Die EU-DSGVO – ein Ungetüm?

Edith Kron, Sebastian Rinn

Sprechen wir doch mal „kurz“ über Datenschutz und auch über die Schweigepflicht in Ihrer Praxis – ein unbequemes, ein trockenes Thema, aber seit dem 25.05.2018 wichtiger denn je! Eines aber vorweg, es gibt keinen Grund, sich Sorgen zu machen. Das bisher gültige Bundesdatenschutzgesetz hat bereits viele Bereiche ausgezeichnet abgedeckt, sodass es für Praxisinhaber wirklich überschaubare Anpassungen gibt. Es wird lästig, es bringt Arbeit mit sich, aber je besser die Daten schon jetzt geschützt sind, umso weniger Aufwand muss betrieben werden. Veränderungen führen immer erst mal zu Unmut und Unruhe, aber einmal implementiert, werden sie zur Selbstverständlichkeit.

Was sich für viele Praxen ändern wird, ist die Optimierung des bisher bestehenden Datenschutzmanagements. Ob mit oder ohne eigenen Datenschutzbeauftragen, die Handhabung sensibler Daten muss strukturiert werden und jetzt auch überprüf- und nachweisbar sein. Und das seit dem 25.05.2018 nicht als Kür, sondern als Pflichtprogramm. Seitdem ist die neue Datenschutz-Grundverordnung (EU-DSGVO), die das bisher gültige Bundesdatenschutzgesetz (BDSG) ablöst, nämlich verpflichtend anzuwenden. Das BDSG wird jedoch nicht gänzlich verschwinden, sondern als BDSG-neu der DSGVO ergänzend zur Seite stehen. In Kraft ist diese Verordnung tatsächlich bereits seit 2016, nun aber ist sie verbindlich anzuwenden und hat die Vereinheitlichung innerhalb der EU zum Ziel. Die wenigsten werden allerdings die ersten Veröffentlichungen bezüglich der Einführung der DSGVO gelesen bzw. zum Anlass genommen haben, die erforderlichen Maßnahmen sukzessive und ganz ohne Druck umzusetzen. Gratulation an die Vorreiter, sie können sich jetzt entspannt ihrem Tagesgeschehen widmen. Deutschland verfügt allerdings schon sehr lange über einen hohen Datenschutzstandard, sodass hier oft nur marginal nachgebessert werden muss.

Kernpunkte sind die Verarbeitung der erhobenen Daten sowie die erweiterten Rechte und Kontrollmöglichkeiten für die Betroffenen, also derjenigen, deren Daten genutzt werden. Im Falle von Gesundheitsdaten handelt es sich ja zweifellos um besonders schützenswerte Daten. Das Internet überschlägt sich derzeit und die Panik ist groß, da empfindliche Bußgelder, bis zu vier Prozent des Vorjahresumsatzes, angedroht werden. Aber gibt es wirklich einen Grund für diese Panik?

Praxisprozesse unter der Lupe

Panisch muss sicherlich niemand werden, aber ein Gutes hat diese neue Verordnung in meinen Augen schon: Der Umgang mit sensiblen Patientendaten wird in den Arztpraxen jetzt doch mal genauer unter die Lupe

genommen. Im Laufe der Jahre, im alltäglichen Trott, fällt oft gar nicht mehr auf, welche Prozesse eigentlich nicht optimal laufen. Durch die derzeitige Medienpräsenz und die hohen Bußgeldandrohungen wurden Praxisinhaber/Praxismanager jetzt aber doch aufgeschreckt und entdecken vermutlich doch den einen oder anderen Verstoß, der ihnen bisher gar nicht bewusst war.

Es muss also nachjustiert werden! Die Internetseite gehört überarbeitet, das Personal geschult, Verfahrensanweisungen geschrieben und räumliche Gegebenheiten angepasst.

Die DSGVO befasst sich nun auch explizit mit der Datensicherheit und schreibt vor, welche Maßnahmen ergriffen werden müssen, um schützenswerte personengebundene Daten „angemessen", insbesondere auch vor Zugriff von außen, zu schützen. Dass die betroffene Person, deren Daten verarbeitet wurden, jetzt auch einen gesetzlichen Anspruch auf die Löschung dieser Daten hat, darf jedoch nicht verunsichern. Die bisher geltenden Aufbewahrungsfristen sind natürlich immer noch einzuhalten.

