1 Stellenwert und Aktualität des Datenschutzes

Thomas Jäschke und Nina Richard

Das Thema Datenschutz hat bereits 2013 durch die Veröffentlichungen im Zusammenhang mit der weltweiten Überwachung der NSA und ihrer Partnerdienste einen erheblichen Aufschwung im öffentlichen Interesse erhalten. Aber nicht erst seit diesen Veröffentlichungen spielt der Datenschutz in Deutschland eine große Rolle. So wurde im Jahr 1970 in Hessen das erste Datenschutzgesetz weltweit beschlossen. Nach und nach zogen die anderen Bundesländer und der Bund nach. Insbesondere durch die immer weiter voranschreitenden Möglichkeiten der automatisierten Verarbeitung von Daten in dieser Zeit wurde ein Korrektiv benötigt, um insbesondere den Möglichkeiten der sogenannten Rasterfahndung im Zusammenhang mit der Roten Armee Fraktion (RAF) entgegenzutreten, bzw. diese in einen geordneten Rahmen einzubetten. Den Höhepunkt der Regulierung fand der Datenschutz im Volkszählungsurteil von 1983, bei dem das Bundesverfassungsgericht das Bürgerrecht der informationellen Selbstbestimmung aus Art. 2 i.V.m. Art. 1 Grundgesetz ableitete.

Dieses Recht findet sich mittlerweile in ähnlicher Weise in der Magna Charta der Europäischen Union wieder und wird regelmäßig gegen die Bestrebungen einzelner Staaten und der EU Kommission durch die höchsten Gerichte verteidigt. Die Wichtigkeit des Datenschutzes in Europa spiegelt sich auch in den Bemühungen wider, den Datenschutz in der EU in einem europäischen Gesetz zu verankern. Die Verhandlungen hierzu gestalteten sich, begründet durch die unterschiedlichen Interessenlagen, allerdings schwierig. Und so trat die neue Europäische Grundverordnung am 24.05.2016 in Kraft und ist ab dem 25.05.2018 anzuwenden.

Die Datenschutzgrundverordnung gilt unmittelbar für alle EU-Mitgliedsstaaten und fordert vielzählige Anpassungen der Gesetze auf Bund und Länderebene, ebenso wie bei speziellen Datenschutzgesetzen.

Das Konzept des Datenschutzes ist allerdings keine Erfindung der jüngeren Geschichte, auch wenn es der Begriff und die weite Ausdehnung des Zuständigkeitsbereichs sind. So gaben sich schon in der Antike Berufsgruppen wie Ärzte, Juristen oder Priester einen Berufskodex, der ihnen eine Verschwiegenheitspflicht, der ihnen anvertrauten Tatsachen, auferlegte. Diese erstreckt sich auch auf die Pflicht, diese Geheimnisse gegen den Eingriff des Staates und seiner Institutionen zu verteidigen. Der deutsche Gesetzgeber hat dieses berufliche Ethos auch schon in der ersten Version des Strafgesetzbuches von 1871, das ein Zuwiderhandeln unter Strafe stellt, sowie in der Strafprozessordnung mit dem Zeugnisverweigerungsrecht berücksichtigt.

Wie bereits beschrieben erhielt der Datenschutz seinen ersten Antrieb durch die neuen technischen Möglichkeiten in den 70er-Jahren des vergangenen Jahrhunderts. Ein solcher Schub ist derzeit ebenfalls erkennbar. So bietet sich in den letzten Jahren nicht mehr nur für Organisationen mit großen IT-Budgets die Möglichkeit, ihre Daten immer besser zu analysieren, um daraus Maßnahmen für die strategische Unternehmenssteuerung abzuleiten. Die Techniken dafür werden immer ausgereifter und die Speicherung von großen Datenmengen, die immer mehr auf Verdacht erzeugt werden, wird immer günstiger. Das Prinzip Hoffnung führt zu den Gedanken, zu einem späteren Zeitpunkt Mittel und Wege zu finden, diese Daten gewinnbringend auszuwerten. So soll die NSA jegliche verschlüsselte Kommunikation im Internet speichern, weil sie davon ausgeht, dass die eingesetzten Verschlüsselungsverfahren zu entschlüsseln sind und es zukünftig neue technische Möglichkeiten gibt, mit denen die eingesetzten Sicherheitsmechanismen wesentlich schneller ausgehebelt werden können.

