Wirksamwerden der EU-Datenschutz-Grundverordnung (EU-DS-GVO) am 25. Mai 2018 – Auswirkungen auf den Umgang mit Patientendaten

Einführung

Die EU-Datenschutz-Grundverordnung (DS-GVO) wird nach zweijähriger Übergangsphase seit Inkrafttreten zum 25.05.2018 wirksam und löst damit die bisher geltende Datenschutzrichtlinie sowie in weiten Teilen auch das nationale Datenschutzrecht ab. Durch die unmittelbare Wirkung der Verordnung in den Mitgliedstaaten wird der Datenschutz in der Europäischen Union weiter harmonisiert und ein einheitliches sowie höheres Schutzniveau bei der Verarbeitung personenbezogener Daten geschaffen. Dafür enthält die Verordnung einige Neuerungen und stellt mit einem drastisch erhöhten Bußgeld von bis zu 20 Millionen Euro oder – wenn dieser Betrag höher ist – 4 % des Jahresumsatzes klar, dass Datenschutzverletzungen nicht als Kavaliersdelikte angesehen werden.

Als Ersteller von radiologischen Aufnahmen und Verarbeiter dieser besonders sensiblen Daten spielt der Datenschutz für Radiologen schon wegen der ärztlichen Schweigepflicht eine herausragende Rolle. Bei der Verarbeitung von Gesundheitsdaten sind nunmehr die Regelungen der DS-GVO sowie, wegen der darin enthaltenen Öffnungsklauseln für den nationalen Gesetzgeber, die Neufassung des Bundesdatenschutzgesetzes (BDSG) maßgeblich.

Schutzbereich der Datenschutz-Grundverordnung

Die in der DS-GVO verankerten Grundsätze und Vorschriften dienen dem Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten und sollen gewährleisten, dass insbesondere ihr Recht auf informationelle Selbstbestimmung gewahrt bleibt. Dafür behält die Verordnung die schon in der Datenschutzrichtlinie verankerten Grundprinzipien des europäischen Datenschutzes – das grundsätzliche Verbot der Verarbeitung mit Erlaubnisvorbehalt, die Datenvermeidung und Datensparsamkeit, die Zweckbindung und die Transparenz – bei und entwickelt diese weiter.

Schutzgut der Verordnung sind personenbezogene Daten, das heißt alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung, identifiziert werden kann (Art. 4 Nr. 1 DS-GVO). Damit sind auch radiologische Aufnahmen, die einer bestimmten Person durch den Vermerk der Patientendaten zugeordnet werden können, von dem Datenbegriff umfasst. Die DS-GVO findet dagegen keine Anwendung auf anonyme Informationen. Gemeint sind damit Daten, die sich von vornherein nicht auf einen identifizierten oder identifizierbaren Menschen beziehen oder die derart bearbeitet worden sind, dass die betroffene Person nicht mehr identifiziert werden kann (vgl. Erwägungsgrund 26 DS-GVO). Art. 6 DS-GVO statuiert ein grundsätzliches Verbot der Verarbeitung von personenbezogenen Daten unter dem Vorbehalt der dort normierten Erlaubnistatbestände. Mit dem Begriff der Verarbeitung ist jeder – mit oder ohne Hilfe von automatisierten Verfahren durchgeführte – Vorgang im Zusammenhang mit personenbezogenen Daten gemeint. Darunter fällt insbesondere das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, die Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von personenbezogenen Daten (Art. 4 Abs. 2 DS-GVO).

Besondere Anforderungen an die Verarbeitung von Gesundheitsdaten

Besondere Kategorien personenbezogener Daten, bei deren Verarbeitung ihrem Wesen nach erhebliche Risiken für die Grundrechte der betroffenen Personen auftreten können, werden in der DS-GVO besonders geschützt. Zu diesen Daten gehören auch Gesundheitsdaten, die sich auf die körperliche oder geistige Gesundheit eines Menschen, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen (Art. 4 Nr. 15 DS-GVO). Für die Zulässigkeit der Verarbeitung dieser besonderen Datenkategorie macht Art. 9 Abs. 2 DS-GVO im Gegensatz zu Art. 6 DS-GVO strengere Ausnahmen vom generellen Verbot der Verarbeitung und sichert so ein erhöhtes Schutzniveau für besonders sensible personenbezogene Daten.

