Datenschutz in neuem Gewand

Die Schonfrist läuft aus: In rund sechs Monaten greift die EU-Datenschutz-Grundverordnung. Die Bundesregierung hat das Datenschutzgesetz bereits angepasst. Damit warten auf Praxen einige Änderungen.

VON REBEKKA HÖHL

Die neue EU-Datenschutzverordnung soll vor allem die Rechte von Privatpersonen stärken.

© BET_NOIRE / GETTY IMAGES/ISTOCK

NEU-ISENBURG. Abwarten? – das kann für Arztpraxen in Sachen EU-Datenschutz-Grundverordnung (EU-DSGVO) keine Alternative mehr sein. Zwar sind sich selbst viele Experten noch unsicher, wie streng die neue Verordnung im Alltag letztlich ausgelegt werden wird. Dennoch drängt die Zeit. Am 25. Mai 2018 endet die Übergangsfrist, bis zu der die EU-Verordnung im nationalen Recht der Mitgliedsstaaten angewendet werden muss. Von diesem Moment an können auch die – deutlich strengeren – Sanktionen verhängt werden. Grund zur Panik besteht für Praxen allerdings nicht. Es gibt zwar einige Neuerungen, in vielen Fällen ist die neue Verordnung aber einfach ein guter Anlass, die gängige Praxis im Umgang mit Patientendaten zu überprüfen.

Gesetzgeber hat Hand angelegt

Immerhin: Die Bundesregierung ist schon tätig geworden. Sie hat das Bundesdatenschutzgesetz angepasst. Die neue Version, die Bundestag und Bundesrat bereits im Mantel des Datenschutz-Anpassungs- und Umsetzungsgesetzes EU (DSAnpUG-EU) passiert hat, tritt fristgemäß Ende Mai 2018 in Kraft. Damit haben Arztpraxen ein weiteres Hilfsmittel an der Hand. Offiziell bedarf die EU-Ordnung zwar keiner nationalen Umsetzungsgesetze, sie greift vielmehr automatisch in allen EU-Mitgliedsstaaten. Durch die Anpassung des deutschen Datenschutzrechtes werden aber einige Fälle konkreter gefasst.

In Sachen Datenschutzbeauftragter hat die Regierung allerdings die Zügel nicht gelockert: Das EU-Recht sieht diesen nur vor, wenn die Hauptaktivität des Betriebs dem Umfang oder seinem Zweck nach die massenhafte, regelmäßige und systematische Beobachtung von betroffenen Personen erfordert oder das Kerngeschäft eines Unternehmens in der massenhaften Verarbeitung sensibler Daten besteht. Beides ist bei Arztpraxen, deren Kerngeschäft die medizinische Leistungserbringung ist, nicht der Fall. Das deutsche Datenschutzrecht wird allerdings auch künftig bei der Forderung bleiben, dass Betriebe, in denen sich mindestens zehn Mitarbeiter dauerhaft mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen, einen eigenen Datenschutzbeauftragten benennen müssen. Zu diesen Mitarbeitern zählt übrigens auch der Praxisinhaber.

Vier Knackpunkte

Die wichtigste Neuerung im EU-Recht ist die Stärkung der Rechte von Privatpersonen. Dabei gibt es vier Knackpunkte, die Praxen in ihren organisatorischen Abläufen berücksichtigen sollten:

- **Die Einwilligung:** Vor jeglicher Datenverarbeitung muss beim Betroffenen eine Einwilligung eingeholt werden. Das gilt auch für Patienten. Am einfachsten lässt sich dies über den Anamnesebogen regeln. Allerdings gilt: Wird die Einwilligung wie hier in Zusammenhang mit anderen Erklärungen/Sachverhalten eingeholt, muss sie deutlich von diesen abgegrenzt werden, damit der Patient erkennt, worin er einwilligt. Außerdem muss sie in klarer, einfacher Sprache verfasst werden. Wer Patienten auch an Termine erinnern will – etwa per Brief, Mail oder SMS – der sollte dies noch einmal getrennt von der Einwilligung zur normalen Verarbeitung der Daten in der Praxis-EDV aufführen.

- **Zweckbindung der Daten:** Die Praxis darf die beim Patienten erhobenen Daten, dazu zählen auch die Diagnosen, immer nur zum Zweck der Leistungserbringung und Abrechnung erheben. Wer bei privatversicherten Patienten die Abrechnung über einen externen Dienstleister laufen lässt, sollte sich hierfür beim Patienten eine getrennte Einwilligungserklärung einholen. Vorsicht ist bei der Weitergabe von Daten zu Studienzwecken geboten. Auf der sicheren Seite sind Ärzte nur dann, wenn sie den Patienten auch hierzu vorher um sein Einverständnis bitten.