Prüfen Sie Ihre Homepage, Ihr Kontaktformular, Ihr Impressum und Ihre Datenschutzerklärung, die für Laien verständlich formuliert sein muss – also kein Juristendeutsch und keine Bandwurmsätze. Viele Praxisinhaber geben die Betreuung ihrer Homepage in externe Hände, verantwortlich bleibt am Ende aber immer der Praxisinhaber selbst. Ebenfalls neu ist die Rechenschaftspflicht. Die Datenverantwortlichen müssen auf Aufforderung nachweisen können, dass die Datenschutz-Grundverordnung auch eingehalten wird.

Datenschutz und Schweigepflicht

Datenschutz in einer Arztpraxis sollte immer schon eine wichtige Rolle gespielt haben, jedoch zeigt der kritische Blick in einigen Praxen, dass es durchaus besser geht. Obwohl die DSGVO primär die Verarbeitung der Daten betrifft, sollte man bei der Umsetzung dieser Verordnung auch einmal mit offenen Augen durch die eigene Praxis gehen, um eventuelle Verstöße gegen die Schweigepflicht bzw. potenzielle Risiken bezüglich des Datenschutzes zu entdecken.

Im stressigen Praxisalltag bleibt leider gelegentlich einiges auf der Strecke. Die Ärzte sind Mediziner und Unternehmer, die angestellten Mitarbeiter Organisationswunder, perfekt in Assistenz und Patientenbetreuung – aber jetzt zusätzlich auch noch die umfangreiche Datenschutz-Grundverordnung zu studieren und umzusetzen, bringt viele an ihre Grenzen.

Liegen Rezepte und/oder Karteikarten auf der Rezeption, auf die andere Patienten, wenn auch nur flüchtig, einen Blick werfen könnten? Sind alle Computer passwort- und vor Einblicken Dritter geschützt – auch im laufenden Betrieb? Liegt bei Anforderungen von Befunden mitbehandelnder Ärzte das Einverständnis des Patienten vor? Können Patienten die Gespräche an der Rezeption zwischen anderen Patienten und Personal mithören, weil das Wartezimmer zugunsten der Ästhetik und modernen Einrichtung von teuren Innenarchitekten offen gestaltet wurde? Auch die Übermittlung von Befunden per unverschlüsselter E-Mail-Programme ist nicht zulässig, erfolgt aber im tagtäglichen Ablauf regelmäßig, um z. B. den Patienten ihre Laborwerte zukommen zu lassen. Sensible Daten könnten so kinderleicht in falsche Hände geraten.

Ebenfalls gängiges Prozedere ist die Herausgabe von Daten (Rezepte, Laborausdrucke) an Angehörige ohne Vorliegen einer schriftlichen Schweigepflichtentbindung. Auch wenn dies jahrelang so praktiziert wurde, weil man die Patienten bzw. deren Angehörigen meist kennt, sollte ab sofort das schriftliche Einverständnis des Patienten vorliegen, damit der Nachweispflicht genüge getan werden kann.

Fehler und Bußgelder vermeiden

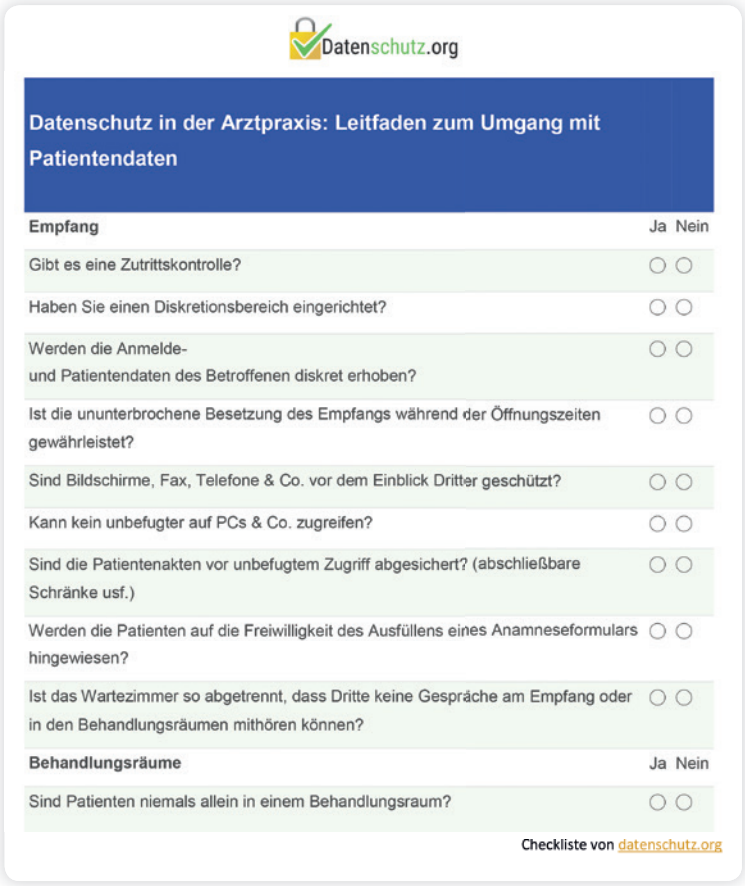
Eine Umstellung von Prozessen, die sich im Laufe der Jahre eingeschlichen haben, wird bei vielen Patienten erst mal zu Unverständnis führen. Aber richtig kommuniziert, wird der Patient letztendlich hoffentlich auch froh sein, dass er seine Daten in verantwortungsvollen Händen weiß.

