Fragen und Antworten zur Datenschutz-Grundverordnung

Wo finde ich die für mich zuständige Aufsichtsbehörde?

- In jedem EU-Land wachen unabhängige Aufsichtsbehörden über die Umsetzung der Vorgaben. In Deutschland sind das die Datenschutzbeauftragten der 16 Bundesländer. Sie haben unter anderem das Recht, Informationen von Firmen, öffentlichen Stellen, aber eben auch von Arztpraxen einzuholen, die sie für ihre Kontrollfunktion benötigen.

- Die für Sie zuständige datenschutzrechtliche Aufsicht:

  Name: Sächsischer Datenschutzbeauftragter
  Anschrift: Devrientstraße 1, 01067 Dresden

Muss ich ein Verzeichnis von Verarbeitungstätigkeiten nur einmal erstellen oder in regelmäßigen Abständen?

- Sie sollten Ihr Verzeichnis immer auf dem aktuellen Stand halten und hin und wieder prüfen, ob es angepasst werden muss. Treten Sie zum Beispiel einem neuen Versorgungsvertrag bei, bei dem Daten von Patienten erhoben, gespeichert oder an Dritte weitergeleitet werden, prüfen Sie, ob Sie Ihr Verzeichnis um diese Tätigkeit ergänzen müssen.

Benötigen Gemeinschaftspraxen wie Einzelpraxen ab zehn Personen einen Datenschutzbeauftragten?

- Ja, denn aus datenschutzrechtlicher Perspektive ist nicht entscheidend, ob es sich um eine Einzelpraxis und um eine andere Praxisform handelt. Die Vorgaben sind dieselben.

In unserer Praxis arbeiten zwei Ärzte und sechs Medizinische Fachangestellte. Benötigen wir einen Datenschutzbeauftragten?

- In der Regel benötigen nur größere Praxen und MVZ einen Datenschutzbeauftragten. Dies ist der Fall, wenn mindestens zehn Personen regelmäßig Daten automatisiert, zum Beispiel am Computer, verarbeiten. Dabei werden die in einer Praxis tätigen Ärzte ebenso gezählt wie deren Mitarbeiter.

Ab zehn Personen muss ein Datenschutzbeauftragter bestellt werden: Müssen es Vollzeitstellen sein oder geht es um die Anzahl der Personen?

- Entscheidend ist die Anzahl der Personen, die in der Praxis tätig sin. Somit ist unerheblich, ob die Personen in Voll- oder Teilzeit oder als Auszubildende beschäftigt sind.

Was unterscheidet interne und externe Datenschutzbeauftragte?

- Wird ein Mitarbeiter mit der Aufgabe betraut, spricht man von einem internen Datenschutzbeauftragten. Der Mitarbeiter steht unter Kündigungsschutz und hat das Recht auf Ausstattung mit den erforderlichen Arbeitsmitteln oder Fortbildung.

- Praxisinhaber können aber auch einen externen Dienstleister beauftragen. Bei dieser Variante fallen zusätzliche Kosten an, zugleich wird das Haftungsrisiko minimiert, denn bei Fehlern im Umgang mit dem Datenschutz haftet der externe Dienstleister. Welche Variante gewählt wird, muss der Praxisinhaber entscheiden.

Eine Mitarbeiterin unserer Praxis soll die Aufgabe des Datenschutzbeauftragten übernehmen. Benötigt sie eine besondere Aus- oder Fortbildung?

- Nach den gesetzlichen Vorgaben muss der Datenschutzbeauftragte die nötige Fachkunde und Zuverlässigkeit haben. Dies bedeutet, dass er die gesetzlichen Regelungen kennen und sicher anwenden muss. Eine Vorgabe, wie sich Ihr(e) Mitarbeiter(in) das nötige Wissen aneignet, gibt es nicht.

- Dies kann im Rahmen einer Schulung, aber auch im Selbststudium erfolgen.

Muss ich meine Patienten eine Bestätigung unterschreiben lassen, dass sie die Datenschutzbestimmungen der Praxis gelesen und verstanden haben oder reicht ein Aushang?

- Sie sind verpflichtet, Ihre Patienten darüber zu informieren, was mit den erhobenen Daten passiert. Die Information muss in erster Linie Angaben zum Zweck sowie zur Rechtsgrundlage der Datenverarbeitung enthalten.

- Um alle Patienten zu erreichen, empfiehlt sich ein Aushang in der Praxis, der gut sichtbar angebracht werden sollte. Auch ein Informationsblatt, das im Wartezimmer ausgelegt wird, ist möglich. So kann sich jeder Patient informieren. Eine Unterschrift oder andere Art der Bestätigung ist aber nicht erforderlich.

Wir bekommen oft Anfragen von Krankenkassen oder Gesundheitsämtern: Dürfen wir hier Auskunft geben?

- Personenbezogene Daten dürfen nur übermittelt werden, wenn eine Rechtsgrundlage es erlaubt. Dies kann eine Einwilligung des Patienten sein, mit der er einer Schweigepflichtentbindung zustimmt, oder eine Rechtsnorm, zum Beispiel eine gesetzliche Bestimmung im SGB V oder eine Regelung im Bundesmantelvertrag-Ärzte.

