Gesundheitsdatenschutz unter der Datenschutz-Grundverordnung

von Prof. Dr. Benedikt Buchner und Simon Schwichtenberg***

Wer gehofft hat, dass die Reform des europäischen Datenschutzrechts auch zu einer Vereinheitlichung des Gesundheitsdatenschutzes führt,[1] wird sich angesichts der Regelungen der Datenschutz-Grundverordnung (DSGVO)[2] enttäuscht sehen. Die Vielzahl von Öffnungsklauseln, die die DSGVO zugunsten mitgliedstaatlicher Regelungen vorsieht, lässt ein einheitliches europäisches Datenschutzrecht in vielen Bereichen – und so auch im Gesundheitsbereich – in weite Ferne rücken. Darüber hinaus lässt der weite Regelungsspielraum, der den Mitgliedstaaten unter der DSGVO verbleibt, auch kaum erwarten, dass der Gesetzgeber im nationalen Rahmen die DSGVO zum Anlass für eine umfassendere Novellierung nehmen wird, die den Gesundheitsdatenschutz in einen konsistenteren und transparenteren Regelungsrahmen überführen würde.

* Prof. Dr. Benedikt Buchner LL.M. (UCLA), Institut für Informations-, Gesundheits- und Medizinrecht (IGMR), Universität Bremen.

** Simon Schwichtenberg, wissenschaftlicher Mitarbeiter am IGMR.

1 Ausführlich zur Reformbedürftigkeit des Gesundheitsdatenschutzrechts *Kingreen/Kühling* (Hrsg.), Gesundheitsdatenschutzrecht (2015); speziell für den Bereich E-Health, DuD 2013, 791 ff.

2 Verordnung (EU) 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

A. Zum Regelungscharakter der DSGVO

Mit dem Instrument der Verordnung möchte der europäische Gesetzgeber an sich erreichen, was ihm nach eigenem Dafürhalten mit der Datenschutz-Richtlinie (DSRL) nicht gelungen ist: eine einheitliche Handhabung des Datenschutzes in der Union, Rechtssicherheit sowie eine öffentliche Wahrnehmung, dass gerade auch im Internet Datenschutz konsequent gewährleistet ist.[3] Eben deshalb soll eine Verordnung erforderlich sein, die anders als die bisherige Datenschutz-Richtlinie den Mitgliedstaaten keinen Umsetzungsspielraum mehr belässt, sondern in allen ihren Teilen verbindlich ist und unmittelbar in jedem Mitgliedstaat gilt (Art. 288 AEUV).

Dass die DSGVO im Vergleich zur bisherigen DSRL tatsächlich mehr Harmonisierungskraft entfalten wird, ist jedoch in vielerlei Hinsicht zweifelhaft. Die Verordnung räumt mit ihren Öffnungsklauseln den Mitgliedstaaten weitreichende Möglichkeiten ein, Ausnahmen, Beschränkungen, Konkretisierungen u.Ä. im einzelstaatlichen Recht zu normieren. Angesichts von mehr als 70 Öffnungsklauseln ist die DSGVO daher eher als ein „atypisches Hybrid aus Verordnung und Richtlinie"[4] einzuordnen. Vor allem für die Verarbeitung von Daten im öffentlichen Interesse bzw. in Ausübung öffentlicher Gewalt eröffnet die DSGVO in Art. 6[5] dem nationalen Gesetzgeber einen erheblichen Regelungsspielraum. Nicht geringer fällt der Regelungsspielraum aber auch für den Bereich des Gesundheitsdatenschutzes aus. Art. 9 Abs. 2 lit. h erlaubt mitgliedstaatliche Regelungen zur Verarbeitung „für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich". Art. 9 Abs. 2 lit. i erlaubt darüber hinaus mitgliedstaatliche Regelungen zur Verarbeitung „aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten". Und Art. 9 Abs. 4 räumt schließlich den Mitgliedstaaten nochmals ausdrücklich die Befugnis ein, weitere Voraussetzungen und Beschränkungen bei der Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten zu normieren.[6]

B. Gesundheitsdatenschutz unter der DSGVO

Der Gesundheitsdatenschutz hierzulande fußt zunächst einmal auf dem klassischen allgemeinen Datenschutzrecht (dazu sogleich I.) sowie den bereichsspezifischen Regelungen, zu denen insbesondere die Landeskrankenhausgesetze zählen (dazu II.). Daneben sind für die Datenverarbeitung im Gesundheitswesen der Sozialdatenschutz (unten III.) und die ärztliche Schweigepflicht (unten IV.) bedeutsam. Für jeden Bereich stellt sich die Frage, ob und welche Änderungen und Ergänzungen die DSGVO mit sich bringen wird.

I. Allgemeines Datenschutzrecht

Zum allgemeinen Datenschutzrecht in Deutschland zählen das BDSG sowie die 16 Landesdatenschutzgesetze. Modifiziert und ergänzt werden deren Regelungen durch vorrangige bereichsspezifische Regelungen zum Gesundheitsdatenschutz. Dieses Zusammenspiel zwischen allgemeinem und besonderem Datenschutzrecht wird sich auch unter der DSGVO fortsetzen. Dabei werden allgemeine Regelungsprinzipien wie das Verbotsprinzip mit Erlaubnisvorbehalt (1), der besondere Schutz sensibler Gesundheitsdaten (2), die Einwilligung und die Vertragserfüllung als Erlaubnistatbestand (3 und 4) sowie die Betroffenenrechte (5) auch künftig in erster Linie im allgemeinen Datenschutzrecht verortet sein.

