BUNDESZAHNÄRZTEKAMMER

Bundeszahnärztekammer
Arbeitsgemeinschaft der Deutschen Zahnärztekammern e.V. (BZÄK)
Chausseestraße 13
10115 Berlin
Telefon: +49 30 40005-0
Fax: +49 30 40005-200
E-Mail: info@bzaek.de
www.bzaek.de

Merkblatt

Das neue Datenschutzrecht

Merkblatt für Zahnärzte

Das neue Datenschutzrecht - Merkblatt für Zahnärzte

Am **25.5.2018** tritt die neue europäische Datenschutz-Grundverordnung (DSGVO) in Kraft. Gleichzeitig wird das alte durch das neue Bundesdatenschutzgesetz (BDSG) ersetzt. Von wenigen Ausnahmen abgesehen, gilt das neue Datenschutzrecht auch für Zahnarztpraxen.

1. Was heißt eigentlich Datenschutz?

Die Verarbeitung von personenbezogenen Daten in der Zahnarztpraxis ist nur erlaubt mit Einwilligung der betroffenen Person oder aufgrund einer gesetzlichen Erlaubnis. Dieses Prinzip gilt nicht nur für Patientendaten, sondern für alle personenbezogenen Daten. Auch Beschäftigtendaten und Lieferantendaten sind durch das Datenschutzrecht geschützt.

Der Datenschutz ergänzt die zahnärztliche Schweigepflicht, die sich aus dem Berufsrecht und dem Strafrecht ergibt. Schweigepflichtig sind alle Mitarbeiter der Praxis, aber auch Dienstleister, die Kenntnis von Patientendaten erlangen. Nach dem jüngst geänderten § 203 Strafgesetzbuch (StGB) muss der Praxisinhaber jeden Dienstleister zur Geheimhaltung verpflichten.

2. Das „Basispaket": Fünf Maßnahmen zum besseren Datenschutz

a. Betrieblicher Datenschutzbeauftragter

Auf jedem Rechner einer Zahnarztpraxis befinden sich sensible Patientendaten. Das heißt jedoch nicht, dass jede Praxis einen Datenschutzbeauftragten haben muss. Es gilt in der Regel wie bisher: Sind mindestens zehn Personen mit der Datenverarbeitung beschäftigt, muss ein Datenschutzbeauftragter benannt werden.

Ob und unter welchen Voraussetzungen einer der Inhaber der Praxis zugleich Datenschutzbeauftragter sein kann, ist unter den Datenschutzrechtlern umstritten. Unklar ist auch, ob ein IT- Leiter zum Datenschutzbeauftragten benannt werden kann. Optimal ist die Bestellung eines angestellten Zahnarztes oder eines anderen Mitarbeiters mit gewisser IT-Affinität. Auch die Benennung eines **externen Datenschutzbeauftragten** ist möglich.

Für eine Datenschutzbehörde ist es leicht zu prüfen, ob eine Zahnarztpraxis einen Datenschutzbeauftragten hat. Jede entsprechende Praxis sollte daher bis zum 25.5.2018 einen Datenschutzbeauftragten benennen. Fällt die Auswahl schwer, sollte man beachten, dass ein schwach geeigneter Datenschutzbeauftragter allemal besser ist als kein Datenschutzbeauftragter.

Der Datenschutzbeauftragte ist der Praxisleitung direkt unterstellt, in der Wahrnehmung seiner gesetzlichen Aufgaben aber **nicht weisungsgebunden**. Er überwacht die Datenverarbeitungsprozesse in der Praxis, unterrichtet und berät die Praxisleitung und wirkt auf die Einhaltung des Datenschutzrechts hin. Zudem soll er die an den Verarbeitungsvorgängen beteiligten Zahnärzte und Mitarbeiter sensibilisieren und schulen. Gibt es eine Beschwerde, ist der Datenschutzbeauftragte **die erste Anlaufstelle** für die Datenschutzbehörde.