An dieser Stelle setzt der Datenschutz an. Dieser kann zwar das Voranschreiten der Technik nicht verhindern und will es auch nicht. Der hierbei verfolgte Ansatz geht in die Richtung, dass die Institutionen nur die Daten erheben und speichern dürfen, die sie wirklich benötigen, und diese Daten zu löschen sind, sobald sie für den ursprünglichen Zweck nicht mehr benötigt werden. Außerdem wird auf einen informierten Bürger gesetzt, der auf Grundlage aller Informationen selbst entscheiden kann, was mit seinen Daten geschehen soll und darf. Klingt dieses Grundprinzip auch so einfach, umso schwerer gelingt die Umsetzung dieser Anforderung. Das hat verschiedene Ursachen. Im Vordergrund steht der Gedanke einer Selbstregulierung, bei der die Unternehmen durch Hinzunahme der betrieblichen Datenschutzbeauftragte die Rechtmäßigkeit der Datenverarbeitung und -speicherung grundsätzlich prüfen und bewerten sowie die dazu notwendigen technischen und organisatorischen Maßnahmen umsetzen. In der Realität werden die Datenschutzbeauftragten jedoch oft nicht in Entscheidungsprozesse eingebunden und können nicht regulierend oder unterstützend eingreifen. Die Datenschutzbehörden sind nicht mit genügend Personal ausgestattet, sodass diese ihre Aufgaben proaktiv wahrnehmen könnten.

Ein anderer Grund, der in der Öffentlichkeit oft genannt wird, ist das mangelnde Interesse der Bevölkerung am Thema Datenschutz. Datenschutz wird dabei oft als sehr sperrig oder behindernd empfunden, was sich insbesondere in den umfangreichen und verklausulierten Datenschutzerklärungen von Diensten und Internetseiten begründet. Andererseits sind für viele Bürger der Preis und Komfort die entscheiden-

den Kriterien für die Entscheidungsfindung bei Dienstleistungen oder Angeboten im Internet. Der letzte Punkt bezieht sich auf die Handhabbarkeit technischer Lösungen, mit denen die Nutzer sich selbst schützen können. So ist es sicherheitsaffinen Technikern in den letzten 20 Jahren nicht gelungen eine Lösung zu entwerfen, die zum einen sicher ist und zum anderen ergonomisch so gestaltet sind, dass sie in der breiten Masse Anklang finden.

Am Ende ist das Thema für den Einzelnen tatsächlich nicht uninteressant, sondern nicht überschaubar. Umso wichtiger ist es für Unternehmen, und Institutionen im Gesundheitswesen ganz besonders, das Vertrauen der Bürger, Patienten, Versicherten, Bewohner, Gäste und Kunden, nicht zu enttäuschen, sondern durch geeignete und angemessene Maßnahmen umzusetzen. Neben der fachlichen Kompetenz sind dies die Grundlage für eine hohe Reputation und auch ein Erfolgsfaktor für den wirtschaftlichen Erfolg.

2 Besonderheiten des Datenschutzes im Gesundheitswesen

Thomas Jäschke und Nina Richard

Das Gesundheitswesen hat, im Vergleich zu anderen Wirtschaftssektoren, einige Besonderheiten. So sind Krankenkassen als auch die Kassenärztlichen Vereinigungen sogenannte Körperschaften des öffentlichen Rechts. Sie sind damit nicht unmittelbar Teil der staatlichen Verwaltung. Der Staat gibt den Körperschaften lediglich den Rahmen vor und führt die Aufsicht.

Die Selbstverwaltung der Krankenkassen wird durch deren Organe Vorstand und Verwaltungsrat ausgeübt. In den kassenärztlichen und kassenzahnärztlichen Vereinigungen wird die Selbstverwaltung von der Vertreterversammlung und dem Vorstand ausgeübt. Im Wesentlichen setzt sich das deutsche Gesundheitswesen aus drei Arten von Akteuren zusammen:

- den Leistungsempfängern,
- den Leistungserbringern und
- den Leistungsträgern.

Die Leistungsempfänger und -träger gaben im Jahr 2015 circa 344 Milliarden Euro für Leistungen der Leistungserbringer aus (Destatis 2015). Das Gesundheitswesen beschäftigte 2015 rund 5,3 Millionen Menschen, was ungefähr jedem achten Angestellten in Deutschland entspricht (Statistisches Bundesamt 2017). Im Jahr 2013 wurden in fast 1.948 Krankenhäusern mit gut 498.666 Betten etwa 19,2 Millionen Patienten vollstationär behandelt. Die Krankenhäuser in Deutschland werden zunehmend privatisiert. Nach aktuellem Stand befinden sich rund 568 in öffentlichem, 674 in freigemeinnützigem 706 in privatwirtschaftlichem Betrieb (Destatis 2014a). Neben den Krankenhäusern gibt es 1.151 Vorsorge- und Rehabilitationseinrichtungen mit rund 164.500 Betten, in denen 2 Millionen Patienten behandelt wurden (Destatis 2014b).