1. Verbotsprinzip mit Erlaubnisvorbehalt

Schon die DSRL hat den Mitgliedstaaten aufgegeben, eine Datenverarbeitung nur dann zuzulassen, wenn eine der in Art. 7 DSRL abschließend bestimmten Voraussetzungen erfüllt ist. Entsprechend ist sowohl im BDSG als auch in den Landesdatenschutzgesetzen jeweils das sog. Verbotsprinzip mit Erlaubnisvorbehalt normiert.[7] Auch Art. 6 Abs. 1 nimmt dieses Grundprinzip auf und gibt vor, dass eine Verarbeitung personenbezogener Daten nur dann rechtmäßig ist, wenn eine der in Art. 6 Abs. 1 abschließend aufgezählten Bedingungen (Einwilligung oder sonstiger, gesetzlich normierter Erlaubnistatbestand) erfüllt ist.

Die Fortgeltung des Verbotsprinzips auch unter der DSGVO war von Anfang an nicht unumstritten, letztlich aber schon deshalb ohne Alternative, weil sich eine Abkehr vom Verbotsprinzip kaum mit Art. 8 GRCh vereinbaren ließe. Nach Art. 8 Abs. 2 GRCh bedarf jede Verarbeitung personenbezogener Daten einer Einwilligung der betroffenen Person oder einer gesetzlichen Legitimation. Ausgangspunkt des Art. 8 GRCh ist, „dass der Einzelne grundsätzlich selbst Herr seiner Daten sein soll".[8] Realistisch ist dies nur, wenn zumindest im Ausgangspunkt nicht das Prinzip der Verarbeitungsfreiheit, sondern das des Verarbeitungsverbots gilt.[9] Grundsätzlich ist und bleibt daher auch künftig eine Verarbeitung personenbezogener Daten zunächst

3 Erwägungsgrund (EG) 7 der Verordnung.

4 *Kühling/Martini*, EuZW 2016, 448 (449); die Rede ist insoweit auch von europarechtlichem „Neuland" (*Pötters*, RDV 2015, 10 (11)).

5 Alle Art. sowie EG im Folgenden ohne Gesetzesbezeichnung sind solche der DSGVO.

6 Zu berücksichtigen ist zudem, dass die DSGVO gemäß Art. 2 Abs. 2 lit. d keine Anwendung auf die Datenverarbeitung bei Polizei und Justiz im Zusammenhang mit Straftaten findet. Doch auch die Polizei und Justiz verarbeiten Gesundheitsdaten. Insoweit gilt dann die „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates". Die Richtlinie sieht eigene, allerdings der DSGVO ähnelnde, Vorgaben vor, die die Mitgliedstaaten im nationalen Recht umzusetzen haben (für die Verarbeitung von Gesundheitsdaten s. insb. deren Art. 10).

7 § 4 Abs. 1 BDSG; für die Landesdatenschutzgesetze s. beispielhaft § 3 Abs. 1 BremDSG, Art. 15 Abs. 1 BayDSG.

8 *Frenz*, Handbuch Europarecht, Bd. 4, Rn. 1380; ähnlich *Streinz/Michl*, EuZW 2011, 384 (385).

9 Zur Drittwirkung des Art. 8 GRCh als „selbstverständliche Reaktion" auf die globale Marktmacht von Unternehmen siehe *von Danwitz*, DuD 2015, 581 (585).

einmal unzulässig, es sei denn, die von der Datenverarbeitung betroffene Person hat in diese wirksam eingewilligt oder die Datenverarbeitung lässt sich auf einen der sonstigen gesetzlichen Erlaubnistatbestände stützen.

2. Besonderer Schutz sensibler Daten

Bereits aus dem bisherigen Datenschutzrecht bekannt ist auch die grundsätzliche Unterscheidung zwischen „normalen" und besonders sensiblen Daten (sog. besondere Kategorien personenbezogener Daten).[10] Zu diesen besonderen Kategorien personenbezogener Daten zählen nach Art. 9 Abs. 1 u.a. Gesundheitsdaten, aber auch genetische und biometrische Daten sowie Daten zum Sexualleben oder der sexuellen Orientierung. All diese Daten werden unter der DSGVO als besonders schutzwürdig eingeordnet und daher nochmals eigenen, strengeren Regelungen unterstellt.[11] Ergänzt wurde die Auflistung im Vergleich zum BDSG und zur DSRL dabei um die Kategorien der biometrischen und genetischen Daten. Damit ist die bisherige Frage, inwieweit sich genetische Daten unter den Begriff des Gesundheitsdatums fassen lassen,[12] dahingehend geklärt, dass genetische Daten zwar grundsätzlich keine Gesundheitsdaten, aber dennoch nicht weniger schutzwürdig sind.

Sollen Gesundheitsdaten (oder andere „besondere" personenbezogene Daten) verarbeitet werden, gilt auch insoweit im Ausgangspunkt das Verbotsprinzip, das noch einmal speziell für besondere Kategorien personenbezogener Daten in Art. 9 normiert ist. Nach Art. 9 Abs. 1 ist eine Verarbeitung von Gesundheitsdaten zunächst einmal „untersagt", Art. 9 Abs. 2 zählt sodann aber diverse Fallkonstellationen auf, in denen dieses Verbot nicht gilt. Um dem besonderen Schutzbedürfnis dieser sensiblen Daten gerecht zu werden, stellt Art. 9 Abs. 2 dabei im Vergleich zu Art. 6 Abs. 1 erhöhte Anforderungen an die Zulässigkeit ihrer Verarbeitung – ebenso wie bislang etwa auch das BDSG in den §§ 13 Abs. 2, 14 Abs. 2, 28 Abs. 6 ff. und 29 Abs. 5 BDSG solche erhöhten Anforderungen normiert.