Aber selbst dort, wo Datenschutz besser funktioniert, lernen wir jetzt, dass immer noch nicht alles beachtet wurde. Da die Bußgelder wirklich empfindlich hoch sind, gilt es, herauszufiltern, wo angepasst, wo der Datenschutz verbessert werden muss – eine Checkliste (ohne Gewähr auf Vollständigkeit) hilft bei den ersten Schritten (Abb. 1).

Was muss also getan werden? In diesem Text können leider nur einige Punkte Erwähnung finden. Sorgen Sie als Praxisinhaber dafür, dass Sie auf dem neusten Stand der Entwicklungen bleiben, denn auch die Aufsichtsbehörden werden erst jetzt mit den Herausforderungen der EU-DSGVO in der praktischen Umsetzung konfrontiert.

Patienten informieren

Die Patienten müssen laut Artikel 13 DSGVO zum Zeitpunkt der (erstmaligen) Erhebung und ggf. Verarbeitung personenbezogener Daten aktiv über die datenschutzrechtliche Verarbeitung informiert werden. Ein gut sichtbar angebrachter Aushang im Wartezimmer oder aber ein Merkblatt, welches den Patienten ausgehändigt wird, scheinen derzeit dafür ausreichend zu sein. Eine entsprechende Dokumentation dieses Prozesses ist jedoch erforderlich.



Datenschutz.org

Datenschutz in der Arztpraxis: Leitfaden zum Umgang mit Patientendaten

Empfang	Ja	Nein
Gibt es eine Zutrittskontrolle?	○	○
Haben Sie einen Diskretionsbereich eingerichtet?	○	○
Werden die Anmelde- und Patientendaten des Betroffenen diskret erhoben?	○	○
Ist die ununterbrochene Besetzung des Empfangs während der Öffnungszeiten gewährleistet?	○	○
Sind Bildschirme, Fax, Telefone & Co. vor dem Einblick Dritter geschützt?	○	○
Kann kein unbefugter auf PCs & Co. zugreifen?	○	○
Sind die Patientenakten vor unbefugtem Zugriff abgesichert? (abschließbare Schränke usf.)	○	○
Werden die Patienten auf die Freiwilligkeit des Ausfüllens eines Anamneseformulars hingewiesen?	○	○
Ist das Wartezimmer so abgetrennt, dass Dritte keine Gespräche am Empfang oder in den Behandlungsräumen mithören können?	○	○
Behandlungsräume	**Ja**	**Nein**
Sind Patienten niemals allein in einem Behandlungsraum?	○	○

Checkliste von datenschutz.org

Tabelle 1: Wo besteht Nachbesserungsbedarf beim Datenschutz – eine Checkliste ohne Gewähr auf Vollständigkeit (abgebildet ein Auszug) bietet www.datenschutz.org

Benötigt jede Arztpraxis einen Datenschutzbeauftragten?

