Zeitschrift: SuchtMagazin
Band: 45 (2019)
Heft: 2

Artikel: Datenschutz im Gesundheitswesen : was ist zu beachten?
Autor: Widmer, Barbara
DOI: https://doi.org/10.5169/seals-865652

Datenschutz im Gesundheitswesen – was ist zu beachten?

2019 - 2
Jg. 45
S. 29 - 33

Die Digitalisierung hat den Gesundheitsbereich längst erreicht und in verschiedener Hinsicht verändert – Cloud-Angebote werden immer attraktiver und die Anonymisierung von Personendaten ist immer schwieriger. Da es sich bei Gesundheitsdaten um besonders schützenswerte Personendaten handelt, gelten für diese erhöhte Datenschutzanforderungen.

BARBARA WIDMER
Dr. iur., LL.M., Certified Internal Auditor CIA. Die Autorin vertritt die Konferenz der kantonalen Datenschutzbeauftragten in verschiedenen Arbeitsgruppen von eHealth Suisse, barbara.widmer@dsb.bs.ch

«Ich habe nichts zu verbergen», «Wir haben nichts zu verbergen» – diese Aussagen sind mit Blick auf den Datenschutz sehr verbreitet. Viele sind der Ansicht, der Datenschutz gehe primär die anderen etwas an. Diese Annahme ist jedoch falsch. Alle haben etwas zu verbergen und daran ist auch nichts falsch. Insbesondere im Gesundheitsbereich ist zu viel Transparenz kein guter Ratgeber. Zwar sind nicht alle Gesundheitsdaten gleich brisant, jedoch kann das ungewollte Bekanntwerden von Daten über Erkrankungen, die im gesellschaftlichen Fokus stehen – wie z. B. Sucht-, psychische, HIV- oder Geschlechtserkrankungen – für die Betroffenen erhebliche Folgen haben.

Im Gesundheitswesen muss dem Datenschutz entsprechend eine erhöhte Bedeutung zukommen. Worin diese besteht und was es dabei zu beachten gilt, zeigt der nachfolgende Beitrag.

Gesundheitsdaten = Personendaten

Gesundheitsdaten qualifizieren sich stets als Personendaten. Nach der schweizerischen Datenschutzgesetzgebung handelt es sich bei Personendaten um Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 3 lit. a DSG)[1]. Eine Person ist bestimmt, wenn sich ihre Identität direkt aus den Daten selbst ergibt, z. B. aus einem Pass oder einer Abonnementskarte. Als bestimmbar gilt eine Person, wenn sich ihre Identität aus dem Datenkontext oder durch gezielte Verknüpfung mit weiteren Daten ergibt.

Die Datenschutzgesetzgebung sieht zwei Kategorien von Personendaten vor: Normale Personendaten und besonders schützenswerte Personendaten.

Normale Personendaten umfassen Daten, die wenig geeignet sind, die Persönlichkeit einer betroffenen Person zu verletzen – wie z. B. den Namen, die Adresse, das Geburtsdatum oder auch reine Finanzdaten, z. B. den Kontostand.

Besonders schützenswerte Personendaten zeichnen sich dagegen dadurch aus, dass sie besonders geeignet sind, die Persönlichkeit einer Person zu verletzen (Maurer-Lambrou & Blechta: Art. 3 Rn. 27). Darunter fallen Daten über die religiöse, weltanschauliche oder politische Gesinnung, Massnahmen der sozialen Hilfe wie z. B. der Bezug von Sozial- oder Sozialversicherungsleistungen oder auch Daten über die Gesundheit und die Intimsphäre (z. B. die sexuelle Ausrichtung) (Art. 3 lit. c DSG). Während die schweizerische Datenschutzgesetzgebung den Begriff der Gesundheitsdaten nicht speziell definiert, hält die neue EU-Datenschutzgesetzgebung fest, Gesundheitsdaten seien personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person bezögen (einschliesslich der Erbringung von Gesundheitsdienstleistungen) und aus denen Informationen über den Gesundheitszustand dieser Person hervorgingen (Art. 4 Ziff. 15 DSGVO)[2].