Ein weitergehender Schutz von besonders schutzwürdigen Daten wie Gesundheitsdaten ist über Art. 9 hinaus auch noch an anderen Stellen in der DSGVO vorgesehen. Dies gilt etwa für den Zweckbindungsgrundsatz nach Art. 5 Abs. 1 lit. b, der nach Art. 6 Abs. 4 lit. c gerade bei der Verarbeitung von sensiblen Daten eine besondere Berücksichtigung erfahren soll. Auch die Ausnahmen vom Verbot der automatisierten Einzelentscheidung nach Art. 22 werden für den Fall, dass besondere Kategorien personenbezogener Daten verarbeitet werden, nochmals enger gezogen (Art. 22 Abs. 4). Weitere gesonderte Regeln zu sensiblen Daten finden sich in Art. 30 Abs. 5 (Pflicht zur Erstellung eines Verarbeitungsverzeichnisses), in Art. 35 Abs. 3 lit. b (Erforderlichkeit einer Datenschutzfolgenabschätzung) und in Art. 37 Abs. 1 lit. c (Pflicht zur Benennung eines Datenschutzbeauftragten).

3. Einwilligung

Der Einwilligung kommt als datenschutzrechtlicher Erlaubnistatbestand im Gesundheitswesen seit jeher eine zentrale Bedeutung zu. Auch unter der DSGVO wird sich daran nichts ändern. Ebenso wie Art. 6 Abs. 1 für die Verarbeitung „normaler" Daten die Einwilligung als allerersten Erlaubnistatbestand anführt, setzt auch Art. 9 Abs. 2 in dem Katalog möglicher Erlaubnistatbestände für eine Verarbeitung besonderer Kategorien die Einwilligung der betroffenen Person in lit. a an die erste Stelle. Um wirksam zu sein, muss die Einwilligung zunächst einmal die allgemeinen Wirksamkeitsvoraussetzungen erfüllen, wie sie für jede Einwilligung gelten, und darüber hinaus nach Art. 9 Abs. 1 lit. a auch noch „ausdrücklich" erfolgen.

Die Bedingungen für eine Einwilligung sind ausweislich der Überschrift in Art. 7 normiert, jedoch sind die Regelungen dort weder abschließend noch sonderlich konsistent.[13] Tatsächlich spricht Art. 7 lediglich einige wenige Aspekte der Einwilligung an und erst in der Zusammenschau mit Art. 4 Nr. 11, Art. 6 Abs. 1 lit. a sowie den Erwägungsgründen ergibt sich ein vollständiges Bild, wie der Erlaubnistatbestand der Einwilligung unter der DSGVO rechtlich ausgestaltet ist und welche Voraussetzungen für die Wirksamkeit einer Einwilligung erfüllt sein müssen. Neben der Informiertheit und der Bestimmtheit jeder Einwilligung sind als Wirksamkeitsvoraussetzungen insbesondere die Freiwilligkeit (a), die Ausdrücklichkeit (b) und die Einwilligungsfähigkeit der betroffenen Person (c) zu berücksichtigen.[14]

a) Freiwilligkeit der Einwilligung

Zentrale Wirksamkeitsvoraussetzung für eine Einwilligung ist deren Freiwilligkeit. Für die DSGVO findet sich diese Voraussetzung in der Definitionsnorm des Art. 4 Nr. 11, welche die Einwilligung als eine Erklärung definiert, die „freiwillig" abgegeben werden muss. Auch nach der DSGVO kann die Einwilligung mithin nur eine Legitimationsgrundlage für die Verarbeitung personenbezogener Daten sein, wenn sich die betroffene Person bei ihrer Erklärung nicht in einer Zwangssituation befunden hat. Von einer faktischen Zwangssituation ist nach den Maßstäben der DSGVO dann auszugehen, wenn zwischen der betroffenen Person und dem Datenverarbeiter ein „klares Ungleichgewicht" besteht und es daher „in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist", dass die Einwilligung freiwillig erteilt worden ist (EG 43).[15]

Die Maßstäbe der DSGVO entsprechen damit dem bisherigen Verständnis von Freiwilligkeit. Das BVerfG hat in seiner Rechtsprechung zur Wirksamkeit von Schweigepflichtentbindungsklauseln klargestellt, dass in Konstellationen, in denen zwischen den Beteiligten ein „erhebliches Verhandlungsungleichgewicht" besteht, die Erteilung einer Einwilligung nicht mehr als Ausdruck einer freien und selbstbestimmten Entscheidung der betroffenen Person über den Umgang mit ihren personenbezogenen Daten gewertet werden kann. Ist eine Einwilligung „praktisch nicht verhandelbar" und verlangt sie von der einzelnen betroffenen

10 Vgl. Art. 8 DSRL und für das bisherige nationale Datenschutzrecht § 3 Abs. 9 BDSG sowie – beispielhaft – § 3 Abs. 3 BremDSG und Art. 15 Abs. 7 BayDSG.
11 EG 51.
12 Siehe dazu *Simitis*, in: Simitis, BDSG, 8. Aufl. 2014, § 3 Rn. 259.
13 Vgl. auch *Gierschmann*, ZD 2016, 51 (54).
14 Zu den Voraussetzungen einer wirksamen Einwilligung nach der DSGVO siehe auch *Schantz*, NJW 2016, 1841 (1844).
15 Kritisch dazu *Schantz*, NJW 2016, 1841 (1844).

Person in zu weitgehendem Umfang ein Einverständnis in die Verarbeitung seiner personenbezogenen Daten, ist diese kein wirksamer Erlaubnistatbestand mehr.[16] Ob die Einwilligung eine Datenverarbeitung legitimieren kann, ist daher auch künftig und insbesondere bei der Verarbeitung von Gesundheitsdaten mit Augenmaß zu beurteilen. Zweifel an der Freiwilligkeit können sich etwa in Notfallsituationen stellen, aber auch in unterversorgten ländlichen Gebieten oder bei der Inanspruchnahme besonders spezialisierter Fachärzte. Oftmals wird sich die betroffene Person hier zumindest subjektiv in einer Zwangslage fühlen, so dass sie nicht mehr frei und selbstbestimmt über das Ob und Wie einer Datenverarbeitung zu entscheiden vermag.[17]