Da lautet die klare Antwort: Jein! Leider sind die Verordnungstexte juristisch etwas vage formuliert, was die Verarbeitung personengebundener Daten betrifft. Allerdings wird derzeit davon ausgegangen, dass lediglich größere Arztpraxen, in denen mindestens zehn Personen (unabhängig vom Status oder der täglichen Arbeitszeit) mit der Verarbeitung personenbezogener Daten beschäftigt sind, einen Datenschutzbeauftragten stellen müssen. Es ist allerdings durchaus denkbar, dass auch kleinere Praxen mit wenigen Mitarbeitern, aber mehr als einem Arzt, einen solchen Datenschutzbeauftragten stellen müssen, z. B. im Falle von besonders risikoreichen Prozessen. Auch hier sind die Formulierungen eher unklar, sodass die zuständige Aufsichtsbehörde für Datenschutz und Informationsfreiheit kontaktiert werden sollte, die länderspezifisch leider hier zu unterschiedlichen Einschätzungen kommt, für die eigene Praxis jedoch eine Aussage treffen wird.

Die Kontaktdaten des Datenschutzbeauftragten müssen schriftlich der zuständigen Aufsichtsbehörde gemeldet und den Patienten zugänglich gemacht werden, z. B. in der Datenschutzerklärung auf der Internetpräsenz und auf dem Patientenmerkblatt/-aushang. Es muss nicht zwingend ein externer Datenschutzbeauftragter benannt werden, sondern es darf durchaus ein besonders geschulter Mitarbeiter der Praxis sein, der über die notwendige Fachkunde verfügt und auch Wissen über die IT-Infrastruktur besitzt. Diese benannte Person muss nicht vorgeschrieben an zertifizierten Lehrgängen teilnehmen, allerdings ist der Praxisinhaber in der Verantwortung, die Fachkunde des Datenschutzbeauftragten nachweisen zu können, und dies geht zwingend mit entsprechenden Fortbildungen einher.

Wegen eines möglichen Interessenkonflikts kann der Praxisinhaber selbst nicht sein eigener Datenschutzbeauftragter werden, diese Aufgabe muss intern oder extern delegiert werden.

Als interner Datenschutzbeauftragter kann man in eine recht schwierige Position innerhalb der Praxis geraten, und das sollte bei der Wahl einer fachlich und charakterlich geeigneten Person berücksichtigt werden. Die umzusetzenden Änderungen müssen praktikabel sein und den Ärzten und Mitarbeitern vermittelt werden. Änderungen sind meistens unbequem und stoßen bei Kollegen (und auch Vorgesetzten) oft auf wenig Verständnis. Mit diesem Widerstand muss ein interner Datenschutzbeauftragter umgehen können.

In dieser Position genießt man übrigens besonderen Kündigungsschutz, der dem von Betriebsratsmitgliedern gleichgesetzt ist. In der DSGVO, die europaweite Gültigkeit hat, findet sich dieser Passus allerdings nicht, der Sonderkündigungsschutz ist im begleitenden BDSG-neu verankert.

Was sind eigentlich personenbezogene Daten?

In einer Arztpraxis sind es natürlich in erster Linie die Gesundheitsdaten des Patienten, die außerdem auch noch zu den besonders schützenswerten Daten gehören. Name, Adresse, Geburtsdatum, Telefonnummer und E-Mail-Adresse – aber z. B. auch die IP-Adresse gehören darüber hinaus zu den personenbezogenen Daten (Urteil des BGH v. 16.05.2017, Az. VI ZR 135/13), deren Verarbeitung nachweisbar sein muss. Nicht nur Patientendaten unterliegen dem besonderen Schutz, auch muss auf Verlangen nachgewiesen werden können, wie z. B. Personaldaten, Bewerberdaten etc. verarbeitet und geschützt werden.

Nachweis verordnungskonformer Datenverarbeitung

Es muss schriftlich erfasst werden (dies kann auch elektronisch erfolgen), wer Zugriff auf welche Daten hat, wie

mit diesen Daten verfahren wird und welche Speicherfristen gelten. Für jeden Prozess mit personenbezogenen Daten sollte eine Verfahrensanweisung erstellt werden, aus der deutlich hervorgeht, wie und von wem diese Daten verarbeitet werden (Abb. 2). Achtung: Das Führen des sogenannten „Verfahrensverzeichnisses" ist in der DSGVO nicht geregelt, allerdings die Nachweisbarkeit. Daher wird die Erstellung von Verzeichnissen dringend empfohlen, um seiner Nachweisbarkeitspflicht überhaupt nachkommen zu können. Vorlagen dafür findet man z. B. auf der Internetpräsenz der KBV oder unter www.bvdnet.de/muster-fuer-verzeichnisse-gemaess-art-30/

Beispiele für Verfahrensnachweise sind z. B. die in- und externe Abrechnung, Datenübermittlung an externe Labore, E-Mail-Verarbeitung, Praxissoftware, Wartungsunternehmen, Aktenvernichtung, Kontaktformulare der Webseiten, Steuerberater, Personalverwaltung etc.