Anforderungen an die Einwilligung

Die Verarbeitung von personenbezogenen Daten ist grundsätzlich gestattet, wenn die betroffene Person in diese eingewilligt hat. Dabei muss die Einwilligung freiwillig, für den bestimmten Fall und unmissverständlich abgegeben werden (Art. 4 Nr. 11 DS-GVO). Für die Rechtmäßigkeit der Verarbeitung von Gesundheitsdaten gelten nach Art. 9 Abs. 2 Buchst. a) DS-GVO strengere Voraussetzungen. Der Patient muss in die Verarbeitung seiner Daten ausdrücklich

einwilligen, sodass eine konkludente oder gar stillschweigende Gestattung wie bisher nicht mehr ausreichend ist. Die Einwilligung muss sich zudem auf einen bestimmten Zweck oder im Falle von mehreren Verarbeitungszwecken auf jeden einzelnen beziehen. Eine umfassende Einwilligung zur nicht näher spezifizierten Verarbeitung von Gesundheitsdaten dürfte nach dieser Regelung daher nicht wirksam sein. Die Zweckbindung der Datenverarbeitung wird in Art. 5 Abs. 1 Buchst.b) DS-GVO allerdings teilweise dahingehend gelockert, dass eine Weiterverarbeitung der Daten für Forschungszwecke nicht als unvereinbar mit dem ursprünglichen Zweck gilt.

Beruht die Verarbeitung von Gesundheitsdaten auf einer Einwilligung, muss im Bedarfsfall nachgewiesen werden können, dass der Patient in die konkrete Datenverarbeitung eingewilligt hat (Art. 7 Abs. 1 DS-GVO). Dafür muss die Einwilligung zwar nicht schriftlich erteilt werden, wegen des Erfordernisses der Nachweisbarkeit und der Dokumentation wird dies aber regelmäßig sinnvoll sein. Der Patient hat zudem das Recht, seine Einwilligung jederzeit frei zu widerrufen, was die Rechtmäßigkeit der bis dahin erfolgten Verarbeitung jedoch nicht berührt.

Gesetzliche Erlaubnistatbestände

Die Einwilligung des Patienten ist nicht erforderlich, wenn die Verarbeitung von vorneherein gesetzlich vorgesehen ist. Für Radiologen relevant sind insbesondere die Erlaubnistatbestände zum Zwecke der individuellen und öffentlichen Gesundheit sowie zur Forschung gemäß Art. 9 Abs. 2 Buchst.h) bis j) DS-GVO. Danach ist die Verarbeitung von Gesundheitsdaten beispielsweise rechtmäßig, wenn sie zur Sicherstellung und Überwachung der Gesundheit, der Kontrolle von Gesundheitsgefahren sowie zur Verwaltung von Leistungen der Gesundheitsversorgung erforderlich und im Recht der Union oder der Mitgliedstaaten vorgesehen ist. Von diesen Öffnungsklauseln hat der deutsche Gesetzgeber in § 22 Abs. 1 BDSG nF Gebrauch gemacht und erlaubt die Verarbeitung von Gesundheitsdaten, wenn sie für die Gesundheitsvorsorge, medizinische Diagnostik, Versorgung und Behandlung im Gesundheitsbereich, zur Durchführung eines Behandlungsvertrages oder aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden Gesundheitsgefahren, erforderlich ist. Ferner erlaubt § 27 BDSG nF die Verarbeitung für wissenschaftliche und statistische Zwecke. Dabei wird in § 22 Abs. 1 BDSG nF ausdrücklich klargestellt, dass die berufs- und strafrechtlichen Vorgaben zur Wahrung des Berufsgeheimnisses einzuhalten sind. Die ärztliche Schweigepflicht gemäß § 203 Abs. 1 Nr. 1 Strafgesetzbuch (StGB) gilt daher parallel zur DS-GVO weiter fort und erfährt Durchbrechungen nur dann, wenn der Gesetzgeber dies ausdrücklich vorsieht. Die bisher bekannten Offenbarungsrechte und -pflichten – wie die Weitergabe von Daten zur Abrechnung von Leistungen gemäß §§ 294 ff. Sozialgesetzbuch Fünftes Buch, die Meldepflicht von bestimmten ansteckenden Krankheiten nach § 8 des Infektionsschutzgesetzes oder die Pflichten des Radiologen zur Vorlage von Röntgenaufnahmen gemäß §§ 17a Abs. 4 und 28 Abs. 8 Röntgenverordnung (RöV) – berührt die DS-GVO daher nicht.