  Allerdings bietet das deutsche Datenschutzrecht (Paragraf 27 DSAnpUG-EU) hier dank Öffnungsklausel in der EU-Verordnung für wissenschaftliche Zwecke etwas mehr Spielraum: In diesem Fall kann auf eine gesonderte Einwilligung verzichtet werden, sofern die Interessen des Verantwortlichen für die Datenverarbeitung die Interessen der betroffenen Person an seinem Ausschluss „erheblich überwiegen". Damit scheint der Gesetzgeber vor allem die künftigen Möglichkeiten von Big-Data-Anwendungen im Hinterkopf gehabt zu haben.

- **Das Recht auf Löschen:** Hauptsächlich getrieben durch die Entwicklungen im Internet und in den Sozialen Medien mit schnellen Unwahrheitsbehauptungen per Knopfdruck, wurde in der EU-Verordnung das Recht von Privatpersonen auf ein Löschen ihrer Daten gestärkt. Für Ärzte ist dies insofern relevant, dass sie vor allem bei einer Datenverknüpfung mit anderen Stellen – etwa in Kooperationen oder wenn sie Praxisdaten in gesicherten Clouds ablegen, schauen müssen, wann und welche Daten evtl. zu löschen sind, wenn ein Patient dies wünscht. Nicht davon betroffen sind allerdings Daten, die Ärzte zum Nachweis der Leistungserbringung oder aus Haftpflichtgründen aufbewahren müssen. Diese Datensicherung darf dann allerdings nur begrenzt und in bestimmten Fällen zugänglich sein.

- **Portabilität der Daten:** Hier werden die Praxis-EDV-Anbieter gefragt sein, geeignete Formate zur Verfügung zu stellen, auch eine Telematikinfrastruktur könnte hier künftig ihren Beitrag leisten. Denn die Patienten haben nach Paragraf 20 der EU-DSGVO das Recht, die sie betreffenden Daten, „in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten" und diese Daten ohne Medienbrüche an Dritte zu übermitteln. Damit machen sich EU-Parlament und -Rat – sicherlich unwissend – auch für die elektronische Patientenakte stark.

Schwachstelle Datensicherung?

Unbedingt prüfen sollten Praxen ihre Datensicherung. Denn künftig sind sie verpflichtet, Verletzungen des Schutzes personenbezogener Daten – wie sie etwa bei Phishing-Attacken vorkommen können – innerhalb von 72 Stunden nach Bekanntwerden an den Bundesdatenschutzbeauftragten zu melden. Dies gilt nur dann nicht, wenn voraussichtlich keine Gefahr von Rechtsgütern der betroffenen Personen besteht. Die vom Schutz-Leck betroffenen Patienten müssen übrigens, wenn sich aus einem Datenklau Nachteile für sie ergeben könnten, ebenfalls informiert werden.

Das heißt, es sollten die technisch gängigen Vorkehrungen zum Schutz von Praxisdaten erfüllt werden: Also Firewall, aktuelle Version des Betriebssystems und Virenscanner.

Wo möglich, sieht die EU-Verordnung auch eine Anonymisierung oder zumindest Pseudonymisierung von Daten vor – dies sollten Praxen vor allem beim elektronischen Austausch von Patientendaten mit anderen Leistungserbringern beherzigen. Der elektronische Arztbrief über einen Kommunikationsdienst wie KV-Connect etwa ist wesentlich sicherer als eine ungeschützte E-Mail oder gar ein Fax.

Als Sanktionen bei Datenschutz-Verstößen drohen nach der EU-Verordnung Unternehmen, zu denen Arztpraxen zu zählen sind, Geldbußen in Höhe von bis zu vier Prozent des gesamten Jahresumsatzes des vorangegangen Geschäftsjahres.

Nur mit Vertrag

- **Ob EDV-Wartung** oder Datensicherung in einem externen Rechenzentrum, der Praxisinhaber bleibt die datenschutzrechtlich verantwortliche Person und muss sich daher davon überzeugen, dass alle Datenschutzregeln eingehalten werden.

- **Über einen Vertrag** der Auftragsdatenverarbeitung kann er sich vom EDV-Dienstleister – also auch vom Praxissoftwareanbieter – bestätigen lassen, dass dieser den Anforderungen der EU-Datenschutzgrundverordnung und zusätzlichen nationalen Regeln genügt.

- **Zusätzlich dürfen** Zertifizierungen, denen sich der Dienstleister stellt, die Prüfung durch den Arzt vor Ort ersetzen.

Die deutsche Datenschutzrechts-Novelle im Netz:
https://tinyurl.com/yaxpl6x9