In Fällen, in denen personenbezogene Daten von externen Unternehmen (Labore, externe Abrechnungsstellen, Aktenvernichtung, externe Rechenzentren, Hosting-Anbieter, Google Analytics etc.) weiterverarbeitet werden, muss mit diesen Unternehmen ein Vertrag zur Auftragsdatenverarbeitung (ADV) geschlossen werden. Darin sollte der externe Anbieter Angaben zur DSGVO-konformen Verarbeitung der Daten dokumentieren und welche technisch-organisatorischen Maßnahmen (TOM) ergriffen wurden, um die sensiblen Daten zu schützen.

© photoschmidt / Shutterstock.com

Datenschutz-Folgenabschätzung?

Auch hierzu sind die Meinungen vielfältig, und rechtssichere, allgemeingültige Informationen werden bisher nicht zur Verfügung gestellt. Der Erwägungsgrund 91 der DSGVO beschreibt dazu folgendermaßen: „[...] Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt. In diesen Fällen sollte eine Datenschutz-Folgenabschätzung nicht zwingend vorgeschrieben sein."

Es gibt jedoch in vielen Arztpraxen durchaus besonders risikobehaftete Prozesse, z. B. die Vernichtung von Datenmaterial durch externe Anbieter. Die zuständigen Aufsichtsbehörden werden aber auch dazu eine individuelle Einschätzung vornehmen. Auch hier wird empfohlen, sich bezüglich fraglicher Prozesse von der zuständigen Aufsichtsbehörde beraten zu lassen und die Auskunft dann umzusetzen. Sollten Datenschutz-Folgenabschätzungen notwendig sein, bedeutet dies jedoch eigentlich auch die Bestellung eines Datenschutzbeauftragten, auch bei kleiner Praxisstärke, da risikoreiche Prozesse stattfinden.

Müssen Einwilligungen der eigenen Beschäftigten eingeholt werden?

Daten, die der Arbeitgeber benötigt, um das Beschäftigungsverhältnis überhaupt adäquat durchführen zu können, bedürfen keiner besonderen Einwilligung der Mitarbeiter. Allerdings wäre ein Einverständnis eigentlich schon erforderlich, wenn z. B. ein Geburtstagskalender im Aufenthaltsraum ausgehängt wird, in dem die Geburtstage der Mitarbeiter eingetragen werden. Diesbezüglich reicht aber das Einverständnis meiner Einschätzung nach auch mündlich. Jedoch sollten alle mündlich erfolgten Einverständniserklärungen gewissenhaft dokumentiert werden, um im Falle einer Prüfung erneut die Nachweispflicht erfüllen zu können.

Meldepflicht für Datenschutzverstöße

Durch die DSGVO sind die Regelungen zur Meldung bei Datenschutzverstößen oder Datenpannen deutlich verschärft worden (auch ein versehentlich falsch gesendeter Arztbrief gehört dazu!). Geregelt ist dort, dass die zuständige Aufsichtsbehörde (innerhalb von 72 Stunden) sowie die betroffenen Personen informiert werden müssen. Die betroffenen Personen erhalten eine Empfehlung, wie mögliche Folgen abgemildert werden können, die Aufsichtsbehörde eine Schilderung der ergriffenen Gegenmaßnahmen.

VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

AUSFÜLLBEISPIEL

Das Muster ist beispielhaft ausgefüllt; aufgeführt sind zwei Verarbeitungstätigkeiten.

VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN
Rechtliche Grundlage: Artikel 30 Absatz 1 Datenschutz-Grundverordnung
Angaben zum Verantwortlichen
Name: Praxis am Europaplatz Anschrift: Europaplatz 1a, 23456 Platzstadt Telefon: 0123 456789 E-Mail: praxis@europaplatz.de Internet-Adresse: www.europaplatzpraxis.de
Angaben zur Person des Datenschutzbeauftragten
Vorname und Name: Sabine Müller Anschrift: Europaplatz 1a, 23456 Platzstadt Telefon: 0123 456788 E-Mail: datenschutzbeauftragte@europaplatz.de
Verarbeitungstätigkeit
Datum der Anlegung: 20. März 2018 Datum der letzten Änderung: 21. März 2018
Bezeichnung der Verarbeitungstätigkeit
Einsatz und Nutzung des Praxisverwaltungssystems
Zwecke der Verarbeitung
Ärztliche Dokumentation, Abrechnung der ärztlichen Leistungen, Qualitätssicherung, Terminmanagement
Beschreibung der Kategorien betroffener Personen
Patienten
Beschreibung der Datenkategorien
Gesundheitsdaten, gegebenenfalls auch genetische Daten
Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden
Intern: Praxispersonal Extern: andere Ärzte / Psychotherapeuten, Kassenärztliche Vereinigungen, Krankenkassen, der Medizini-