b) Ausdrücklichkeit der Einwilligung

Dass – über die allgemeinen Wirksamkeitsvoraussetzungen hinaus – die Einwilligung im Fall der Verarbeitung besonders schutzwürdiger Daten ausdrücklich erteilt werden muss, sieht auch bislang schon das BDSG (entsprechend den Vorgaben der DSRL)[18] vor.[19] Soll die Verarbeitung von Gesundheitsdaten mit einer Einwilligung legitimiert werden, muss sich diese Einwilligung ausdrücklich auch auf diese Gesundheitsdaten beziehen, diese Daten müssen in der Einwilligung also explizit genannt werden.[20] Für die DSGVO gilt nichts anderes, da diese den Begriff der Ausdrücklichkeit ohne Änderung aus der DSRL übernommen hat. Um den eindeutigen Bezug der Einwilligung auf die Gesundheitsdaten sicherzustellen und zudem auch der Nachweispflicht des Art. 7 Abs. 1 nachzukommen, empfiehlt es sich, im Gesundheitsbereich auch zukünftig auf eine schriftliche Einwilligung zu setzen, auch wenn die DSGVO, anders als bislang das BDSG[21], die Schriftform der Einwilligung grundsätzlich nicht für deren Wirksamkeit voraussetzt.[22]

c) Einwilligung durch Minderjährige

Bislang gilt, dass es für die Erteilung einer wirksamen Einwilligung keiner Geschäftsfähigkeit im Sinne der bürgerlich-rechtlichen Vorschriften bedarf. Auch Minderjährige können wirksam in eine Datenpreisgabe einwilligen oder den Arzt von der Schweigepflicht entbinden, wenn sie die entsprechende Einsichtsfähigkeit haben. Letzteres wiederum muss einzelfallbezogen beurteilt werden und hängt von der Fähigkeit des Minderjährigen zu selbständigem und verantwortungsbewusstem Handeln ebenso ab wie von Art und Zweck der konkreten Datenpreisgabe.[23] An der Rechtsunsicherheit, die damit gerade auch für Ärzte und Gesundheitseinrichtungen einhergeht, wird sich unter der DSGVO nichts ändern. Zwar führt Art. 8 Abs. 1 abweichend von den dargestellten Grundsätzen eine bestimmte Altersgrenze ein, die für die Annahme der Einsichts- bzw. Einwilligungsfähigkeit eines Minderjährigen ausschlaggebend sein soll. Diese starre Altersgrenze gilt allerdings nur für Konstellationen, in denen einem Minderjährigen sog. Dienste der Informationsgesellschaft angeboten werden; hier geht Art. 8 Abs. 1 von einer Einsichtsfähigkeit des Minderjährigen ab Vollendung des 16. Lebensjahres aus. Für den Gesundheitsbereich ist diese Konstellation im Behandlungsalltag allerdings ohne Relevanz.

4. Vertrag mit einem Angehörigen eines Gesundheitsberufs

Grundidee des allgemeinen Datenschutzrechts ist, dass eine Datenverarbeitung stets auch insoweit erlaubt ist, als diese im Rahmen eines vertraglichen Schuldverhältnisses erforderlich ist. Schon das bisherige Datenschutzrecht sah einen Erlaubnistatbestand für die Datenverarbeitung zur Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses vor.[24] Eben ein solcher Erlaubnistatbestand findet sich künftig auch in der DSGVO in Art. 6 Abs. 1 lit. b. Normiert wird damit zunächst einmal eine Selbstverständlichkeit: Stets muss eine Verarbeitung solcher Daten zulässig sein, ohne deren Kenntnis die datenverarbeitende Stelle ein vertragliches Schuldverhältnis überhaupt nicht durchführen könnte. Diese Grundidee wird auch für den Gesundheitsdatenschutz übernommen, indem nach Art. 9 Abs. 2 lit. h a.E. auch der Vertrag „mit einem Angehörigen eines Gesundheitsberufs" (in der Regel also der Behandlungsvertrag) als Grundlage für die Zulässigkeit der Verarbeitung von Gesundheitsdaten dienen kann, soweit die Datenverarbeitung zur Vertragserfüllung erforderlich ist.

Nicht durchgreifen kann die Kritik, dass damit das Recht auf informationelle Selbstbestimmung der Privatautonomie geopfert werde.[25] Vielmehr ist es gerade auch ein Aspekt der informationellen Selbstbestimmung, dass die betroffene Person auf Basis einer selbst getroffenen Entscheidung mit dem für die Datenverarbeitung Verantwortlichen ein Schuldverhältnis eingeht und damit auch die in diesem Zusammenhang erforderliche Datenverarbeitung in Gang setzt.[26] Die u.U. schwächere Stellung der betroffenen Person gegenüber einem Arzt bei Abschluss eines Behandlungsvertrages, insbesondere aufgrund eines Wissensdefizits oder auch eines Mangels an Alternativen, wird dabei durch den Schutz des Patienten nach den §§ 630a ff. BGB zumindest teilweise kompensiert.[27]

16 BVerfG, DuD 2006, 817 (819) – Schweigepflichtentbindungsklausel.
17 Vgl. *Buchner*, in: Buchner, Datenschutz im Gesundheitswesen, A/2.2.1.
18 Art. 8 Abs. 2 lit. a DSRL.
19 § 4a Abs. 3 BDSG.
20 *Simitis*, in: Simitis, BDSG, 8. Aufl. 2014, § 3 Rn. 86.
21 § 4a Abs. 1 S. 2 BDSG.
22 Vgl. *Dochow*, GesR 2016, 401 (404).
23 Siehe dazu Simitis, in: Semitis, BDSG, 8. Aufl. 2014, § 4 Rn. 21 ff.
24 § 28 Abs. 1 S. 1 Nr. 1 BDSG als Umsetzung von Art. 7 lit. b DSRL.
25 So aber *Dochow*, GesR 2016, 401 (405).
26 Vgl. für Art. 7 lit. b DSRL *Dammann/Simitis*, EG-Datenschutzrichtlinie (1997), Art. 7 Rn. 5; s.a. OLG Frankfurt, NJW-RR 2005, 1280 (1282): „Die in § 28 Abs. 1 BDSG getroffene Regelung findet ihre Rechtfertigung darin, dass der Betroffene eine autonome Entscheidung für einen Vertragsabschluss (oder die Begründung eines Vertrauensverhältnisses) getroffen hat, womit er zugleich auch sein informationelles Selbstbestimmungsrecht ausgeübt hat."
27 Siehe zum Ziel des Patientenrechtegesetzes: „Die Komplexität der Medizin und die Vielfalt von Behandlungsmöglichkeiten verlangen zunächst nach Regelungen, die Patientinnen und Patienten und Behandelnde auf Augenhöhe bringen" (BT-Drucks. 17/10488, S. 9).