Patientenrechte nach der Datenschutz-Grundverordnung

Zum Schutz der betroffenen Personen stattet die DS-GVO diese mit umfangreichen Rechten aus, die zwar dem Grunde nach schon vorher bestanden, aber nun weiter präzisiert werden. In der radiologischen Praxis besonders relevant wird wohl der Auskunftsanspruch aus Art. 15 Abs. 1 DS-GVO werden. Er gewährt den betroffenen Personen das Recht zu erfahren, zu welchen Zwecken die Daten verarbeitet werden, wie lange sie gespeichert, an wen sie weitergegeben werden oder welcher Logik die Speicherung folgt und bezieht sich auch auf Patientenakten. Ein Recht auf Einsichtnahme in die Patientenakten gewährt zwar bereits § 630 g Bürgerliches Gesetzbuch. Während darin aber ein Anspruch auf Herausgabe einer Abschrift nur gegen Erstattung der Kosten besteht, geht Art. 15 Abs. 3 DS-GVO von einer grundsätzlichen Unentgeltlichkeit der ersten Auskunftserteilung aus. Wegen des Vorrangs des Unionsrechts wird die erste Abschrift für den Patienten daher kostenlos sein.

Gesetzlich verankert ist in Art. 17 DS-GVO nunmehr das sog. „Recht auf Vergessenwerden“, das in der Rechtsprechung des Europäischen Gerichtshofs bereits anerkannt war. Von diesem Anspruch auf Löschung der gespeicherten Gesundheitsdaten sind allerdings solche Daten ausgenommen, die zum Zwecke der Gesundheitsvorsorge, für die medizinische Diagnostik, die Versorgung und Behandlung im Gesundheitsbereich oder zur Abwehr von schwerwiegenden Gesundheitsgefahren erforderlich sind oder wenn der Löschungsanspruch die wissenschaftliche Forschung erheblich erschwert oder unmöglich macht. Damit sind in jedem Fall Daten ausgenommen, die Radiologen zum Nachweis der Leistungserbringung, aus Haftpflichtgründen oder zur Erfüllung der Pflichten aus der RöV sowie den berufs- und steuerrechtlichen Regelungen aufbewahren müssen. Bei anderen Datenbeständen bedarf es daher stets einer Prüfung, ob diese von den genannten Ausnahmen umfasst sind.

Pflichten des Radiologen als verantwortlicher Datenverarbeiter

Daneben beinhaltet die DS-GVO weitere Verpflichtungen, die den Radiologen als verantwortlichen Verarbeiter treffen. Verantwortlicher ist gemäß Art. 4 Nr. 7 DS-GVO jede natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Das bedeutet, dass jeder, der Daten für sich verarbeitet, indem er sie erhebt, speichert oder weitergibt, Verantwortlicher im Sinne der DS-GVO sein kann. Die folgenden Verpflichtungen treffen daher sowohl den niedergelassenen Radiologen als auch den im Krankenhaus tätigen, wenn er selbst über Zweck und Mittel der Verarbeitung entscheidet. Wird dies z. B. im Rahmen von radiologischen Kooperationen von zwei oder mehreren Verantwortlichen festgelegt, so sind sie nach Art. 26 DS-GVO gemeinsam verantwortlich. Die Verantwortung behält der Radiologe auch dann, wenn er einen Dritten mit der Verarbeitung