Tabelle. 2: Für jeden Prozess mit personenbezogenen Daten sollte eine Verfahrensanweisung erstellt werden, aus der deutlich hervorgeht, wie und von wem diese Daten verarbeitet werden (abgebildet ein Auszug). © KBV

Muss die EDV angepasst werden?

Wurden bereits technische Schutzmaßnahmen für die eigene Praxis-EDV ergriffen, um Datenverlust bzw. den Zugriff Unbefugter auf die Daten zu verhindern, sind Sie hier bereits gut aufgestellt. Dazu gehören u. a. regelmäßige Back-ups, die jedoch nicht physisch permanent an das Praxisnetzwerk angebunden sein sollten. Netzwerkfestplatten stellen kein sicheres Back-up dar! Ratsam sind Band- oder RDX-Laufwerke mit verschlüsselten Back-ups, welche an einem sicheren Ort (feuerfester Safe) zu verwahren sind. Weiterhin sollte ein sicheres internes Netzwerk gewährleistet sein, auf das Unbefugte nicht einfach zugreifen können (Trennung von Gast- und Praxis-WLAN-Netzen! Keine Mitarbeiter-Handys im Praxis-WLAN!). Das Netzwerk muss durch eine wirkungsvolle Firewall gegen Zugriffe aus dem Internet geschützt sein. Auf alle Rechner gehören aktuelle Virenschutzprogramme. Ein weiterer wichtiger Punkt ist die Wahl des Serverstandorts. Dieser sollte in einem nicht öffentlichen Raum, am besten mit permanentem Zugangsschutz und bei größeren Praxen auch mit Zugangskontrolle, untergebracht werden. Die Arbeitsrechner in der Praxis müssen beim Verlassen des Arbeitsplatzes (und sei es nur kurz) wirkungsvoll mit einem Passwort gesperrt werden, um Unbefugten zu keiner Zeit Zugriff zu ermöglichen. In der Praxisverwaltungssoftware müssen personenbezogene Accounts für die Mitarbeiter mit individueller Rechteverwaltung angelegt werden können. Das in vielen Praxen praktizierte Verfahren, die gleichen Zugangsdaten für alle Benutzer einzusetzen, entspricht nicht den aktuellen Anforderungen!

Dürfen Daten weiterhin an externe Verrechnungsstellen weitergeleitet werden?

Natürlich. Der Patient erteilt dafür vorher sein schriftliches Einverständnis. Jedoch dürfen nur abrechnungsrelevante Daten zur Verfügung gestellt werden. Jeder darüber hinausgehende Eintrag ist nach § 203 StGB strafbar. Arztpraxen, die ihrer Abrechnungsstelle die vollständige Patientenakte zukommen lassen oder dem Abrechnungsunternehmen vollen Zugriff auf die Patientendaten geben, müssen diesen Prozess umgehend überarbeiten.

Fazit

Grund zur Panik? Nein! Grund zur Anpassung interner Prozesse? Unbedingt sofort!

Sollte bisher noch keine Anpassung erfolgt sein, gilt es jetzt, diese schnell in die Wege zu leiten. Das Thema erfordert außerdem zwingend, up to date zu bleiben, da sich im Laufe der nächsten Monate sicherlich die jetzt noch offenen Fragen klären werden. Bei Fragen, die eigene Praxis betreffend, unterstützt die zuständige Aufsichtsbehörde. Eine Übersicht der zuständigen Aufsichtsbehörden findet man z. B. hier: www.datenschutz-wiki.de/Aufsichtsbehörden_und_Landesdatenschutzbeauftragte

Kontakt

Edith Kron
Kron Praxisprojekte
Haroldstraße 22
40213 Düsseldorf
Tel.: 0157 81275816
edith@kron-praxisprojekte.de

Infos zur Autorin

Sebastian Rinn
Zertif. Datenschutzbeauftragter