Der „Letzte-Hilfe-Baukasten“ im Datenschutz für radiologische Praxen

Datenschutz-Grundverordnung

Autorin: Heike Mareck, Rechtsanwältin und externe Datenschutzbeauftragte, Dortmund, www.kanzlei-mareck.de

Machen wir uns nichts vor: Es wird knapp, wenn radiologische Praxen sich erst jetzt mit dem Datenschutz beschäftigen. Denn am 25.5.18 entfaltet die europäische Datenschutz-Grundverordnung (kurz DS-GVO) ihre volle Wirkung. Und zeitgleich tritt noch das überarbeitete Bundesdatenschutzgesetz (BDSG n.F.) in Kraft. Radiologische Praxen, die in der Vergangenheit ihre Prozesse datenschutzrechtlich erfasst und dokumentiert haben, müssen wenig befürchten, sie müssen jetzt alles „nur“ einmal in neue Vorlagen und Vorgaben umsetzen. Alle anderen sollten Gas geben. Nachfolgend daher zehn Tipps aus dem „DS-GVO-Letzte-Hilfe-Baukasten“.

Projektverantwortlichen auswählen

Datenschutz ist Chefsache. Natürlich kann der Chef Aufgaben delegieren. Jemand in der Praxis, zum Beispiel eine MTRA, muss sich sofort und unverzüglich mit den neuen Datenschutzregelungen vertraut machen. Tipp: Wählen Sie direkt eine Vertretung mit aus, damit sichergestellt ist, dass die Fristen der DS-GVO auch eingehalten werden, wenn der Hauptansprechpartner mal verhindert (Urlaub, Krankheit etc.) ist.

Datenschutzbeauftragten benennen

Radiologische Praxen müssen einen Datenschutzbeauftragten berufen, sofern zehn oder mehr Mitarbeiter, inklusive Teilzeitbeschäftigte, Aushilfen etc., ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Auch wenn es weniger als zehn Mitarbeiter sind, kann auf einen Datenschutzbeauftragten nicht verzichtet werden, wenn die Praxis Daten verarbeitet, für die eine sogenannte Datenschutz-Folgenabschätzung notwendig ist. Als Datenschutzbeauftragte kommt auch eine MTRA in Frage (aber nie der Chef, da eine Interessenkollision vermutet wird), aber auch ein externer Datenschutzbeauftragter.

Zunächst Ist-Analyse durchführen

Wo werden „personenbezogene Daten“ verarbeitet - sprich gespeichert, genutzt, übermittelt und gelöscht? In einer radiologischen Praxis geht es in der Regel um

Patientendaten, Beschäftigtendaten und Daten von Partnern (z. B. Lieferanten).

Verzeichnis der Verarbeitungstätigkeiten anlegen

Ihre Praxis muss identifizieren und dokumentieren, welche personenbezogenen Daten sie verarbeitet, woher diese stammen und an wen sie weitergegeben werden. In einem Verzeichnis muss der Datenweg angegeben werden, von der Erhebung über die Speicherung bis

hin zur Nutzung. Fassen Sie dafür zunächst Tätigkeiten, die demselben Zweck dienen, zusammen (so zum Beispiel Praxisverwaltungssystem für die Patientendokumentation oder die Personalverwaltung beim Führen der Personalakten etc.). Das Verarbeitungsverzeichnis ist stets aktuell zu halten. Ein solches Verzeichnis war bereits nach dem alten BDSG Pflicht. Ein Musterformular hierfür finden Sie auf der Website der Kassenärztlichen Bundesvereinigung (KBV) unter http://www.kbv.de/html/datensicherheit.php

Datenschutz-Folgenabschätzung durchführen – wenn nötig

Diese ist durchzuführen, wenn die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko zur Folge hat. Dies gilt zum Beispiel, wenn die Daten eine Identifizierung und Kategorisierung der Person ermöglichen nach Kriterien wie Sexualität, Krankheiten, Finanzen, rassische oder ethnische Herkunft oder politische Ansichten.

Neue Prozesse etablieren

Als Praxis müssen Sie sicherstellen, dass Sie Auskunftsanfragen von Betroffenen vollständig im vorgeschriebenen Zeitraum beantworten können. Neben den bisherigen Einsichtsrechten in medizinische Akten sieht Art. 15 DS-GVO ein Auskunftsrecht für die betroffene Person vor. Regeln Sie also, wer zukünftig die Auskünfte erteilt und wie die Vollständigkeit der Akten (Papierform, elektronische Art, Protokollierung) aussehen sollte. Auch wichtig: Das Erarbeiten von Löschkonzepten und festen Mechanismen, etwa zu den Meldepflichten bei Datenpannen.

Verträge zur Auftragsverarbeitung checken

Sie müssen jederzeit in der Lage sein, Auskunft über Ihre Auftragsverarbeitungen (zum Beispiel Datenträgervernichtung, externe Lohn- und Gehaltsbuchhaltung) geben zu können. Die bestehenden Auftragsverarbeitungsverträge sollten darauf kontrolliert werden, ob sie auch datenschutzkonform sind. Hiervon ausgenommen ist aber der Steuerberater oder die Rechtsanwaltskanzlei, diese sind keine Auftragsverarbeiter.

Datenschutz-Erklärungen überarbeiten

Sie haben eine Website, nutzen die sozialen Netzwerke, wie Facebook, Twitter, versenden einen Newsletter oder erinnern per Telefon oder SMS an Termine? Dann müssen Sie Ihre bestehende Datenschutz-Erklärung unbedingt aktualisieren. Diese muss überarbeitet werden, hier drohen derzeit fast die höchsten Gefahren abgemahnt zu werden. Da diese bei den sogenannten freien Berufen stets weitergehende Informationen auf der Website erforderlich machen, sollten Sie sich hier juristischen Beistand suchen.

Einwilligungen prüfen

Das Erfassen, Bearbeiten, Speichern etc. von Patientendaten ist gesetzlich gestattet. Aber in besonderen Fällen muss der Patient zustimmen, zum Beispiel bei der Einbeziehung einer privatärztlichen Verrechnungsstelle. In diesen Fällen müssen Praxen nachweisen können, dass die Patienten eine Einwilligungserklärung zur Datenverarbeitung unterschrieben haben. Wichtig: Ab dem 25.5.2018 müssen die Einwilligungserklärungen einen Hinweis darauf enthalten, dass der Patient jederzeit seine Einwilligung wiederrufen kann. Sehen Sie sich daher noch einmal Ihren bisherigen Einwilligungsprozess an und überprüfen Sie, ob Ihre Einwilligungen datenschutzkonform formuliert sind, gesondert eingeholt und archiviert wurden.

Mitarbeiterschulungen

Praxen müssen die eigenen Mitarbeiter so schulen, dass sie in der Lage sind, ihre Datenschutzaufgaben zu erfüllen. Die Schulungen sind zu dokumentieren.