von Gesundheitsdaten beauftragt. Dieser sog. Auftragsverarbeiter ist dabei stets wegen einer drohenden Strafbarkeit vertraglich zur Geheimhaltung zu verpflichten. Bis Ende letzten Jahres machte sich ein Radiologe in vielen Fällen wegen Verletzung der Schweigepflicht strafbar, wenn er ohne Einwilligung des Patienten Daten an Dienstleister wie Cloud-Anbieter weitergab. Die Neufassung des § 203 StGB vom 9. November 2017 regelt nun die Voraussetzungen, unter denen die Inanspruchnahme von externen IT-Dienstleistern strafrechtlich zulässig ist. Ein Arzt macht sich jedoch nach dem neuen § 203 Abs. 4 Satz 2 Nr. 1 StGB strafbar, wenn er nicht dafür Sorge trägt, dass ein Dienstleister z. B. durch Vertrag zur Geheimhaltung verpflichtet wurde und dieser später Patientendaten offenbart.

Informationspflichten

Den Verantwortlichen treffen nach der DS-GVO umfassende Pflichten zur Information des Patienten. Nach Art. 13 DS-GVO muss der Patient im Vorfeld darüber informiert werden, wer für die Verarbeitung verantwortlich ist, was konkret mit den Daten passiert und welche Rechte ihm nach der DS-GVO diesbezüglich zustehen. Im Falle einer Datenschutzverletzung, wie einem Verlust von Daten oder einem „Hackerangriff“, ist die betroffene Person davon gemäß Art. 34 DS-GVO unverzüglich zu benachrichtigen und der Vorfall innerhalb von 72 Stunden der Aufsichtsbehörde zu melden (Art. 32 DS-GVO).

Die Informationspflichten des Radiologen finden ihre Grenze allerdings dort, in denen sie die ärztliche Schweigepflicht berühren. Dies stellt § 29 BSDG nF für die Auskunfts- und Informationspflichten aus Art. 14, 15 und 34 DS-GVO klar und beschränkt auch die behördliche Befugnis aus Art. 58 DS-GVO, Zugang zu gespeicherten personenbezogenen Daten zu erhalten, wenn dies mit § 203 Abs. 1 Nr. 1 StGB in Konflikt steht.

Datenschutz-Folgenabschätzung

Mit der DS-GVO neu eingeführt wurde die sog. Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO. Der Verantwortliche ist danach zur Durchführung einer Folgenabschätzung verpflichtet, wenn – insbesondere bei der Verwendung neuer Technologien – aufgrund der Art und des Umfangs der Verarbeitung voraussichtlich ein hohes Risiko für die Sicherheit der betroffenen Daten besteht. Die Vorschrift benennt auch bestimmte Fallgruppen, bei denen stets von einem solchen Risiko ausgegangen wird. Radiologen trifft immer dann die Pflicht, wenn die Verarbeitung von Gesundheitsdaten im umfangreichen Maße erfolgt. Die Schwelle zur umfangreichen Verarbeitung soll in der Regel nicht überschritten sein, wenn sie Patientendaten betrifft und nur durch einen einzelnen Arzt erfolgt (vgl. Erwägungsgrund 91 DS-GVO). Das bedeutet, dass Krankenhäuser und größere Praxen immer eine Folgenabschätzung durchführen müssen und niedergelassene Radiologen nur davon ausgenommen sind, wenn sie die Praxis alleine führen und lediglich lokal agieren. Zeigt sich dabei, dass die Verarbeitung von Daten ein hohes Risiko zur Folge hätte, muss der Verantwortliche die Aufsichtsbehörde konsultieren.

