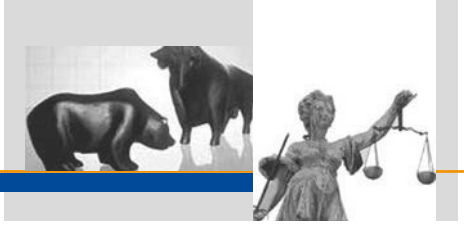


Datenschutz – Alles Neu macht der 25. Mai 2018?!

Auch wenn noch Uneinigkeit herrscht, wie streng die Aufsichtsbehörden die neue EU Datenschutz Grundverordnung hinsichtlich Praxen und der verarbeiteten Gesundheitsdaten auslegen und kontrollieren werden – Abwarten ist den Praxen hinsichtlich der drohenden Sanktionen nicht zu empfehlen. Die Gesetzesänderung bietet auch einen Anlass den Umgang mit Patientendaten in der eigenen Praxis auf Verbesserungsmöglichkeiten zu überprüfen. Denn sicherlich möchte kein Praxis-Inhaber ein Datenleck riskieren und damit als Schlagzeile auf den Titelseiten landen: „Hacker erbeuten hunderte Patientenakten – welchem Arzt können Sie noch vertrauen?"

Mag. (FH) Simone Uecker

Simone Uecker

Ab 25. Mai 2018 gilt die EU Datenschutz Grundverordnung (EU-DSGVO) und ersetzt damit bisher geltendes nationales Recht. Ergänzend wird das Bundesdatenschutzgesetz (BDSG) novelliert und Landesgesetze, wie z. B. das Bayerische Datenschutzgesetz werden überarbeitet. Somit ergibt sich ab Mai 2018 ein neues Bild der Anforderungen an den Datenschutz, die bei Verstößen mit massiven Bußgeldern bis zu 20 Mio. EUR oder 4% des letzten Jahresumsatzes (nicht Gewinn!) bedroht sind. Aus dem bisher „zahnlosen Tiger" der deutschen Datenschutzgesetzgebung wird also in wenigen Tagen eine mächtige Bedrohung für Unternehmen im Allgemeinen und Praxen im Besonderen.

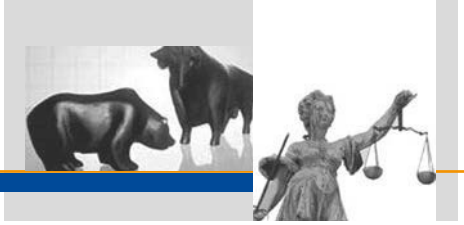
/// Alle Praxen sind betroffen

Die EU-weit einheitlichen Regelungen der EU-DSGVO betreffen jede Verarbeitung (d.h. das Erheben, das Erfassen, die Organisation, die Speicherung etc.) personenbezogener Daten und gelten somit für faktisch jedes Unternehmen, das in der EU tätig wird. Jede Form von Gesundheitsdaten unterliegt nach dem Willen der EU-DSGVO als besonders sensible Daten speziellen Regeln und Anforderungen, mit denen sich alle niedergelassene Ärzte im Detail auseinandersetzen müssen. Verantwortlich ist grundsätzlich der Praxis-Inhaber!

Die spezielle Anforderung an die Bestellung und Veröffentlichung eines Datenschutzbeauftragten betrifft jedoch nur jene Praxen, die mehr als 9 Mitarbeiter mit der automatisierten Datenverarbeitung beschäftigen (der Inhaber zählt mit) oder in denen mehr als ein einzelner Arzt tätig ist!

Ab zwei tätigen Ärzten oder ab dem 10. Mitarbeiter ist also in der Regel ein Datenschutzbeauftragter verpflichtend. Dieser Datenschutzbeauftragte muss übrigens ab 25. Mai 2018 auch der zuständigen Kontrollbehörde gemeldet werden, es muss spezielle Qualifikationen nachweisen und genießt – im Falle der Benennung eines internen Mitarbeiters – auch speziellen Kündigungsschutz.