Die Kontaktdaten des Datenschutzbeauftragten, wie mindestens Adresse, Telefonnummer und E-Mail nicht aber der Name des Datenschutzbeauftragten, sind innerbetrieblich als auch beispielsweise durch Angabe auf der Homepage der Praxis außerbetrieblich zu veröffentlichen. Die Kontaktdaten sind ebenfalls einschließlich des Namens des Datenschutzbeauftragten gegenüber der Datenschutzbehörde als Aufsichtsbehörde mitzuteilen.

b. Verzeichnis von Verarbeitungstätigkeiten

Die DSGVO schreibt für **jedes Datenverarbeitungsverfahren** ein Verzeichnis von Verarbeitungstätigkeiten vor.

Als Verfahren gelten beispielsweise:

- (elektronische) Patientenakten;
- (Zahn-)arztinformationssysteme;
- elektronische Diktier- und Spracherkennungsprogramme;
- Buchhaltungssoftware;
- Software zur Versendung und Verwaltung von E-Mails;
- Adressdatenbanken;
- Software zur Terminverwaltung;
- elektronische Personalakten.

Für die Verzeichnisse von Verarbeitungstätigkeiten ist keine bestimmte Form vorgeschrieben. Sie können als **Word- oder Exceldatei** geführt werden und müssen folgende Angaben enthalten:

- den Namen und die Kontaktdaten der Praxis;
- den Namen und die Kontaktdaten des betrieblichen Datenschutzbeauftragten (falls erforderlich);
- die Zwecke der Datenverarbeitung;
- die Art der Personen, deren Daten verarbeitet werden (Patienten, Beschäftigte oder Lieferanten);
- die Art der verarbeiteten Daten;
- die möglichen Empfänger der Daten, an die Daten übermittelt werden (z.B. Krankenkassen und Verrechnungsstellen);
- die Übermittlung von Daten in die USA oder in ein anderes Land außerhalb der EU (z. B. bei der Nutzung von Webmail-Diensten oder anderen Cloud-Diensten); Löschfristen;
- Maßnahmen der Datensicherheit.

Die Erstellung der Verzeichnisse ist ein **mühsamer Prozess**, da es meist gar nicht so einfach ist, den Überblick darüber zu gewinnen, welche Datenverarbeitungsprozesse es in der Praxis gibt. Dies gilt umso mehr, wenn Zahnärzte und Mitarbeiter beruflich Smartphones, Tablets und Laptops nutzen. Auch Programme auf derartigen Endgeräten können als Datenverarbeitungsverfahren zählen, für die die Pflicht zur Führung eines ent-sprechenden Verzeichnisses gilt.

Wenn erstmalig Verzeichnisse von Verarbeitungstätigkeiten angelegt werden, ist die nach aller Erfahrung mit einem **hilfreichen Klärungsprozess** verbunden. Denn stets sind die Verarbeitungszwecke zu definieren, und die Festlegung von Löschfristen gibt Anlass, Daten nicht unüberlegt für alle Ewigkeit auf Datenträgern „verstauben" zu lassen. Wenn Verzeichnisse von Verarbeitungstätigkeiten angelegt werden, ist dies ein guter Anlass, über die Effizienz, Nachvollziehbarkeit und Sinnhaftigkeit der eigenen Datenverwaltung nachzudenken. Dies kann nicht nur dem Schutz von Patientendaten und der Datensicherheit dienen, sondern auch der Effizienz der Arbeitsabläufe in der Praxis.

c. „Gap Analysis"

Die Verzeichnisse von Verarbeitungstätigkeiten sind der Ausgangspunkt für eine „Lückensuche", die in den DSGVO-Umstellungsprozessen „Gap Analysis" genannt wird.

Jedes einzelne Verfahren muss in der „Gap Analysis" überprüft werden im Hinblick auf mögliche Schwachstellen. Zu diesen Schwachstellen zählen vor allem:

- **Datensparsamkeit**: Ist die Vorhaltung von Daten und deren Verarbeitung tatsächlich notwendig?
- **Datenrichtigkeit:** Ist gewährleistet, dass Patientendaten stets auf dem neuesten Stand sind, Fehler berichtigt und unrichtige Daten gelöscht werden?