Die Qualifizierung von Daten als normale oder besonders schützenswerte Personendaten ist insofern von Bedeutung, als die Datenschutzgesetzgebung für deren rechtmässige Bearbeitung unterschiedliche Voraussetzungen vorsieht.

Voraussetzungen für die Bearbeitung von Gesundheitsdaten

Die Datenschutzgesetzgebung enthält Vorgaben, unter welchen Voraussetzungen Personendaten und damit auch Gesundheitsdaten bearbeitet werden dürfen.

Bearbeiten

Was unter «Bearbeiten» zu verstehen ist, definiert die Datenschutzgesetzgebung für ihren Anwendungsbereich selbständig. Nach Art. 3 lit. e DSG umfasst das Bearbeiten jeden Umgang mit Personendaten, unabhängig davon, ob die Bearbeitung digital oder analog erfolgt. Erfasst sind das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten. Der Begriff der Bearbeitung ist somit weit zu verstehen und umfasst JEDEN Umgang mit Personendaten.

Voraussetzungen

Die Voraussetzungen für ein rechtmässiges Bearbeiten von Personendaten hängen einerseits davon ab, ob es sich bei der bearbeitenden Instanz um ein öffentliches Organ (Gemeinde, Kanton, Bund) oder eine natürliche oder juris-

tische Person des Privatrechts (Verein, Stiftung, AG, GmbH) handelt und andererseits von der Art der bearbeiteten Personendaten:

Öffentliche Organe sind mit wenigen Ausnahmen dann befugt, Personendaten zu bearbeiten, wenn es dafür eine gesetzliche Grundlage gibt (Art. 17 Abs. 1 DSG). Findet eine Bearbeitung von besonders schützenswerten Personendaten statt, gelten für die Ausgestaltung dieser gesetzlichen Grundlage erhöhte Anforderungen (Art. 17 Abs. 2 DSG). Jedenfalls findet sich diese gesetzliche Grundlage nicht im Datenschutzgesetz, sondern in der jeweils anwendbaren Spezialgesetzgebung – z. B. in der Sozialversicherungs-, der Gesundheits- oder Sozialhilfegesetzgebung.

Natürliche und juristische Personen des Privatrechts dürfen Personendaten in der Regel dann bearbeiten, wenn die betroffenen Personen in die Bearbeitung eingewilligt haben (Art. 13 Abs. 1 DSG). Die Einwilligung ist dabei nur gültig, wenn sie nach angemessener Information (in Kenntnis der Sachlage) und freiwillig (ohne Druck) erfolgt (Rampini Corrado Art. 13 Rn. 4). Bei der Bearbeitung von besonders schützenswerten Personendaten muss die Einwilligung zudem ausdrücklich erfolgen – aus Beweisgründen empfiehlt sich Schriftlichkeit (Art. 4 Abs. 5 DSG). Erhalten natürliche oder juristische Personen des Privatrechts von einem öffentlichen Organ einen Leistungsauftrag (im Gesundheitswesen verbreitet der Fall), werden sie in datenschutzrechtlicher Hinsicht im Umfang dieses Leistungsauftrags gleich behandelt wie das beauftragende öffentliche Organ. Für sie gelten somit für die Bearbeitung von Personendaten im Rahmen des Leistungsauftrags dieselben datenschutzrechtlichen Voraussetzungen wie für das öffentliche Organ (Art. 3 lit. h DSG).

Cloud-Dienste und Gesundheitsdaten

Cloud-Dienste werden immer attraktiver – auch im Gesundheitsbereich. Da der Gesundheitsbereich stets die Bearbeitung von besonders schützenswerten Personendaten umfasst, ist beim Einsatz von Cloud-Diensten jedoch eine gewisse Vorsicht geboten. Worauf zu achten ist, wird nachfolgend erläutert.

Was sind Cloud-Dienste?

Cloud-Dienste werden von IT-Unternehmen angeboten und bestehen in der Nutzung von Rechenleistung, Speicherplatz oder Software über das Internet gegen Bezahlung (Bräutigam & Thalhofer: 1194). Der Cloud-Nutzende und der Cloud-Anbietende legen in einem Vertrag fest, welche Leistungen zu welchem Betrag zu erbringen sind.