5. Betroffenenrechte

Das Datenschutzrecht räumt dem Einzelnen eine ganze Reihe von sog. Betroffenenrechten ein, insbesondere Auskunftsrechte[28] sowie Berichtigungs-, Sperrungs- und Löschungsansprüche[29]. Die DSGVO wird hier dem Grunde nach keine wesentlichen Änderungen mit sich bringen. So hat auch nach der DSGVO die verantwortliche Stelle die betroffene Person nach Art. 13 darüber zu informieren, dass Daten über sie verarbeitet werden. Umfangreicher sind dabei die Informationen geworden, welche der betroffenen Person nach Art. 13 Abs. 1 und 2 mitgeteilt werden müssen. Die Rechte, die die betroffene Person hat, sind bereits aus dem BDSG bekannt. Neben dem Auskunftsanspruch nach Art. 15 (dazu sogleich) kann die betroffene Person insbesondere nach Art. 16 die Berichtigung unrichtiger Daten und nach Art. 17 unter bestimmten Voraussetzungen die Löschung von Daten verlangen. Trotz seiner prominenten Überschrift („Recht auf Vergessenwerden") ist dabei Art. 17 vom Regelungsgehalt her nichts anderes als ein klassischer Löschungsanspruch, der in seinen Grundzügen den Löschungsvorschriften aus § 20 Abs. 2 und § 35 Abs. 2 S. 2 BDSG vergleichbar ist.[30]

Praktisch wichtigstes Betroffenenrecht ist im Gesundheitsbereich das Recht auf Auskunft, welches sich – unabhängig vom Datenschutzrecht – auch als Anspruch aus dem Behandlungsvertrag (vgl. § 630g Abs. 1 BGB) sowie berufsrechtlich aus § 10 Abs. 2 MBO-Ä ableitet (Recht auf Akteneinsicht). Dieses Recht des Patienten auf Akteneinsicht gilt jedoch im deutschen Recht nicht uneingeschränkt. So darf der Arzt einem Patienten die Einsichtnahme in seine Behandlungsunterlagen verweigern, wenn sich bei Herausgabe und Kenntnis des Patienten von diesen Aufzeichnungen in therapeutischer Hinsicht negative gesundheitliche Konsequenzen für den Patienten ergeben können (sog. therapeutischer Vorbehalt). Auch greift das Recht auf Akteneinsicht nicht, soweit einer Einsichtnahme erhebliche Rechte des Arztes oder Dritter entgegenstehen (vgl. § 10 Abs. 2 MBO-Ä, § 630g Abs. 1 BGB). Beide Einschränkungen können auch unter der DSGVO beibehalten werden, da nach Art. 23 Abs. 1 lit. i die Mitgliedstaaten durch Rechtsvorschrift das Auskunftsrecht zum Schutz der betroffenen Person selbst oder zum Schutz der Rechte anderer Personen einschränken können.

II. Bereichsspezifischer Gesundheitsdatenschutz

Für den bereichsspezifischen Gesundheitsdatenschutz sind vor allem die datenschutzrechtlichen Regelungen in den Krankenhausgesetzen der Länder (LKHG) von Bedeutung.

1. Landeskrankenhausrecht

Die datenschutzrechtlichen Regelungen im Landeskrankenhausrecht stellen ein ebenso unübersichtliches wie uneinheitliches Regelungsgeflecht dar. Die LKHG der einzelnen Bundesländer enthalten hier teils mehr, teils weniger Regelungen zum Datenschutz im Krankenhaus mit jeweils unterschiedlichem Inhalt, die ergänzend zum allgemeinen Datenschutzrecht gelten sollen.[31] Zwei Bundesländer haben überhaupt keine Regelungen,[32] Bremen und Nordrhein-Westfalen dafür sogar jeweils ein eigenständiges Datenschutzgesetz für Krankenhäuser bzw. Gesundheitseinrichtungen.[33]

Der Anwendungsbereich der LKHG erstreckt sich zunächst einmal auf Krankenhäuser *in Trägerschaft der Länder sowie der Kommunen*. Darüber hinaus beanspruchen die LKHG jedoch auch Geltung für Krankenhäuser in privater Trägerschaft. Begründen lässt sich ein solcher Vorrang landesrechtlicher Regelungen gegenüber dem BDSG damit, dass die Landesgesetze besondere berufliche Geheimhaltungspflichten regeln, die gemäß § 1 Abs. 3 S. 2 BDSG vom Geltungsanspruch des BDSG „unberührt" bleiben sollen.[34] Und auch unter der DSGVO werden die datenschutzrechtlichen Regelungen der LKHG ihren Anwendungsbereich behalten. Art. 9 Abs. 2 lit. h DSGVO eröffnet den Mitgliedstaaten die Möglichkeit, durch Rechtsvorschrift eine Datenverarbeitung für Zwecke der Gesundheitsvorsorge, für die medizinische Diagnostik sowie die Versorgung und Behandlung im Gesundheitsbereich oder für die Verwaltung von Systemen und Diensten im Gesundheitsbereich zu erlauben. Ebenso können die Mitgliedstaaten „aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit" nach Art. 9 Abs. 2 lit. i eine Datenverarbeitung erlauben.