- Anfragen von Krankenkassen auf einem vertragsärztlichen Formular beruhen auf so einer Rechtsnorm, deshalb müssen Praxen solche Anfragen beantworten. Anders bei formlosen Anfragen: Bei diesen muss die Krankenkasse angeben, aufgrund welcher Rechtsgrundlage sie Auskunft haben will. Ansonsten sind Praxen nicht verpflichtet zu antworten.

- Auch Anfragen anderer Stellen, etwa von Berufsgenossenschaften, Sozialgerichten oder Gesundheitsämtern, müssen eine Rechtsgrundlage haben. Es kann zum Beispiel sein, dass personenbezogene Daten an Gesundheitsämter übermittelt werden müssen, weil für bestimmte Krankheiten Meldepflicht aufgrund des Infektionsschutzgesetzes besteht.

Was muss ich bei einem Datenschutzvorfall tun?

- Verlust des Praxis-Laptops, Hackerangriff oder unbewusste Veröffentlichung von personenbezogenen Daten im Internet: Bei Datenschutzvorfällen muss der Datenschutzbeauftragte der Praxis darüber informiert werden. Stellt er eine Verletzung des Schutzes personenbezogener Daten fest, muss innerhalb von 72 Stunden eine Meldung an die Datenschutzaufsichtsbehörde erfolgen.

Fragen und Antworten zur Datenschutz-Grundverordnung (KVS – intern, abgestimmte Antworten unseres Datenschutzbeauftragten Herrn Kluge)

Ärztliche Aufzeichnungen sind für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren, soweit nicht nach gesetzlichen Vorschriften eine längere Aufbewahrungspflicht besteht (§ 10 Abs. 3 der Berufsordnung der Sächsischen Landesärztekammer). Bedeutet dies, dass nach Ablauf der zehn Jahre diese Dokumentationen zu löschen/vernichten sind?

Artikel 5 Abs. 1 lit. e EU-DSGVO ist zu entnehmen, dass Daten personenbezogen nur so lange gespeichert werden dürfen, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Daraus resultiert, dass ärztliche Aufzeichnungen von Patientendaten nach Ablauf der zehn Jahr zu löschen bzw. zu vernichten sind, es sei denn, dass eine längere Aufbewahrung explizit bestimmt ist, wie z. B. bei der Röntgenverordnung.
Hier muss der Arzt im Zweifelsfall selbst einschätzen, ob er Aufzeichnungen zu Patienten länger aufbewahrt (etwa aufgrund eventueller Haftungsansprüche). Sinnvoll ist die Nutzung der Archivierungsfunktion im PVS und die Sperrung der Daten für die Bearbeitung nach Ablauf der Aufbewahrungsfrist.

Namentlicher Aufruf von Patienten in Praxis auch nach DSGVO statthaft?

Wird als unproblematisch eingeschätzt, da der Name einer Person ein normales Identifikationsmerkmal darstellt und insofern als nicht besonders schutzwürdig einzustufen ist. Über den namentlichen Aufruf hinaus, sollte jedoch sichergestellt werden, dass andere Patienten keine weiteren Informationen über den Aufgerufenen erhalten, beispielsweise sollte beim Aufruf nicht genannt werden, für welche Behandlung oder Erkrankung der Patient in der Praxis ist.
Unterscheidung zur Behörde (bei der Nummern gezogen werden): Es besteht zwischen Patient und Arzt ein besonderes Vertrauensverhältnis, so dass es unverhältnismäßig wäre, dieses über das „Ziehen von Nummern“ (Der Patient als bloße Nummer) zu beeinträchtigen. Zwischen Behörde und Bürger besteht ein solches Vertrauensverhältnis nicht.

Befundanforderung

Fordert ein Hausarzt von Fachärzten zur Vervollständigung seiner Patientenakten Befunde an, bedarf es der Einwilligung durch den Patienten.

Laborleistungen

Für die Befunde aus beauftragten Laborleistungen hält auch der sächsische Datenschutzbeauftragte eine separate schriftliche Einwilligung des Patienten für entbehrlich. Hier kann auf schlüssiges Handeln (etwa die Abgabe von Blut oder Urin) durch den Patienten abgestellt werden. Da der Patient selbst zum Labor keinen direkten Kontakt hat, wäre insofern eine Probenabgabe entbehrlich, wenn der Patient die Auswertung durch den Hausarzt/behandelnden Arzt nicht wünscht. Demnach weiß der Patient, dass die Werte an den behandelnden Arzt für die Auswertung übermittelt werden.

E-Mails zur Terminvergabe oder für sonstige Kommunikation

Wird dieses Instrument benutzt, sollte der Patient darauf hingewiesen werden, dass es sich um einen ungeschützten Übermittlungsweg handelt. Wünscht der Patient eine Antwort via E-Mail sollte er im Vorfeld seine Einwilligung dazu gegeben haben.

Einwilligungserklärung zur Patienteninformation?

Für eine diesbezügliche Einwilligung durch den Patienten gibt es keinen Raum, da eine Verweigerung der Einwilligung bedeuten würde, dass kein Behandlungsvertrag zustande kommt. Zudem basieren die Ausführungen in der Patienteninformation auf gesetzlichen Regelungen, die die Behandlung zumindest der Versicherten in der GKV regeln.