Aus datenschutzrechtlicher Sicht handelt es sich bei Cloud-Dienstleistungen um sog. Auftragsdatenbearbeitun-

gen. Der Cloud-Anbietende bearbeitet durch das Zurverfügungstellen von Rechenleistung, Speicherplatz oder Software die Daten des Cloud-Nutzenden in dessen Auftrag. Umfassen die Daten des Cloud-Nutzenden Personendaten, findet durch den Cloud-Anbietenden somit eine Bearbeitung von Personendaten statt.

Auftragsdatenbearbeitungen

Auftragsdatenbearbeitungen gestalten sich in der Regel komplex. Nach Art. 10a DSG sind sie zulässig

- soweit der Auftragnehmer die Daten nur so bearbeitet, wie es der Auftraggeber selbst tun dürfte und
- einer Auslagerung der Daten an den Auftragnehmer keine gesetzliche oder vertragliche Geheimhaltungspflicht entgegensteht.

Die erste Voraussetzung bedingt die Klärung, wie der Auftraggeber die Personendaten selbst bearbeiten darf. Dies ergibt sich aus dem auf den Auftraggeber anwendbaren Datenschutzgesetz sowie allfälligen für ihn geltende bereichsspezifische Gesetze. Aufgrund der Regelung von Art. 10a DSG darf der Auftragnehmer die Daten nur in Übereinstimmung mit dem auf den Auftraggeber anwendbaren Datenschutzgesetz und allfälligen für diesen geltende bereichsspezifische Gesetze bearbeiten. Der Auftragnehmer kann somit nicht selbst entscheiden, wie er die Daten bearbeiten möchte. Gleichzeitig bleibt der Auftraggeber dafür verantwortlich, dass der Auftragnehmer sich an diese Vorgabe hält. Diese Verantwortung lässt sich am zielführendsten durch eine vertragliche Vereinbarung wahrnehmen.

Bei der zweiten Voraussetzung gilt es zu prüfen, ob der Auftraggeber einer Geheimhaltungspflicht unterliegt, die einer Auslagerung der Datenbearbeitung an einen Dritten entgegenstehen könnte. Diese Frage lässt sich stets nur mit Blick auf den konkreten Einzelfall beantworten.

Vertragliche Regelung von Cloud-Diensten

Für die Ausgestaltung der oben genannten vertraglichen Regelung zwischen dem Cloud-Anbietenden und dem Cloud-Nutzenden gelten insbesondere bei Bearbeitungen, die besonders schützenswerte Personendaten umfassen, erhöhte Anforderungen. In diesen Fällen ist es besonders wichtig, durch vertragliche Regelung sicherzustellen, dass der Cloud-Anbietende die Daten, wie von Art. 10a DSG gefordert, nur so bearbeitet, wie es der Cloud-Nutzende selbst tun dürfte. Insbesondere mit grossen Cloud-Anbietenden, die über eine gewisse Marktmacht verfügen und standardisierte Cloud-Dienstleistungen anbieten, wird es bedingt möglich sein, individuelle Verträge auszuhandeln

(Bergt: 45). Oft besteht bei diesen Angeboten auch wenig Transparenz darüber, wo die Server, auf denen die Dienstleistungen erbracht werden, ihren Standort haben. In entsprechenden Fällen lohnt es sich, auf kleinere Cloud-Anbietende auszuweichen. Mit diesen lassen sich in der Regel individuelle Vereinbarungen abschliessen.

Mit Blick auf den Vertragsinhalt gilt es bei Cloud-Nutzungen, die besonders schützenswerte Personendaten wie z. B. Gesundheitsdaten umfassen, insbesondere folgende Punkte zu beachten: Der Cloud-Anbietende sollte verpflichtet werden, die Daten nur auf Servern mit Standort in der Schweiz zu speichern und die Serverstandorte nicht ohne Vorinformation des Cloud-Nutzenden ins Ausland zu verlegen. Der Cloud-Anbietende sollte nur nach schriftlicher Einwilligung des Cloud-Nutzenden berechtigt sein, Subunternehmer beizuziehen (Bergt: 43). Im Weiteren sollte die Anwendbarkeit von schweizerischem Recht und ein schweizerischer Gerichtsstand vereinbart werden. Dies erleichtert im Streitfall die Rechtsdurchsetzung (siehe dazu auch Widmer: 168 ff.).