Sofern ein Datenschutzbeauftragter für die Praxis zu bestellen ist, sollte dieser die Umsetzung der erforderlichen Maßnahmen und Dokumentationserfordernisse möglichst von Beginn an unterstützen, begleiten, beraten und überprüfen. Hier bietet ein qualifizierter externer Datenschutzbeauftragter den Vorteil technische Standards, Verfahren und Best Practices einbringen zu können und als Externer Schwachstellen und Verbesserungspotentiale objektiver einzuschätzen. Die vertraglichen Vereinbarungen mit dem externen Datenschutzbeauftragen sollten im Vorfeld hinsichtlich der zu erwartenden Kosten und des Leistungsumfangs jedoch genau geprüft werden. Vielfach sind langfristige Vertragsdauern üblich und machen somit einen Wechsel bei Unzufriedenheit und mangelnder Erfahrung mit dem Datenschutz in Praxen schwierig. Hingegen kann die Bestellung eines internen Datenschutzbeauftragen zu weitreichenden Konsequenzen führen, z. B. hinsichtlich Freistellung für Datenschutztätigkeiten anstatt der eigentlichen Tätigkeit, kostenintensiven Fortbildungen zur Qualifikation und spezieller Kündigungsschutz. Dies sollte in der Abwägung zwischen den Kosten und Nutzen des externen vs. internen Datenschutzbeauftragten unbedingt Beachtung finden.



/// Schnittpunkte zum QM

Datenschutz wird bereits im gesetzlichen Qualitätsmanagement gefordert, doch die Anforderungen der EU-DSGVO bzw. des BDSG gehen weit über die QM-Anforderungen hinaus. Dennoch können die Datenschutz-Verzeichnisse zugleich als ergänzender QM Bestandteil betrachtet werden und sollten damit auch dem regelmäßigen Aktualisierungszyklus des QM folgen (Plan-Do-Check-Act/PDCA Zyklus). Die regelmäßige Überprüfung der Risikobeurteilung und die Aktualisierung des Datenschutzes in Abstimmung auf geänderte Prozesse und Vorgehensweisen muss somit sichergestellt sein. Hier empfiehlt sich ein regelmäßiger, zumindest jährlicher Audit, der Verbesserungspotentiale aufdeckt. Darüber hinaus sollten Datenschutzaspekte in jeder Prozessänderung und in der Planung neuer Techniken von Anfang an berücksichtigt werden. Wird zum Beispiel die Einführung einer neuen Praxis-Software überlegt, sollten die datenschutzrechtlichen Anforderungen bereits in die Auswahl der geeigneten Software als Kriterium einbezogen werden (privacy by design).

Als Ergänzung zum QM sollten auch jene Prozesse vorab definiert werden, um den umfassenden Rechten der Patienten Rechnung zu tragen. So müssen Auskünfte hinsichtlich der gespeicherten Daten des anfragenden Patienten zeitnah erfüllt werden können und die Datenlöschung nach gesetzlichen Anforderungen müssen sichergestellt sein. Das Abwarten auf den „Ernstfall“ (also z. B. das Vorliegen eines Antrag des Patienten auf Auskunft zu den eignen Daten) kann ohne entsprechende Vorbereitung kostenintensive Unterstützung durch den IT-Dienstleister der Praxis, übermäßigen Arbeitsaufwand und sogar Bußgelder im Falle nicht zeitgerechter Umsetzung nach sich ziehen.

/// Typisches Vorgehen

Ein Grundverständnis über die Anforderungen an die eigene Praxis ist die Basis, die sich jeder Praxis-Inhaber schnellstmöglich erarbeiten muss. Hierzu können Online-Checklisten helfen, wie beispielsweise das Online-Tool zur Selbsteinschätzung des Bayerischen Landesamts für Datenschutzaufsicht (https://www.lda.bayern.de/tool/start.html). Auch die Einholung von Angeboten durch externe Datenschutzbeauftragte oder Praxisberater können einen guten Startpunkt liefern. Doch hier sei auch zur Vorsicht gemahnt: Angebote speziell für Praxen sind Mangelware und Erfahrung mit praktikablen und umsetzbaren Maßnahmen zum Datenschutz in Praxen können leider nur wenige externe Dienstleister vorweisen. Hier kann ein klärendes Gespräch im Vorfeld helfen, das Angebot und die Kompetenz des Dienstleisters richtig einzuschätzen! Die Prüfung des bestehenden Bewusstseins zum Datenschutz in der Praxis, der gesetzlichen Grundlage zur Datenverarbeitung, der bestehenden Dokumentation (beispielsweise im Rahmen des QM), der verwendeten Verfahren zur Datenverarbeitung, der IT-Struktur und der externen Partner sind die ersten Schritte, um die erforderlichen Maßnahmen und Dokumentationserfordernisse zu definieren. Diese To-Do-Liste muss dann schnellstmöglich – idealerweise noch vor dem 25. Mai 2018 – umgesetzt werden.