2. Erlaubnistatbestände für eine Datenverarbeitung

Die bisherigen Erlaubnistatbestände für eine Datenverarbeitung, wie sie in den LKHG normiert sind, lassen sich jeweils zumindest unter eine dieser beiden Öffnungsklauseln der DSGVO einordnen. So sind etwa Regelungen, die eine Verarbeitung von Patientendaten zur Erfüllung des Behandlungsvertrages einschließlich der Dokumentationspflichten, zur sozialen Betreuung und Beratung der Pflege der Patienten und zur Leistungsabrechnung erlauben,[35] von Art. 9 Abs. 2 lit. h erfasst. Sofern vorhanden, können Erlaubnistatbestände, die die Übermittlung von Patientendaten regeln,[36] ebenfalls grundsätzlich bestehen bleiben, da sie wie die Regelungen zur sonstigen Datenverarbeitung unter Art. 9 Abs. 2 lit. h fallen. Der DSGVO liegt ein weiterer Verarbeitungsbegriff als bislang dem BDSG zugrunde. Der Begriff der Verarbeitung nach Art. 9 Abs. 2 lit. h umfasst jede Form des Datenumgangs und mithin auch die Datenübermittlung. Zu beachten ist jedoch die Einschränkung des Art. 9 Abs. 3, nach der eine Datenverarbeitung nach Art. 9 Abs. 2 lit. h nur zulässig ist, wenn diese durch Fachpersonal erfolgt, welches einer Geheimhaltungspflicht unterliegt. Unter diese fällt die ärztliche Schweigepflicht[37] ebenso wie auch das Sozialgeheimnis[38]. Erlaubnistatbestände im Landeskrankenhausrecht, die eine Datenverarbeitung etwa zur Qua-

28 §§ 19, 34 BDSG.
29 Vgl. §§ 20, 35 BDSG.
30 Vgl. *Schantz*, NJW 2016, 1841 (1845).
31 Überblick bei *Buchner*, in: Buchner, Datenschutz im Gesundheitswesen, A/1.4.2.
32 In Niedersachsen und Schleswig-Holstein gibt es bislang kein Krankenhausgesetz mit Regelungen zum Datenschutz.
33 Bremen: BremKHDSG (Bremisches Krankenhausdatenschutzgesetz vom 25. April 1989); NRW: GDSG NW (Gesetz zum Schutz personenbezogener Daten im Gesundheitswesen – Gesundheitsdatenschutzgesetz vom 22. Februar 1994).
34 *Buchner*, in: Buchner, Datenschutz im Gesundheitswesen, A/1.4.2.
35 S. bspw. § 2 Abs. 1 BremKHDSG, Art. 27 Abs. 2 S. 1 BayKrG, § 33 Abs. 2 KHG-SN.
36 S. bspw. 3 f. BremKHDSG, Art. 27 Abs. 5 S. 1 BayKrG, § 27 Abs. 6 ThürKHG.
37 § 9 MBO-Ä, siehe dazu unten IV.
38 § 35 SGB I.

litätssicherung in der stationären Versorgung oder zur Erkennung, Verhütung und Bekämpfung von Krankenhausinfektionen erlauben,[39] können sowohl unter Art. 9 Abs. 2 lit. h als auch unter lit. i fallen. Zum einen erfolgen die Qualitätssicherung und das Entgegenwirken von Krankenhausinfektionen zur individuellen sowie kollektiven Gesundheitsvorsorge nach Art. 9 Abs. 2 lit. h, dienen damit zum anderen aber auch dem öffentlichen Interesse nach lit. i.

Stets zu beachten und umzusetzen im Rahmen der mitgliedstaatlichen Erlaubnistatbestände ist nach den Vorgaben der DSGVO der Grundsatz der Erforderlichkeit (s. lit. h und lit. i jeweils a.E.) Soweit sich daher die in lit. h und lit. i angeführten Zwecksetzungen mit pseudonymisierten oder gar anonymisierten Daten erreicht lassen, ist eine Verarbeitung *personenbezogener* Daten in diesem Umfang nicht zulässig. In den LKHG wird die Vorgabe bereits regelmäßig berücksichtigt, entweder indem z.T. explizit eine Anonymisierung und Pseudonymisierung von Patientendaten vorgesehen ist[40], oder aber zumindest auf den Grundsatz der Erforderlichkeit abgestellt wird.

Nicht ausgeschlossen ist schließlich, dass im mitgliedstaatlichen Recht auch noch strengere Vorgaben für die Verarbeitung von Gesundheitsdaten aufgestellt werden, als dies nach Art. 9 Abs. 2 lit. h und lit. i DSGVO vorgesehen ist. Art. 9 Abs. 4 DSGVO lässt solche zusätzlichen Bedingungen („einschließlich Beschränkungen") für die Verarbeitung von genetischen, biometrischen und Gesundheitsdaten ausdrücklich zu. Zulässig sind daher etwa Regelungen, die, anders als die DSGVO, eine Einwilligung in die Verarbeitung von Patientendaten nur dann als wirksam ansehen, wenn diese schriftlich erteilt wurde.[41]

III. Sozialdatenschutz

Das bisherige Recht des Sozialdatenschutzes ist von dem Bestreben gekennzeichnet, den Schutz von Sozialdaten umfassend und eigenständig zu regeln. Gesetzliche Erlaubnistatbestände, die eine Verarbeitung von Sozialdaten legitimieren können, finden sich im SGB X und für den Bereich GKV im SGB V. Die allgemeinen Grundsätze der zulässigen Erhebung, Verwendung und Nutzung von Sozialdaten sind in den §§ 67 ff. SGB X normiert. Für den Bereich der GKV gelten sodann die bereichsspezifischen Vorschriften der §§ 284 ff. SGB V, die als Spezialnormen Vorrang haben vor den Vorschriften des SGB X. Die sozialrechtlichen Regelungen präsentieren sich damit als ein eigenständiges und umfassendes datenschutzrechtliches Regelungsregime, das als „Vollregelung"[42] Rückgriffe auf das allgemeine Datenschutzrecht weitgehend entbehrlich machen soll.[43]