- **Rechtmäßigkeit:** Ist die Datenverarbeitung überhaupt erlaubt? Dient die Datenverarbeitung der Erfüllung des Behandlungsvertrages, der Gesundheitsvorsorge oder dem Schutz der öffentlichen Gesundheit? Gibt es Einwilligungen der Patienten?
- **Löschfristen:** Werden Daten gelöscht, sobald sie nicht mehr benötigt werden? Gibt es eine Löschroutine, die eine rechtzeitige Löschung auch unter Berücksichtigung von anderen Löschfristen gewährleistet?
- **Zugriffsrechte:** Haben Mitarbeiter ausschließlich Zugriff auf Daten, die sie für ihre jeweiligen Aufgaben benötigen?
- **Zugangskontrolle:** Sind die Rechner in den Praxisräumen ausreichend gegen den Zugang durch Unbefugte geschützt? Gibt es eine Zugangssicherung und Passwörter für die Rechner, Tablets und Smartphones der Praxis? Gibt es abschließbare Praxisräume und Aktenschränke?
- **Schutz gegen Hacker und Malware:** Gibt es eine Firewall? Sind aktuelle Virenscanner installiert?

Am Ende jeder „Gap Analysis" steht ein **Maßnahmenplan** mit dem Ziel der möglichst umfassenden Daten-schutzkonformität aller Verfahren.

d. Datensicherheit

„Technische und organisatorische Maßnahmen" sind zu ergreifen, um die Sicherheit der in der Praxis verarbeiteten Personendaten zu gewährleisten.
Folgende Maßnahmen sind vorgeschrieben:

- **Verschlüsselung:** Soweit möglich, sollen personenbezogene Daten verschlüsselt werden. Es empfiehlt sich daher beispielsweise, die Verschlüsselung von E-Mails mit Verschlüsselungsprogrammen zu ermöglichen.
- **Pseudonymisierung:** Wenn „Klarnamen" nicht gebraucht werden, sind diese Namen unkenntlich zu machen und durch Pseudonyme zu ersetzen.
- **Stabilität:** Die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme ist auf Dauer sicherzustellen. Hierzu bedarf es einer fachkundigen Einschätzung einer IT-Fachfirma oder eines fachkundigen Mitarbeiters.
- **Wiederherstellbarkeit:** Verarbeitungsprozesse müssen gegen Datenverlust geschützt werden durch eine fachgerechte Datensicherung. Auch hierzu bedarf es der Unterstützung durch IT-Fachleute.
- **Regelmäßige Überprüfung:** Eine regelmäßige Routineprüfung ist für die Datensicherheit gleichfalls vorgeschrieben.

Wie in anderen Lebensbereichen gibt es auch beim Datenschutz keine „100 %-ige" Sicherheit. Dementsprechend schreibt das neue Datenschutzrecht keinen „optimalen Schutz" vor, sondern ein **„angemessenes Schutzniveau"**, das anhand der bestehenden Risiken und des Stands der Technik zu bestimmen ist. Investitionen, die außer Verhältnis zu der Größe der Praxis stehen, fordert die DSGVO/das BDSG nicht.

Dokumentationspflichten werden im neuen Recht groß geschrieben. Es sollte daher ein Papier geben, das die Bemühungen um „technische und organisatorische Maßnahmen" der Datensicherheit und deren Durchführung belegt.

e. „Papierform"

Bei der Datenverarbeitung bedienen sich Zahnärzte auch der Unterstützung durch **Dienstleister** aller Art.

Dies können IT-Servicefirmen sein, externe Abrechnungs- oder Buchhaltungsbüros oder auch Cloud- Dienstleister für die Textverarbeitung, Terminverwaltung oder Spracherkennung. All diese Verfahren waren bereits nach bisherigem Recht als **Auftragsdatenverarbeitung** anzusehen mit der Folge, dass es schriftlicher Verträge bedurfte. Nach neuem Recht bleibt dies so, allerdings müssen bestehende Verträge an das neue Datenschutzrecht an-

gepasst werden. Selbstverständlich müssen dabei auch weiterhin andere rechtliche Anforderungen, wie sie sich z.B. aus dem jeweiligen Berufsrecht ergeben, eingehalten werden. Sofern noch keine Verträge existieren, sollte ein Vertragsschluss vor dem 25.5.2018 nachgeholt werden.