/// Wer schreibt der bleibt!

Die Anforderungen zur Erfüllung der EU-DSGVO und des BDSG richten sich an jegliche personenbezogene Daten – also Patientendaten ebenso wie Mitarbeiter- und Lieferantendaten.

Ab 25. Mai 2018 gilt das Prinzip der „Rechenschaftspflicht“, also quasi einer Beweislastumkehr, bei der die Praxis nachweisen muss, dass sie ein Gesamtkonzept zur Einhaltung der Datenschutzrechte hat. Die Formvorschriften zu diesem Nachweis regelt die EU-DSGVO sehr detailliert.

Für Praxen bedeutet dies nicht nur eine umfangreiche Dokumentation der eingesetzten Verfahren sowie der eingesetzten Maßnahmen zum Datenschutz und den Nachweis der Schulung und Unterweisung der Mitarbeiter. Auch jeder Datenaustausch mit Externen unterliegt umfassenden Dokumentations- und Kontrollpflichten – dies betrifft z. B. die Zusammenarbeit mit Abrechnungsgesellschaften, externen Abrechnungsexperten, externen Laboren, IT Dienstleistern zur Wartung/Fernwartung von Systemen, die Nutzung von Google Analytics oder die Nutzung externer Speicherlösungen („Cloud“).

Das Vorliegen eines Verzeichnisses von Verarbeitungstätigkeiten, die Verpflichtung von Beschäftigten, die vertraglichen Regelungen mit Auftragsverarbeitern, die Risikobewertung und -analyse sowie ggf. eine Datenschutz-Folgenabschätzung sind einige wesentliche Stichpunkte, die im Rahmen der Rechenschaftspflicht vorgelegt werden müssen.

/// Kleine Investitionen – Große praktische Wirkung

Der kritische Blick auf die einsetzten Verfahren und Prozesse ist zugleich auch eine Chance für die Praxis, um den praktisch angewendeten Datenschutz mit technischen und organisatorischen Maßnahmen zu verbessern.

Bereits kleine Investitionen oder Verhaltensänderungen können große Wirkung bringen und hier liegt einer der wesentlichen Vorteile im strukturierten Zugang zum Datenschutz. Ergänzend zur Erstellung der erforderlichen Dokumentationen und Verzeichnisse sollte auch kurzfristig eine Mitarbeiterschulung durchgeführt werden zur Aktualisierung des Bewusstseins, zur Aufklärung über die gesetzlichen Anforderungen und zur Verpflichtung auf die Umsetzung.

Gesetzeskonformer Datenschutz nach höchsten Standards hat durchaus das Potential sich zum Wettbewerbsvorteil und Marketinginstrument zu entwickeln. Die EU-DSGVO sieht explizit die Schaffung und Förderung von Zertifizierungen im Datenschutz vor.

Allerdings müssen geeignete Zertifikate und Akkreditierungen von Zertifizierungsstellen erst mit in Kraft treten der neuen Gesetzgebung geschaffen werden. Bestehende Zertifizierungen müssen erst überprüft und ggf. hinsichtlich der EU-DSGVO überarbeitet werden.

/// Fazit

Abwarten ist keine Option – Die Datenschutz-Aufsichtsbehörden sind sich der besonderen Sensibilität von Gesundheitsdaten sehr bewusst und ab dem 25. Mai 2018 gilt die EU-DSGVO ohne weitere Übergangsfrist mit ihren hohen Anforderungen an den Umgang mit sensiblen Gesundheitsdaten, Beweislastumkehr zu Lasten der Praxen und empfindlichen Bußgeldern bei Verfehlungen.

Zumindest ein Basis-Check über die gesetzlichen Anforderungen an den Datenschutz in der Praxis muss schnellstmöglich erfolgen, um informiert reagieren zu können! Wer aktiv auf Datenschutz setzt kann sich bei seinen Patienten einen Wettbewerbsvorteil erarbeiten – Transparenz in der Datensicherheit schafft Vertrauen.

AUTORIN
Mag. (FH) Simone Uecker

KONTAKT

4MED Consult
Amselweg 8
82194 Gröbenzell
E-Mail: simone.uecker@4med-consult.de
Internet: www.4med-consult.de