Die weitgehenden Öffnungsklauseln der DSGVO für den Gesundheits- und Sozialbereich erlauben es dem Grunde nach, dass das Sozialdatenschutzrecht auch künftig als solch ein eigenständiger Regelungsbereich erhalten bleibt. Eine andere Frage ist, ob der Gesetzgeber die DSGVO nicht gleichwohl zum Anlass nehmen sollte, das „hochkomplexe Regelungsgeflecht" beim Sozialdatenschutz einer Totalrevision zu unterziehen und diesen zunehmend unstrukturiert gewordenen Regelungsbereich umfassend zu bereinigen.[44]

Fraglich ist, inwieweit die viel kritisierte Rechtsprechung des BSG zur Reichweite der Einwilligung als Erlaubnistatbestand für eine Datenverarbeitung im Bereich der GKV unter der DSGVO Bestand haben wird. Im konkreten Fall hatte das BSG mit Verweis auf die besondere Bedeutung des Sozialdatenschutzes in Bezug auf sensible Gesundheitsdaten die Weitergabe solcher Daten an Dritte, die nicht dem strengen Sozialdatenschutz unterliegen, von einer ausdrücklichen gesetzlichen Gestattung anhängig gemacht. Einen allgemeinen datenschutzrechtlichen Grundsatz der Art, dass unabhängig von einer gesetzlichen Ermächtigung eine Datenübermittlung stets auch zulässig ist, wenn eine Einwilligung des Betroffenen vorliegt, hat das BSG für den Bereich der GKV abgelehnt.[45] Zwar können auch unter der DSGVO nach Art. 9 Abs. 2 lit. a die Mitgliedstaaten vorsehen, dass in bestimmten Fällen die Verarbeitung von Gesundheitsdaten nicht durch eine Einwilligung der betroffenen Person legitimiert werden kann. Fraglich ist jedoch, ob das, was das BSG aus der Regelungssystematik und -intention des SGB V (indirekt) herausliest, der Vorgabe des Art. 9 Abs. 2 lit. a genügt, dass sich eine Ausnahme vom Grundsatz der Einwilligung als Erlaubnistatbestand aus dem Recht der Mitgliedstaaten ergeben muss.[46]

IV. Ärztliche Schweigepflicht

Das informationelle Selbstbestimmungsrecht des Patienten korrespondiert auf Seiten des Arztes mit dessen Schweigepflicht. Die ärztliche Schweigepflicht zählt zum Kernbereich der ärztlichen Berufsethik. Sie bildet die Grundlage für die besondere Vertrauensbeziehung zwischen Arzt und Patienten und ist in den ärztlichen Berufsordnungen geregelt sowie durch § 203 Abs. 1 Nr. 1 StGB strafrechtlich abgesichert. Das Verhältnis zwischen Datenschutzrecht und ärztlicher Schweigepflicht ist in manchen Einzelfragen umstritten.[47] Unabhängig davon gilt aber grundsätzlich, dass es sich beim allgemeinen Datenschutzrecht und der ärztlichen Schweigepflicht um zwei Schutzebenen handelt, die unabhängig voneinander gelten und zu beachten sind.[48] Diese Zweigleisigkeit wird sich auch unter der DSGVO fortsetzen – und damit werden auch all die Probleme bestehen bleiben, die aus dem unabgestimmten Nebeneinander von Datenschutzrecht und ärztlicher Schweigepflicht folgen.[49]

1. Beispiel Outsourcing

Ein Paradebeispiel für das unabgestimmte Nebeneinander von Datenschutzrecht und ärztlicher Schweigepflicht sind die rechtli-

39 S. bspw. § 2 Abs. 5 BremKHDSG, § 10 Abs. 2 HmbKHG.
40 So § 2 Abs. 5 BremKHDSG, § 34 KHG-M-V.
41 S. bspw. § 2 BremKHDSG, § 24 Abs. 3 LKG-Bln.
42 *Dix* in: Simitis, BDSG, 8. Aufl. 2014, § 1 Rn. 160.
43 *Kircher* in: Kingreen/Kühling, Gesundheitsdatenschutzrecht (2015), S. 202 f.
44 In diesem Sinne *Weichert*, DANA 2016, 48 (51); ebenso *Schaar*, DANA 2016, 80 (81).
45 BSG, NJOZ 2009, 2959 (2969).
46 Vgl. dazu *Dochow*, GesR 2016, 401 (405): „fraglich, ob es aufgrund fehlender Schaffung gesetzlicher Einwilligungsmöglichkeiten damit schon generell als ausdrücklich untersagt gelten soll, dass durch eine Einwilligung das Datenverarbeitungsverbot gem. Art. 9 Abs. 1 DSGVO aufgehoben werden kann."
47 Vgl. im Einzelnen *Buchner*: in Buchner, Datenschutz im Gesundheitswesen, A/1.4.1.
48 Vgl. *Dix* in: Simitis, BDSG, 8. Aufl. 2014, § 1 Rn. 175.
49 Vgl. *Dochow*, GesR 2016, 401 (408).

