STELLUNGNAHME DES DVTA

Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (EU-Datenschutzgrundverordnung), die darauf abzielt, den Schutz von personenbezogenen Daten innerhalb der Europäischen Union sicherzustellen und den freien Datenverkehr zu gewährleisten, ist sehr zu begrüßen.
Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts (Art. 8 Abs. 1 der Charta der Grundrechte der Europäischen Union [im Folgenden „Charta“] sowie Art. 16 Abs. 1 des Vertrags über die Arbeitsweise der Europäischen Union [AEUV]).
Gerade im Gesundheitswesen fallen im Rahmen eines Behandlungsprozesses, angefangen bei der Aufnahme des Patienten, bei Untersuchungen, wie zum Beispiel bildgebenden Verfahren oder Blutanalysen, Diagnose, Therapie bis hin zur Abrechnung, begleitenden Prozessen, wie Meldepflichten, statistische Auswertungen, Forschung, wie auch bei der nachgelagerten Rehabilitation eine Vielzahl hochsensibler Patientendaten an, deren Schutz vor unbefugtem Zugriff Dritter einerseits geschützt werden muss, wie andererseits gewährleistet sein muss, dass diejenigen, die die Daten für eine optimale Gesundheitsversorgung und Abrechnung benötigen, sie auch erhalten. Dieses Thema wird umso brisanter, je mehr telemedizinische Verfahren involviert sind.
Die neue Datenschutzgrundverordnung trägt dem dadurch Rechnung, dass der Einzelne, Herr/Frau über seine/ihre personenbezogenen Daten ist.
Art. 6 Abs. 1 schreibt daher vor, dass die Verarbeitung personenbezogener Daten insbesondere nur rechtmäßig ist, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:
Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere festgelegte Zwecke gegeben. Ist dieser Zweck nicht mehr gegeben, müssen die Daten gelöscht werden, es sei denn, dass zum Beispiel gesetzlich etwas anderes geregelt ist (Art. 17 Recht auf Löschung [„Recht auf Vergessenwerden“]).
Diese „Einwilligung der betroffenen Person“ muss dabei, um wirksam zu sein, eine „ohne Zwang, für den konkreten Fall, in Kenntnis der Sachlage und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen Handlung sein, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“.
Es ist auch gut, dass die neue Datenschutzgrundverordnung die Definition sehr weit fasst, um sowohl aktuelle wie künftig mögliche Personendaten zu erfassen.
Nach Art. 4 Abs. 1 der neuen Datenschutzgrundverordnung sind „personenbezogene Daten“ alle Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person („betroffene Person“) beziehen; als bestimmbar wird eine Person angesehen, „die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Onlinekennung oder zu einem oder mehreren besonderen Merkmalen bestimmt werden kann, die Ausdruck ihrer physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind“.
Datenvermeidung und Datensparsamkeit spielen weiterhin eine große Rolle. Daten, die anonymisiert werden können, sind zu anonymisieren, das heißt, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Sie unterliegen dann nicht der Datenschutzgrundverordnung.
Im Bereich der Teleradiologie spielt zum Beispiel die Pseudonymisierung eine große Rolle, um den Schutz der Patientendaten zu erreichen. Die Pseudonymisierung erfasst nach Art. 4 Abs. 5 der neuen Datenschutzgrundverordnung die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern in diesen zusätzliche Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die die Nichtzuordnung zu einer bestimmten oder bestimmbaren Person gewährleisten.
Es ist zu begrüßen, dass die neue Datenschutzgrundverordnung ein hohes Schutzniveau selbst bei pseudonymisierten Daten vorsieht. Aufgrund der hohen Arbeitsverdichtung sind jedoch die geforderte gesonderte Aufbewahrung und organisatorischen Maßnahmen so zu minimieren, dass Ärzte, MTA etc. hiermit nicht zusätzlich belastet werden, sondern die knappe Zeit für ihre medizinischen Kernaufgaben nutzen können.
Gleiches gilt für die umfassend geregelten Informationsrechte und -pflichten, die für den Betroffenen sehr zu begrüßen sind, für die für die Verarbeitung Verantwortlichen aber auch realisierbar sein sollten. Dies soll auch gerade im Hinblick auf die in Art. 31 geregelte Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und den Betroffenen, „ohne unangemessene Verzögerung“, im Fall der Aufsichtsbehörde „möglichst binnen höchstens 72 Stunden“ gemeldet werden, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten führt.
Ein guter Datenschutzbeauftragter ist daher wichtig, insbesondere auch, um Verstöße gegen die neuen Datenschutzgrundverordnung zu vermeiden, da diese mit einer Geldbuße von bis zu 20 Millionen Euro oder vier Prozent des Jahresumsatzes ausmachen.
Aus der Sicht der Einzelnen, ob nun als Bürger, Patient oder Arbeitnehmer, ist der weitgefasste Schutz der Daten, das Recht zu bestimmen, wer wann welche Daten, wofür oder auch nicht, verwenden darf, und über die gespeicherten Daten oder deren Freigabe an Dritte informiert zu werden, absolut begrüßenswert, damit der Bürger nicht „gläsern“ wird.

Elske Müller-Rawlins