DIE MEDIZIN IM VISIER DER DATENSCHÜTZER

Dr. iur. Remus Muresan | 23. Juli 2019

(Auch) die Medizin gerät zusehends ins Visier der Datenschutzbehörden. Besonders hart bekam dies unlängst ein Spital in Portugal zu spüren, dem wegen Verstössen gegen die EU-DSGVO eine Busse von fast einer halben Million Euro auferlegt wurde. Aber auch in anderen EU-Ländern richten die Datenschützer ihr Augenmerk auf die Ärzteschaft. In der Schweiz hingegen ist es in dieser Hinsicht bislang vergleichsweise ruhig. Sollte sich dies ändern und sollten die Datenschutzbehörden bei Spitälern und Arztpraxen künftig etwas genauer hinsehen, könnte es für einzelne von ihnen allerdings ein ziemlich unangenehmes «Erwachen» geben.

Was jedoch zunächst den Bereich der Europäischen Union (EU) anbelangt, ist die im portugiesischen Fall verhängte Busse zwar ungewöhnlich hoch. Der Fall illustriert jedoch gerade deshalb in aller Deutlichkeit, dass die Medizin (auch) dem Thema Datenschutz besonderes Augenmerk schenken muss. Die entsprechenden Vorgänge sind letztlich auf den Erlass der EU-Datenschutz-Grundverordnung (EU-DSGVO) zurückzuführen. Gestützt auf die Grundsätze der EU-DSGVO hat die portugiesische Datenschutzbehörde CNPD bereits vor etwa einem Jahr, im Juli 2018, die erwähnte Busse – in der Höhe von EUR 400'000 – gegen ein Spital in Barreiro, einer Stadt in der Nähe von Lissabon, verhängt. Die CNPD hatte im Rahmen einer Untersuchung festgestellt, dass das fragliche Spital sehr grosszügig mit der Gewährung des Zugangs zu Patientendaten gewesen war – es hatte durch seine IT-Abteilung fast 1'000 Arztprofile (mit jeweils umfassendem Zugriff auf alle Patientenakten) einrichten lassen, obwohl im Spital nur knapp 300 Ärzte beschäftigt waren. Wie sich herausstellte, war auch nichtärztliches Personal wie Ernährungsberater, Psychologen oder Physiotherapeuten mit solchen Arztprofilen ausgestattet worden. Darüber hinaus ermöglichten die Arztprofile uneingeschränkten Zugang zu jeweils allen Patientendaten, ungeachtet der jeweiligen Fachrichtung des Arztes. Die portugiesische Datenschutzbehörde befand, dass das betroffene Spital damit seine gemäss EU-DSGVO bestehende Verpflichtung, angemessene technische und organisatorische Massnahmen zum Schutz der Patientendaten zu ergreifen, verletzt hatte. Das Spital hat in der Folge Rechtsmittel gegen die Busse eingelegt; das Verfahren ist gegenwärtig noch hängig.

Was dagegen etwa auf Ärzte im deutschen Bundesland Bayern zukommt, ist noch eher ungewiss. Zwar wurden auch sie vom zuständigen Datenschützer – dem Landesdatenschutzbeauftragten – ins Visier genommen: Seit einiger Zeit unterzieht dieser individuelle Ärzte sog. unabhängigen Datenschutzprüfungen. Dabei werden die Betroffenen allerdings – jedenfalls zunächst – deutlich weniger hart angefasst als in Portugal: Sie erhalten vom Datenschutzbeauftragten «lediglich» Fragebögen, mittels derer sie Auskunft über die von ihnen getroffenen Datenschutzvorkehrungen geben sollen; besonderes Augenmerk liegt dabei offenbar auf Massnahmen gegen mögliche «Cyberattacken» auf Patientendaten mittels «Malware». Doch die Tragweite und potenziellen Folgen der Beantwortung der entsprechenden Fragen durch die Ärzte sind vollkommen offen; auch hier können u.U. durchaus Sanktionen drohen. Darüber hinaus sind aber auch schon die rechtliche Qualifizierung der Fragebögen sowie die möglichen Folgen im Falle der Weigerung, diese auszufüllen, unklar (vgl. näher bzw. eingehend zum Ganzen: TIM OEHLER, MedR 2019, S. 457 ff.).

Verglichen mit solchen Entwicklungen sind die Ärzte, Spitäler und anderen Akteure des Medizin- bzw. Gesundheitswesens in der Schweiz in datenschutzrechtlicher Hinsicht bislang weitestgehend unbehelligt geblieben. Zwar musste die Krankenversicherung Helsana kürzlich einen vom Bundesverwaltungsgericht bestätigten Rüffel des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) hinnehmen, weil sie eine App betrieb, die in unzulässiger Weise Personendaten von Versicherten sammelte bzw. miteinander verknüpfte (Urteil A-3548/2018 vom 19. März 2019). Abgesehen davon aber fokussieren die Bundes- und kantonalen Datenschützer offensichtlich eher auf andere Sachbereiche. Sollte sich dies allerdings ändern, scheint es durchaus wahrscheinlich, dass der Gesundheitsbereich einige, teilweise empfindliche Interventionen würde gewärtigen müssen.