Wegen des Umgangs mit sensiblen Daten trifft den verantwortlichen Radiologen dagegen gemäß Art. 30 DS-GVO immer die Pflicht zur Führung eines Verzeichnisses über die Verarbeitungstätigkeiten, das der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen ist.

Bestellung eines Datenschutzbeauftragten

Die Frage, ob eine Praxis einen Datenschutzbeauftragten bestellen muss, ist eng mit der Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung verknüpft. Art. 37 DS-GVO normiert bestimmte Fälle, in denen zwingend ein Datenschutzbeauftragter zu bestellen ist und gibt den Mitgliedstaaten darüber hinaus die Möglichkeit, im nationalen Recht für weitere Fälle die Bestellung vorzuschreiben. Davon hat der Bundesgesetzgeber in § 38 Abs. 1 BDSG nF Gebrauch gemacht und schreibt darin zunächst die geltende Rechtslage fort. Wie bisher haben radiologische Praxen einen Datenschutzbeauftragten zu bestellen, wenn in der Regel mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Diese Verpflichtung besteht unabhängig von der Anzahl der beschäftigten Personen, wenn eine Praxis wegen des Umfangs der Verarbeitung von Gesundheitsdaten bereits die Pflicht zur Datenschutz-Folgenabschätzung trifft. In der Regel wird ein niedergelassener Radiologe daher einen Datenschutzbeauftragten zu benennen haben.

Datenübermittlung an Drittstaaten

Sollen im Rahmen von radiologischen Kooperationen Gesundheitsdaten wie radiologische Aufnahmen zur Auswertung oder sonstigen Verarbeitung, z. B. zum Zwecke datenbankbasierter und computergestützter Befundungen oder der Teleradiologie, an Partner in Drittstaaten übermittelt werden, enthält die DS-GVO in Kapitel V besondere Bestimmungen, um den Schutz der betroffenen Daten weiterhin zu gewährleisten. Eine Übermittlung in einen Drittstaat ist danach zulässig, wenn die Kommission entschieden hat, dass ein adäquater Schutz besteht oder der verantwortliche Radiologe durch vertragliche Regelungen sicherstellt, dass durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen, die einen Schutz der Gesundheitsdaten sichern. Abgesehen davon ist die Übermittlung in einen Drittstaat ohne vergleichbares Schutzniveau dann zulässig, wenn die betroffene Person ausdrücklich eingewilligt hat und sie vorher über Risiken der Datenweitergabe informiert worden ist. Aus Gründen der Vorsicht ist es empfehlenswert, grundsätzlich eine Einwilligung des Patienten für eine Datenübermittlung an einen Drittstaat einzuholen.

Fazit

Radiologen werden sich in der Regel allein aus berufsrechtlichen Gründen bereits eingehend mit dem Schutz von Patientendaten befasst haben. Wichtig ist, spätestens bis zum 25. Mai 2018 zu überprüfen, ob die Sicherung der Patientendaten den Anforderungen der DS-GVO genügt und bereits alle notwendigen technischen und organisatorischen Maßnahmen ergriffen worden sind. Insbesondere sollte in den überwiegenden Fällen bereits ein Datenschutzbeauftragter bestellt und eine Datenschutz-Folgenabschätzung vorgenommen worden sein. In jedem Fall müssen bis zum Stichtag ein Verzeichnis der Verarbeitungstätigkeiten erstellt, alle Vorlagen für die Einwilligung der Patienten sowie Verträge mit Dienstleistern in Einklang mit der aktuellen Rechtslage gebracht und bestehende Kooperationen dahingehend überprüft werden, ob die neuen Datenschutzvorgaben noch eingehalten werden.

Prof. Dr. Peter Wigge
Rechtsanwalt
Fachanwalt für Medizinrecht

Sophia K. Meinecke
Rechtsanwältin

Rechtsanwälte Wigge
Scharnhorststraße 40
48 151 Münster
Telefon: (0251) 53 595 – 0
Telefax: (0251) 53 595 – 99
E-Mail: kanzlei@ra-wigge.de
www.ra-wigge.de