Ergänzt wird das Feld der Leistungserbringer durch 13.000 Pflegeheime und etwas weniger ambulante Pflegedienste. 2015 gab es 2,86 Millionen Pflegebedürftige, Tendenz steigend, von denen rund 783.000 in Pflegeheimen und 692.000 durch ambulante Dienste betreut wurden (Destatis 2017).

Die Seite der Leistungsträger ist in Deutschland von dualer Natur. So gibt es die Gesetzlichen Krankenversicherungen (kurz GKV), denen 72,30% (GKV-Spitzenverband 2015, S. 23) aller Versicherten angehören und deren Aufgaben in der Sozialgesetzgebung, insbesondere im Sozialgesetzbuch Fünftes Buch (SGB V), festgelegt sind, und die privaten Krankenversicherungen (PKV), deren Leistungen individualvertraglich zwischen dem Versicherten und dem Versichernden geregelt werden (Nagel u. Braasch 2007, S. 118). Hinzu kommen die Leistungen wie beispielsweise Individuelle Gesundheitsleistungen (kurz: IGeL-Leistungen) oder rezeptfreie Medikamente, die von den Versicherten selber getragen und somit nicht durch die Kostenträger übernommen werden.

Eine wesentliche Besonderheit des Gesundheitswesens stellen die stark differenzierten Träger der einzelnen Akteure dar, was zu unterschiedlich zu beachtenden Gesetzen führt. Auf der einen Seite sind die privatwirtschaftlichen Teilnehmer zu finden. Zu diesen gehören die nicht-angestellten Ärzte und Apotheker sowie die Versicherer der PKV. Für diese Gruppe ist das Bundesdatenschutzgesetz einschlägig und spielt somit die wichtigste Rolle für Datenschutzregelungen (vgl. § 1 Abs. 2 Punkt 3 BDSG). Zusätzlich gibt es Einrichtungen, für die das Bundesdatenschutzgesetz in Teilen gilt, da die Einrichtungen sich in Trägerschaft eines Bundeslandes befinden und das jeweilige Landesdatenschutzgesetz wettbewerbsrelevante Teile an das Bundesdatenschutzgesetz „delegiert". Diese Regelungen wurden in die Landesdatenschutzgesetze aufgenommen, um den jeweiligen Einrichtungen eine Teilnahme am Wettbewerb zu ermöglichen, ohne zusätzliche Auflagen erfüllen zu müssen, die für ihre Konkurrenz nicht besteht (vgl. z.B. § 2 Abs. 3 NDSG oder § 2 Abs. 2 DSG NRW). Hiervon sind in der Regel kommunale Krankenhäuser und ähnliche Einrichtungen betroffen. Für Unikliniken, die in der Trägerschaft der Länder stehen, gilt dies nicht, da bei diesen nicht von einem Wettbewerb ausgegangen wird. Des Weiteren gibt es im Gesundheitswesen Einrichtungen, die durch religiöse Gemeinschaften betrieben werden. Diese fallen aufgrund des Selbstbestimmungsrechtes der Kirchen in Deutschland (vgl. z.B. BVerfG, 2 BvR 661/12 vom 22.10.2014, Rn. [1–183]) unter die jeweiligen Gesetze der Kirche beziehungsweise der regionalzuständigen Organisationseinheit (beispielsweise einem Bistum in der katholischen Kirche). Neben den entsprechenden primären Datenschutzgesetzen besteht weiterhin die Möglichkeit, dass auf Bundeslandebene noch Gesundheits- oder Krankenhaus(datenschutz)gesetze verabschiedet wurden, die zu berücksichtigen sind. In diesen Fällen wurde auf der kirchlichen Ebene die entsprechende Gesetzesstruktur nachgebildet. Zusätzlich müssen die Sozialdaten von Betroffenen, die Leistungen der Sozialversicherungen beziehen, nach den Regelungen der Sozialgesetzgebung verarbeitet werden. Dies gilt nicht nur für die Gesundheitsdaten der gesetzlichen Versicherten, sondern auch für Daten, die in der Pflege oder der Jugendhilfe erhoben werden. Diese Regeln sind dementsprechend für die GKV auf die von ihr verarbeiteten Daten anzuwenden. Detaillierter wird das Thema in Kapitel II.1 aufbereitet.

In Deutschland gibt es darüber hinaus das Berufsgeheimnis, das sich unter anderem auf Ärzte und Apotheker erstreckt. Dies hat zur Folge, dass eine Auslagerung der Verarbeitung personenbezogener Daten, insofern diese unter das Berufsgeheimnis fallen, nach dem heutigen Stand schwer umsetzbar ist. Die Fragestellungen dazu sind nicht abschließend geklärt. Weiterhin haben die einzelnen Berufsgruppen im Ge-

sundheitswesen eigene Berufsordnungen, die ebenfalls Datenschutzaspekte enthalten, die für den Einzelnen zu berücksichtigen sind.

