Datenschutz wird wichtiger

Schon heute spielt Datenschutz in Arztpraxen eine große Rolle. Ab Mitte Mai müssen Ärzte und Psychotherapeuten gemäß der neuen Datenschutz-Grundverordnung (DSGVO) jedoch auch nachweisen, dass sie die datenschutzrechtlichen Vorgaben einhalten, zum Beispiel gegenüber Aufsichtsbehörden. Zudem müssen sie Patienten zum Datenschutz in der Praxis informieren. Bei Verstößen sieht die DSGVO deutlich höhere Sanktionen vor als bisher üblich.

Schutz von Patienten und Mitarbeitern im Fokus

Ziel der Datenschutz-Grundverordnung ist es, personenbezogene Daten in allen gesellschaftlichen Bereichen zu schützen. Sie vereinheitlicht die Regeln zur Verarbeitung personenbezogener Daten.

In der Praxis zählen dazu: **Erheben und Abfragen, Ordnen, Speichern, Anpassen und Ändern, Auslesen und Weiterleiten, Löschen und Vernichten der Daten**.

Dabei geht es insbesondere um den Schutz von Patientendaten und der Personaldaten der Praxismitarbeiter. Rein private Daten des Praxisinhabers, wie etwa auf dem Rechner gespeicherte Kontaktdaten von Familien und Freunden, sind von den neuen Regeln indes ausgenommen, erläutert die KBV [1,2].

Checkliste: Das benötigen Praxen ab 25. Mai

Alle Praxen:

- **Verzeichnis von Verarbeitungstätigkeiten, das die Praxis auf Verlangen der Aufsichtsbehörde vorlegen kann**: Darin werden Tätigkeiten beziehungsweise Vorgänge erfasst, bei denen in der Praxis personenbezogene Daten verarbeitet werden. Beispiele hierfür sind die Nutzung des Praxisverwaltungssystems oder das Führen von Personalakten.
- **Interner Datenschutzplan mit einer Aufstellung der technischen und organisatorischen Maßnahmen in der Praxis:** Dieser legt zum Beispiel klare Verhaltensweisen bei der Erfassung von Patientendaten fest und regelt Verantwortlichkeiten oder Zugriffsbeschränkungen für Mitarbeiter.
- **Patienteninformation zum Datenschutz in der Praxis:** Praxen müssen Patienten in der Regel zum Zeitpunkt der Datenerhebung darüber informieren, was mit ihren Daten passiert. Hierfür bieten sich laut KBV ein Aushang in der Praxis, ein Informationsblatt im Wartezimmer oder auch ein Hinweis auf der Praxis-Homepage an.
- **Vereinbarung zur Auftragsverarbeitung mit Softwareanbietern und anderen Dienstleistern, die auf Patienten- oder Mitarbeiterdaten zugreifen können**: Die Auftraggeber müssen sich davon überzeugen, dass der Dienstleister die Vorschriften des Datenschutzes einhält und entsprechende technische und organisatorische Maßnahmen durchführt. Die Firmen sollen dem Auftragsnehmer dazu ein Datenschutzsiegel oder eine Zertifizierung, zum Beispiel ISO/IEC 27001, vorlegen.

Praxen und MVZ ab 10 Personen:

- **Einen internen oder externen Datenschutzbeauftragten,** wenn in der Praxis mindestens zehn Personen regelmäßig personenbezogene Daten automatisiert

verarbeiten, zum Beispiel am Empfang. Die Aufgabe des Datenschutzbeauftragten kann ein fachlich qualifizierter Mitarbeiter (nicht der Praxisinhaber) oder ein externer Datenschützer übernehmen. Name und Kontaktdaten müssen dem Landesdatenschutzbeauftragten mitgeteilt werden.

Datenschutz-Grundverordnung: Erforderliche Maßnahmen und mögliche Sanktionen

Erforderliche Maßnahmen in Ausnahmefällen

- In seltenen Fällen kann eine Datenschutz-Folgenabschätzung nötig sein, zum Beispiel wenn große Mengen an personenbezogenen Daten verarbeitet oder die Praxisräume systematisch videoüberwacht werden. Bestehen möglicherweise hohe Risiken bei der Datenverarbeitung, ist eine externe Datenschutzprüfung zu empfehlen, heißt es bei der KBV. In Zweifelsfall empfiehlt es sich, dies beim Landesdatenschutzbeauftragten zu erfragen. Diese Praxen benötigen unabhängig von der Anzahl der Mitarbeiter ebenfalls einen Datenschutzbeauftragten.
- Praxen, die mit Einwilligungserklärungen des Patienten arbeiten, zum Beispiel bei der Weitergabe von Daten an eine privatärztliche Verrechnungsstelle, müssen die Erklärung um einen Hinweis auf Widerrufbarkeit ergänzen.
- Praxen, die eine Internet- oder Facebook-Seite anbieten, sollten die Datenschutzerklärung prüfen und gegebenenfalls anpassen; dies gilt ebenso, wenn personenbezogene Daten zum Beispiel über Kontaktformulare oder für einen Praxis-Newsletter erfasst und gespeichert werden.