Denn in Sektoren, die derart intensiv mit höchst sensiblen Personendaten umgehen wie die Medizin wimmelt es geradezu von potenziellen datenschutzrechtlichen Risiken, Unklarheiten und Konflikten. Dies betrifft nicht nur besonders komplexe Aspekte wie etwa das elektronische Patientendossier (EPD) oder Gentests. Vielmehr stellen sich entsprechende Fragen jeden Tag und in jeder beliebigen Arztpraxis, in jedem Spital und Labor sowie auch auf medizinischen «Nebenschauplätzen» wie etwa im Zusammenhang mit Dopingkontrollen im Sport. Dass dabei alle Vorgänge stets in Übereinstimmung mit den datenschutzrechtlichen Vorgaben stattfinden, darf wohl mit einer gewissen Berechtigung bezweifelt werden.

Entsprechende Fragen werfen nur etwa schon die Fragebögen auf, die Patienten beim Spitaleintritt oder vor der Behandlung durch einen Arzt regelmässig ausfüllen «müssen». Datenschutzrechtlich betrachtet, müssen sie dies eben gerade *nicht*; zudem sind die Patientinnen und Patienten gemäss den Empfehlungen des EDÖB ausdrücklich auf den Fragebögen darüber zu informieren, dass die Angaben freiwillig sind. In der Praxis wird dies freilich nur selten konsequent umgesetzt. In diesem Zusammenhang ist auch noch wenig geklärt, wie sich die Rechtslage darstellt, wenn ein Patient sich einmal weigern sollte, bestimmte Angaben zu machen. Darf der Arzt dann die Behandlung – etwa unter Hinweis darauf, dass er die geforderten Angaben für eine adäquate Behandlung benötigt – verweigern? Ähnliche Fragen stellen sich bspw. auch im Zusammenhang mit dem EPD in Spitälern (vgl. näher dazu ISABEL BAUR et al., jusletter-Beitrag vom 28. August 2017, Rz. 42 ff.).

Im Rahmen der Diskussionen um Datenschutz in der Medizin sollte ganz generell auch der Umstand nicht unberücksichtigt bleiben, dass die Patienten einerseits ein Interesse am Schutz ihrer Daten haben dürften, es ihnen aber fraglos auch sehr nützt, wenn der Datenschutz einem Austausch von wesentlichen Informationen zwischen behandelnden Ärzten – z.B. über Medikamentenunverträglichkeiten o.dgl. – nicht im Wege steht. Hier ergeben sich insbesondere Konflikte zwischen dem Patientenwohl und Fragen der Reichweite bzw. der Anforderungen an eine gültige Einwilligung zur Datenweitergabe – auch diesbezüglich ist indessen noch vieles ungeklärt. Und schliesslich besteht die Gefahr, dass ein «überzüchteter» Datenschutz den täglichen Betrieb in einer Arztpraxis erheblich beeinträchtigen kann. So empfiehlt der EDÖB etwa Patienten, die Zweifel hinsichtlich der Verhältnismässigkeit der auf Gesundheitsfragebögen geforderten Angaben haben, den Arzt darauf anzusprechen. Wenn nun – insbesondere in hoch frequentierten Praxen mit 50 und mehr Patienten pro Tag – zahlreiche Personen von dieser Möglichkeit Gebrauch machen würden, hätte dies erhebliche Auswirkungen auf den Praxisbetrieb.

Ein weiteres, besonders virulentes Thema ist schliesslich die Gewährleistung der Sicherheit von Patientendaten. Vor allem kleinere und mittelgrosse Arztpraxen dürften die diesbezüglich zu erfüllenden Anforderungen unterschätzen. Sollten solchen Praxen Fragebögen wie die eingangs erwähnten, in Bayern verschickten zugestellt oder ihnen in anderer Weise datenschutzrechtlich «auf den Zahn gefühlt» werden, könnte dies im Einzelfall nicht unerhebliche Konsequenzen haben. Denn die Verpflichtung zur Ergreifung «angemessener technischer und organisatorischer Massnahmen» zum Schutz von Patientendaten, deren Verletzung in Portugal zur Verhängung der ebenfalls eingangs erwähnten Busse geführt hat, besteht auch in der Schweiz. Dies allerdings nicht aufgrund der EU-DSGVO, sondern aufgrund des

schweizerischen Datenschutzgesetzes (DSG; vgl. insbesondere dessen Art. 7 Abs. 1). Zwar können die Bussen in der Schweiz nicht solche Grössenordnungen erreichen, wie dies in Portugal der Fall war: Selbst mit der beabsichtigten Verschärfung des DSG (das sich gegenwärtig in Revision befindet) sollen sie auf höchstens CHF 250'000 limitiert sein. Aber auch das kann für eine Arztpraxis im Einzelfall bereits eine durchaus einschneidende Sanktion darstellen. Und der EDÖB weist zu Recht darauf hin: «Wichtig ist, dass die Ärzte sich bewusst sind, dass sie am Ende die Verantwortung für die Folgen einer schlecht geführten Informatik tragen». Dass dieses Bewusstsein flächendeckend vorherrscht, ist nicht unbedingt als gegeben anzunehmen...