daten weder durch Unbefugte eingesehen noch gelöscht oder gar unbemerkt verändert werden können.

Dako 2016/50

Zum Thema

Über die Autoren

Mag. jur. Siegfried Gruber ist Senior Berater bei O.P.P. – Beratungs GmbH. Mag. Ing. Markus Oman, CSE, ist geschäftsführender Gesellschafter der O.P.P. – Beratungsgruppe.
Kontakt: Tel: +43 (0)699 125 180 89, E-Mail: datenschutz@opp-beratung.com, Internet: www.opp-beratung.com