Zum notwendigen „Paperwork" gehören auch **Datenschutzinformationen**. Die Informationspflichten sind nach neuem Recht wesentlich umfangreicher, als dies bisher der Fall war. Die Datenschutzbestimmungen auf **Praxis-Websites müssen** überarbeitet werden. Zudem empfehlen sich allgemeine **„Hinweise zur Datenverarbeitung"**, die jeder Patient erhalten und unterschreiben sollte. Dass sich entsprechende Formulare einbürgern werden, ist sicher.

Die neuen **Informationspflichten** umfassen unter anderem

- den Namen und die Kontaktdaten der Praxis;
- den Namen und die Kontaktdaten des betrieblichen Datenschutzbeauftragten;
- die Art der verarbeiteten Daten;
- die Zwecke der Datenverarbeitung;
- die Art der Personen, deren Daten verarbeitet werden (Patienten, Beschäftigte oder Lieferanten);
- die möglichen Empfänger der Daten, an die die Daten übermittelt werden (z. B. Krankenkassen und Verrechnungsstellen);
- die Übermittlung von Daten in die USA oder in ein anderes Land außerhalb der EU (z. B. bei der Nutzung von Webmail-Diensten oder anderen Cloud-Diensten);
- Löschfristen;
- die datenschutzrechtlichen Ansprüche des Patienten (Auskunft, Berichtigung, Löschung, Sperrung, Widerspruchsrecht, Datenübertragbarkeit);
- das Recht des Patienten auf Widerruf einer Einwilligung;
- das Recht des Patienten auf Beschwerde bei einer Datenschutzbehörde.

3. Weitere Schritte zur Datenschutzkonformität

Nach dem ersten „Maßnahmenpaket" gibt es noch weitere Schritte zur Datenschutzkonformität, die ratsam erscheinen:

- **Betroffenenrechte:** In der Praxis sollte es klare
- Regeln geben, wie zu verfahren ist, wenn beispielsweise ein (früherer) Patient sein gesetzliches Recht auf „Datenübertragbarkeit" geltend macht und die Herausgabe aller Daten verlangt, die die Praxis über ihn gespeichert hat.
- **Meldepflichten:** Jeder Datenschutzverstoß muss in Zukunft innerhalb von maximal 72 Stunden bei der zuständigen Datenschutzbehörde gemeldet werden. Auch wenn es für Ärzte einige Ausnahmen von der Meldepflicht gibt, gilt die Meldepflicht grundsätzlich auch für Zahnarztpraxen. Verliert ein Mitarbeiter sein Dienst-Handy und befinden sich auf dem Handy Patientendaten, kann dies zu einer Meldepflicht führen. Der bloße Verstoß gegen die Meldepflicht kann ein Bußgeld nach sich ziehen. Daher muss jedenfalls gewährleistet werden, dass die Praxisleitung oder der Datenschutzbeauftragte zeitnah von jeder „Datenpanne" erfahren.
- **Datenschutzrichtlinien:** In praxisinternen Richtlinien sollten die Praxisinhaber klare Regeln für die Datenverarbeitung aufstellen mit dem Ziel des rechtskonformen Handelns.

4. Bußgelder nach dem neuen Datenschutzrecht

Bei Verstößen gegen das neue Recht drohen Bußgelder bis zu 20 Mio. EUR. Eine Übergangsfrist gibt es nach dem 25.5.2018 nicht. Praxen, deren Datenverarbeitung nach dem 25.5.2018 nicht dem neuen Recht entsprechen, müssen mit Bußgeldern rechnen. Dies umso mehr, als neue, **förmliche Beschwerdebefugnisse** der Betroffenen eingeführt werden. Beschweren sich in Zukunft Mitarbeiter oder Patienten bei der zuständigen Datenschutz-

behörde, darf die Behörde nicht untätig bleiben und muss der Beschwerde nachgehen. Auch strafbewehrte Sanktionen sind bei Verstößen gegen das Datenschutzrecht möglich.