Anzumerken ist, dass die Datenschutzgesetzgebung Verträgen mit ausländischen Cloud-Anbietenden und/oder Serverstandorten im Ausland und/oder der Vereinbarung eines ausländischen Gerichtsstands oder der Anwendung von ausländischem Recht auch bei besonders schützenswerten Personendaten nicht entgegensteht. Jedoch ist es bei einer entsprechenden Sachlage bedeutend schwieriger, sicherzustellen, dass der Cloud-Anbietende die Daten nur so bearbeitet, wie es der Cloud-Nutzende selbst tun dürfte und auch die Rechtsdurchsetzung gestaltet sich bei einem Gerichtsstand im Ausland schwieriger. Jedenfalls muss sich der Cloud-Nutzende bewusst sein, dass er stets dafür verantwortlich bleibt, dass der Cloud-Anbietende die Daten nur so bearbeitet, wie er es selbst tun dürfte.

Anonymisierung von Personendaten

Die Digitalisierung hat dazu geführt, dass grosse Datenmengen gesammelt, gespeichert und miteinander verknüpft werden können (Stichwort Big Data). Dies erschwert die Anonymisierung von Personendaten erheblich. Nachfolgend wird aufgezeigt, was es in diesem Zusammenhang zu beachten gilt.

Begriff der Anonymisierung

Die Datenschutzgesetzgebung definiert den Begriff der Anonymisierung nicht. Allerdings finden sich Hinweise in den Materialien zur Datenschutzgesetzgebung. Die Botschaft zum Entwurf des neuen Datenschutzgesetzes des Bundes hält fest, eine Anonymisierung von Personendaten setze voraus, dass eine Reidentifizierung durch Dritte unmöglich sei oder eine solche nur mit einem hohen Aufwand, den kein/e InteressentIn auf sich nehmen würde, möglich wäre (Schweizerischer Bundesrat 2017: 7019). Aus der Rechtsprechung des europäischen Gerichtshofs ergibt sich, dass ein hoher Aufwand im vorgenannten Sinne dann vorliegt, wenn die Reidentifizierung den Einsatz enormer zeitlicher und finanzieller Ressourcen sowie den Einsatz von erheblichem Fachwissen bedingt (Urteil vom 19.10.2016, Breyer, C-582/14, EU:C:2016:779, Rn. 46).

Gefahr vermeintlicher Anonymisierung

Eine verbreitete Gefahr im Zusammenhang mit der Anonymisierung von Personendaten liegt darin, dass die Daten nur vermeintlich anonymisiert sind. Dies ist insbesondere in den folgenden zwei Fällen gegeben:

- Rückschlüsse sind aus dem Kontext möglich: Personendaten stehen regelmässig im Kontext mit anderen Daten. Sollen diese anonymisiert werden, besteht die Gefahr, dass sich aus den Informationen im Kontext dieser Personendaten Rückschlüsse auf die betroffenen Personen ziehen lassen. Dabei muss sich ein solcher Rückschluss nicht aus den Kontextdaten alleine ergeben. Vielmehr kann ein solcher auch durch eine Kombination der Kontextdaten mit weiteren Datenquellen entstehen (z. B. durch den Einsatz von Google, Recherchen in öffentlichen Registern wie dem Handels- oder Grundbuchregister oder Recherchen in den sozialen Medien). Da sich kaum feststellen lässt, welche anderen Quellen ausserhalb des ursprünglichen Datensatzes vorhanden sind, die in Kombination mit den Kontextdaten zu einem Rückschluss auf die betroffenen Personen führen kön-

nen, gestalten sich Anonymisierungen zunehmend schwierig.
- Daten sind pseudonymisiert: Als anonymisiert geglaubte Daten sind bei genauerer Betrachtung oft nur pseudonymisiert. Pseudonymisierte Daten liegen vor, wenn der Personenbezug (z. B. Name, Adresse) durch ein Kennzeichen ersetzt wird, mit der Absicht, die Bestimmung der betroffenen Personen auszuschliessen oder wesentlich zu erschweren. Solche Kennzeichen stellen z. B. Kundennummern oder die AHV-Nummer dar. Personen, die den Zuordnungsschlüssel nicht kennen, können aus diesen Nummern nicht ohne weiteres auf die damit verbundenen Personen schliessen.