Härtere Sanktionen als bisher

Das Ausmaß der Sanktionen richtet sich vor allem nach der Schwere und der Dauer des Vorfalls sowie nach dessen Auswirkungen auf die Patienten, erklärt die KBV. [1] Leichte Verstöße werden zunächst zu einer Beratung führen. Dennoch sollten Praxen alle nötigen Vorkehrungen treffen.

So sieht die DSGVO bei Verstößen generell deutlich härtere Sanktionen vor als bisher üblich. Die Aufsichtsbehörden können im Einzelfall Geldbußen von bis zu 20 Millionen Euro verhängen. Liegt kein Verzeichnis von Verarbeitungstätigkeiten vor, können bis zu zehn Millionen Euro oder bis zu zwei Prozent des Jahresumsatzes verlangt werden. Möglich sind zudem Schadensersatzforderungen von Betroffenen inklusive Schmerzensgeld, zum Beispiel wegen Rufverletzung.

CHECKLISTE: DAS IST IN PUNCTO DATENSCHUTZ

Das ist ab 25. Mai 2018 zu tun:

Nach der neuen Datenschutz-Grundverordnung der Europäischen Union müssen Ärzte und Psychotherapeuten nicht nur die datenschutzrechtlichen Vorgaben einhalten, sondern dies auch nachweisen.

ALLE PRAXEN UND MEDIZINISCHEN VERSORGUNGSZENTREN

- Erstellen eines Verzeichnisses von Verarbeitungstätigkeiten, die in der Praxis anfallen.

- Zusammenstellung der technischen und organisatorischen Maßnahmen, die die Praxis zum Schutz von personenbezogenen Daten ergreift.

- Bereitstellung einer Patienteninformation zum Datenschutz in der Praxis, zum Beispiel als Aushang in den Praxisräumen und auf der Praxis-Website.

- Verträge zur Auftragsverarbeitung mit Softwareanbietern und anderen Dienstleistern anpassen oder neu abschließen. Solche Verträge sind notwendig, wenn Auftragnehmer auf Patienten- oder Mitarbeiterdaten zugreifen können.

GROSSE PRAXEN UND MEDIZINISCHE VERSORGUNGSZENTREN

- Beauftragen eines Datenschutzbeauftragten, wenn in der Praxis mindestens zehn Personen regelmäßig personenbezogene Daten automatisiert verarbeiten, zum Beispiel am Empfang oder bei der Abrechnung. Übernimmt ein Mitarbeiter diese Aufgabe, benötigt dieser eventuell eine Schulung.

- Melden der Kontaktdaten des Datenschutzbeauftragten der Praxis an die zuständige Aufsichtsbehörde.

DAS KANN AUSERDEM ERFORDERLICH SEIN

- In seltenen Fällen kann eine Datenschutz-Folgenabschätzung nötig sein, z.B., wenn große Mengen an personenbezogenen Daten verarbeitet oder die Praxisräume systematisch videoüberwacht werden. Diese Praxen benötigen unabhängig von ihrer Größe ebenfalls einen Datenschutzbeauftragten.

- Praxen, die mit Einwilligungserklärungen des Patienten arbeiten, zum Beispiel zur Weitergabe von Daten an eine privatärztliche Verrechnungsstelle, müssen die Erklärung um einen Hinweis auf Widerrufbarkeit ergänzen.

- Praxen, die eine Internet- oder Facebook-Seite anbieten, sollten die Datenschutzerklärung prüfen und gegebenenfalls anpassen; dies gilt ebenso, wenn personenbezogene Daten zum Beispiel über Kontaktformulare oder für einen Praxis-Newsletter erfasst und gespeichert werden. Informationen, die Ihnen bei der Erledigung der Aufgaben helfen sollen, finden Sie in der Praxisinformation der KBV

www.kbv.de/datenschutz

.