chen Rahmenbedingungen für ein Outsourcing im Gesundheitsbereich. In Zeiten eines immer komplexer werdenden Behandlungsalltags sind Gesundheitseinrichtungen etwa im Bereich der Dokumentation, der Abrechnung und der IT zunehmend auf die Einbindung externer Dienstleister angewiesen, welche dann oftmals auch mit einer Offenbarung von Patientendaten gegenüber diesen Dienstleistern einhergeht.[50] Im allgemeinen Datenschutzrecht hat das Outsourcing bislang durch § 11 BDSG und entsprechende Vorschriften in den Landesdatenschutzgesetzen eine Privilegierung erfahren. Dem § 11 BDSG liegt der Gedanke zugrunde, dass Auftragnehmer und Auftraggeber eine rechtliche Einheit bilden. Unter den Voraussetzungen des § 11 BDSG ist die Datenübermittlung vom Auftraggeber, bspw. dem Arzt, an den Auftragnehmer, den Dienstleister, datenschutzrechtlich irrelevant. Es bedarf folglich keines datenschutzrechtlichen Erlaubnistatbestands für diese Datenübermittlung. Diese datenschutzrechtliche Privilegierung der Auftragsdatenverarbeitung läuft jedoch ins Leere, soweit es sich bei den übermittelten Daten um solche handelt, die auch der ärztlichen Schweigepflicht unterliegen. Nach vorherrschender Auffassung kann § 11 BDSG gerade keine Befugnis begründen, Daten zu offenbaren, die der ärztlichen Schweigepflicht unterliegen. Eine Übermittlung von Daten an einen Auftragnehmer kann somit zwar datenschutzrechtlich zulässig sein, stellt aber ohne Einwilligung der betroffenen Person einen Verstoß gegen die ärztliche Schweigepflicht dar.[51]

2. Outsourcing unter der DSGVO

Dieser Wertungswiderspruch zwischen Datenschutzrecht und ärztlicher Schweigepflicht wird auch unter der DSGVO bestehen bleiben.[52] Die DSGVO normiert die Auftragsdatenverarbeitung in Art. 28 f. Die Regeln zur Auftragsverarbeitung der DSGVO sind dabei eng an § 11 BDSG angelehnt. Zwar geht aus Art. 28 nicht direkt hervor, ob die Auftragsdatenverarbeitung auch nach der DSGVO privilegiert ist, die Datenübermittlung an den Auftragnehmer also ohne Rückgriff auf eine datenschutzrechtliche Erlaubnisnorm zulässig ist. Vorgeschlagen wird daher, eine Datenübermittlung immer nach Art. 6 Abs. 1 lit. f. als zulässig zu erachten, sofern die Voraussetzungen des Art. 28 erfüllt sind. Problematisch an einer Rechtfertigung der Datenübermittlung nach Art. 6 Abs. 1 lit. f wäre jedoch, dass dieser Erlaubnistatbestand gerade nicht bei der Übermittlung von Gesundheitsdaten greift.[53] Eine Übermittlung von Gesundheitsdaten an den Auftragnehmer wäre somit nicht mehr nur aus strafrechtlicher, sondern auch aus datenschutzrechtlicher Sicht problematisch. Sie wäre datenschutzrechtlich nur zulässig, wenn nach Art. 9 lit. h ein entsprechender Erlaubnistatbestand zur Übermittlung im Unionsrecht oder in den Mitgliedstaaten existieren würde oder die Übermittlung vertraglich zwischen dem Arzt und dem Patienten vereinbart worden wäre.

Letztendlich ist aber auch ohne explizite Regelung von einer Privilegierung der Auftragsdatenverarbeitung auszugehen. Andernfalls wäre schon wenig nachvollziehbar, weshalb die DSGVO überhaupt eine Differenzierung zwischen Verantwortlichem und Auftragsverarbeiter vornimmt. Eine solche Differenzierung wäre nicht erforderlich, wenn die Auftragsdatenverarbeitung ohnehin wie eine normale Verarbeitung zu behandeln wäre. Mit der Differenzierung zwischen dem Verantwortlichen und dem Auftragsverarbeiter wollte der europäische Gesetzgeber augenscheinlich die Auftragsdatenverarbeitung in ihrer bisherigen Form auch in die DSGVO übernehmen. Damit bleibt dann aber auch der eben skizzierte Wertungswiderspruch zwischen Datenschutzrecht und ärztlicher Schweigepflicht bestehen.

C. Ausblick

Am Gesundheitsdatenschutz zeigt sich exemplarisch, dass die DSGVO in vielerlei Hinsicht mehr Richtlinie als Verordnung ist. Betrachtet man die Regelungsspielräume im Einzelnen, die die DSGVO den Mitgliedstaaten belässt, fällt auf, dass diese in vielerlei Hinsicht eben solche Fragestellungen betreffen, die hierzulande seit langem einer klaren und konsistenten Regelung harren, egal ob es um große Würfe wie den Gesundheitsdatenschutz oder auch den Beschäftigtendatenschutz geht oder auch nur um Einzelfragen wie die der Einwilligungsfähigkeit von Minderjährigen. So oder so ist aber aktuell allererste Herausforderung für den nationalen Gesetzgeber, noch in dieser Legislaturperiode ein Nachfolgegesetz für das BDSG auf den Weg zu bringen. Schon die Auseinandersetzungen um dieses ABDSG (Allgemeines Bundesdatenschutzgesetz) zeigen, wie kontrovers der Anpassungsbedarf im nationalen Datenschutzrecht aus Anlass des neuen europäischen Datenschutzrechts beurteilt wird.[54] Auch vor diesem Hintergrund ist die Hoffnung gering, dass der nationale Gesetzgeber die DSGVO zum Anlass nehmen wird, in einer zweiten Runde zu einem späteren Zeitpunkt einmal den Gesundheitsdatenschutz in einen konsistenteren und transparenteren Regelungsrahmen zu überführen.

50 Vgl. etwa *Giesen*, NStZ 2012, 122; *Petri*, DuD 2014, 862.
51 Vgl. *Buchner*, MedR 2013, 337 (338).
52 Vgl. *Dochow*, GesR 2016, 401 (408).
53 Siehe dazu und zu einer Auseinandersetzung mit verschiedenen Ansätzen zur Privilegierung *Koós/Englisch*, ZD 2014, 276 (284 f.).
54 Der erste (umstrittene) Referentenentwurf zum ABDSG samt kritischer Stellungnahmen von BMJV und BfDI ist abrufbar unter https://netzpolitik.org.