Bei pseudonymisierten Daten besteht somit stets eine Zuordnungsregel, mit welcher die Kenner der Regel einen Personenbezug herstellen können. Für Personen, die Zugriff auf die Zuordnungsregel haben, handelt es sich somit auch im Fall von pseudonymisierten Daten stets um Personendaten. Inwiefern es sich für Personen, die keinen Zugriff auf die Zuordnungsregel haben, um pseudonymisierte Daten handelt, hängt wesentlich von der Qualität der Massnahmen ab, die zum Schutz der Zuordnungsregel vor unbefugter Kenntnisnahme getroffen wurden. Je einfacher sich ein Zugang zu einer Zuordnungsregel erreichen lässt, desto weniger lässt sich von pseudonymisierten Daten sprechen.

Fazit

Wie in allen Bereichen schreitet die Digitalisierung auch im Gesundheitswesen stetig voran. Gesundheitsdaten werden immer häufiger im Rahmen digitaler Angebote bearbeitet – so z. B. im Rahmen des elektronischen Patientendossiers, von datenverarbeitenden Medizinprodukten, Lifestyle- und Wellbeing-Apps, Onlineberatungsplattformen oder von Bots zu Therapiezwecken.

Diese neuen Arten der Datenverarbeitung sind durchaus zu begrüssen. Sie führen jedoch dazu, dass dem Datenschutz eine erhöhte Aufmerksamkeit zukommen muss. Diese Einsicht ist in vielen Bereichen – auch im Gesundheitsbereich – erst bedingt angekommen. Es wird noch viel Aufklärungsarbeit und Umdenken notwendig sein, bis sich die Digitalisierung und der Datenschutz im Gesundheitsbereich in angemessenem Verhältnis gefunden haben. Insbesondere im Gesundheitsbereich liegt ein hohes Datenschutzniveau jedoch im Interesse aller: Denn jeder und jede ist früher oder später in der eigenen Person auf den Gesundheitsbereich angewiesen...

Literatur

Bergt, Matthias (2013): Vertragsgestaltung und Kontrolle bei Auftragsdatenverarbeitung. S. 37-51 in: Jürgen Taeger (Hrsg.), Law as a service (LaaS) – Recht im Internet- und Cloud-Zeitalter. Tagungsband Herbstakademie. Band 1. Oldenburg: OLWIR. www.tinyurl.com/y3o4n6rq, Zugriff 06.03.2019.

Maurer-Lambrou, Urs/Blechta, Gabor (Hrsg.) (2014): Datenschutzgesetz (DSG) Öffentlichkeitsgesetz (BGÖ). Basler Kommentar. 3. Auflage. Basel: Helbing-Lichtenhahn Verlag.

Schweizerischer Bundesrat (2017): Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.09.2017. BBl 2017: 6941-7192. www.tinyurl.com/yyypefer, Zugriff 27.02.19.

Talhofer, Thomas/Bräutigam, Peter (2013): Cloud-Computing. S. 1191-1275 in: Peter Bräutigam (Hrsg.), IT-Outsourcing und Cloud-Computing. 3. Auflage. Berlin: Erich Schmidt Verlag.

Widmer, Barbara (2014): Auftragsdatenbearbeitung – zum Vierten. Digma: 168-180.

Endnoten

[1] Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992, SR 235.1. Dieses Gesetz befindet sich zurzeit in Totalrevision. Wann diese beendet sein wird, lässt sich schwer voraussagen. Gestützt auf den Entwurf der Totalrevision ist jedoch davon auszugehen, dass die im vorliegenden Beitrag gemachten Aussagen nach der Revision unverändert Gültigkeit haben. Aus Gründen der Leserlichkeit wird darauf verzichtet, jeweils auch die Artikel des Entwurfs anzugeben. Interessierte LeserInnen finden diesen unter www.tinyurl.com/yd5s3agg (Gesetzestext ab Seite 7206).

[2] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119/1 vom 04.05.2016.