Im Vergleich zum Datenschutz werden mit den Dokumentationspflichten andere Ziele verfolgt. So ist eines der Grundprinzipien des Datenschutzes die Datenminimierung sowie die Speicherbegrenzung (vgl. Art. 5, 1. (b) und (e)), die verlangt, dass die Verarbeitung von Daten auf ein notwendiges Maß beschränkt wird und personenbezogene Daten nur so lange gespeichert werden dürfen, wie es notwendig ist und diese ggf. gelöscht werden. Diese Vorschrift ist allerdings subsidiär, weshalb die Aufbewahrungsfristen der Löschung vorzuziehen sind. Aus dem technischen Blickwinkel stellt es für viele IT-Systeme ein Problem dar, zum Ende der Aufbewahrungsfrist entsprechende Daten zu löschen. Dies liegt insbesondere darin begründet, dass für viele Datenkategorien unterschiedlichste Aufbewahrungsfristen bestehen, sodass keine generelle technische Regel gefunden werden kann, die besagt, dass alle Daten nach n Jahren gelöscht werden können. Hinzu kommt, dass immer mehr dieser Daten zur Qualitätssicherung ausgewertet werden und in entsprechender Form vorliegen müssen. Außerdem können sich aus dem BGB Schadensersatzansprüche ergeben, die erst nach 30 Jahre verjährt sind (§ 199 Abs. 2 BGB). Eine genaue Aufschlüsselung dieser Problematik findet sich in Kapitel II.3 .

Dokumentationspflichten, Erhebung von Daten zur Abrechnung und der Wunsch nach Forschung und kontinuierlicher Verbesserung der Qualität bei den Leistungserbringern führen zu einer immer umfangreicheren Menge an Daten und das Verlangen diese auszuwerten. Solange diese Daten im Bezug zu einer Person stehen sind die datenschutzrelevanten Gesetze und Regelungen zu beachten. Aktuelle Trends, wie Cloud Computing und Big Data, die in der Industrie einen hohen Stellenwert einnehmen und im Gesundheitswesen verursacht durch den zunehmenden Kostendruck auch großes Interesse wecken, stoßen auf die Herausforderungen personenbezogene Daten zu verarbeiten, die zu anderen Zwecken erhoben wurden und daher gar nicht verwendet werden dürften. Hier ist meistens eine Einzelbewertung unter Berücksichtigung der Verhältnismäßigkeit erforderlich.

Literatur

Destatis (2017) Pressemitteilung. URL: https://www.destatis.de/DE/PresseService/Presse/Pressemitteilungen/2017/01/PD17_017_224.html (abgerufen am 03.04.18)

Destatis (2015) Gesundheitsausgaben nach Ausgabenträgern. Statistisches Bundesamt. URL: https://www.destatis.de/DE/ZahlenFakten/GesellschaftStaat/Gesundheit/Gesundheitsausgaben/Tabellen/Ausgabentraeger.html (abgerufen am 04.09.17)

Destatis (2014a) Gesundheit – Grunddaten der Krankenhäuser. Stand: 02.12.2014. Statistisches Bundesamt. URL: https://www.destatis.de/DE/PresseService/Presse/Pressemitteilungen/2017/08/PD17_276_231.html (abgerufen am 03.04.18)

Destatis (2014b) Gesundheit – Grunddaten der Vorsorge- oder Rehabilitationseinrichtungen. Stand: 02.12.2014. Statistisches Bundesamt. URL: https://www.destatis.de/DE/Publikationen/Thematisch/Gesundheit/VorsorgeRehabilitation/GrunddatenVorsorgeReha2120612157004.pdf?__blob=publicationFile (abgerufen am 03.04.18)

GKV-Spitzenverband (2015) https://www.gkv-spitzenverband.de/media/grafiken/gkv_kennzahlen/kennzahlen_gkv_2017_q1/300dpi_6/GKV-Kennzahlen_MitgliederVersicherte_2017.jpg. Hrsg. von GKV-Spitzenverband Berlin

Nagel E, Braasch P (2007) Das Gesundheitswesen in Deutschland: Struktur, Leistungen, Weiterentwicklung. 4., völlig überarb. und erw. Aufl. Deutscher Ärzte-Verlag Köln

Statistisches Bundesamt (2017) URL: https://www.awo.org/statistisches-bundesamt-beschaeftigte-im-gesundheitswesen-0 (abgerufen am 03.04.18)