Das neue Datenschutzrecht
Merkblatt für Zahnarztpraxen

Landeszahnärztekammer Thüringen

Die Verarbeitung personenbezogener Daten in der Zahnarztpraxis ist generell nur mit Einwilligung der betroffenen Person oder aufgrund einer gesetzlichen Erlaubnis gestattet. Dieses Grundprinzip gilt nicht nur für Patientendaten, sondern für alle personenbezogenen Daten. Somit sind beispielsweise auch Daten von Beschäftigten und Dienstleistern geschützt.

In jeder Zahnarztpraxis ergänzt der gesetzliche Datenschutz die ärztliche Schweigepflicht, die sich aus dem Berufsrecht und dem Strafrecht ergibt. Schweigepflichtig sind alle Mitarbeiter der Praxis, aber auch Dienstleister, die Kenntnis von Patientendaten erlangen. Deshalb muss der Praxisinhaber jeden Dienstleister zur Geheimhaltung verpflichten.

Europäische Datenschutz-Grundverordnung
www.lzkth.de/de/datenschutz-01

Bundesdatenschutzgesetz
www.lzkth.de/de/datenschutz-02

Berufsordnung der Thüringer Zahnärzte
www.lzkth.de/de/datenschutz-03

Datenschutzleitfaden der BZÄK und KZBV
www.lzkth.de/de/datenschutz-04

Mustervorlage: Verpflichtungserklärung auf das Datengeheimnis für Praxismitarbeiter
www.lzkth.de/de/datenschutz-05

Anlagen zur Verpflichtungserklärung auf das Datengeheimnis für Praxismitarbeiter
www.lzkth.de/de/datenschutz-051
www.lzkth.de/de/datenschutz-052
www.lzkth.de/de/datenschutz-053
www.lzkth.de/de/datenschutz-054
www.lzkth.de/de/datenschutz-055
www.lzkth.de/de/datenschutz-056

Mustervorlage: Verfahrensanweisung zur Umsetzung des Datenschutzes für Praxismitarbeiter
www.lzkth.de/de/datenschutz-06

Die angegebenen Internet-Verweise leiten Sie bequem zu den wichtigsten Merkblättern, Mustertexten und Musterverträgen innerhalb des Qualitätsmanagementsystems ZQMS weiter. Das ZQMS steht im Internet allen Thüringer Zahnärztinnen und Zahnärzten kostenfrei zur Verfügung.

Melden Sie sich einfach mit Ihrem Benutzernamen und Ihrem Passwort an oder registrieren Sie sich erstmalig mit wenigen Klicks als neuer Nutzer unter ***www.zqms.de****.*

Maßnahmen für einen besseren Datenschutz

1. Datenschutzbeauftragten benennen

Nicht jede Zahnarztpraxis muss einen Datenschutzbeauftragten bestellen. **Sind mindestens zehn Personen ständig mit der automatisierten Datenverarbeitung beschäftigt, muss die Praxis einen betrieblichen Datenschutzbeauftragten haben.** In der Ermittlung der Personenzahl ist der (oder die mehreren) Praxisinhaber mit einzurechnen. Ebenso ist die Art der Beschäftigung (Zahnarzt oder ZFA, Voll- oder Teilzeit, Auszubildende o. a.) unerheblich. Wichtig ist auch, dass die automatisierte Verarbeitung personenbezogener Daten nicht Hauptaufgabe der beschäftigten Person sein muss, um „ständig“ zur Personenanzahl hinzugezählt werden zu müssen.

Hinweise zur Ermittlung der Personen, die mit Datenverarbeitung in der Zahnarztpraxis befasst sind
www.lzkth.de/de/datenschutz-07

Mustervorlage: Erfassung der Anzahl datenverarbeitender Personen in der Zahnarztpraxis
www.lzkth.de/de/datenschutz-08

Rechtliche Hinweise zur Bestellung eines Datenschutzbeauftragten
www.lzkth.de/de/datenschutz-09

Mustervorlage: Bestellung eines Datenschutzbeauftragten für die Zahnarztpraxis
www.lzkth.de/de/datenschutz-10

Die Datenschutzbehörde kann leicht prüfen, ob eine Praxis einen Datenschutzbeauftragten besitzt. Jede entsprechende Praxis sollte daher bis zum 25. Mai 2018 einen Datenschutzbeauftragten benennen und der in Thüringen zuständigen Stelle mitteilen:

Thüringer Landesbeauftragter für
den Datenschutz und die Informationsfreiheit
Postfach 900455
99107 Erfurt

www.tlfdi.de

Die Kontaktdaten des Datenschutzbeauftragten, mindestens die Adresse, Telefonnummer und E-Mail – nicht aber der Name – müssen sowohl innerbetrieblich als auch außerbetrieblich (beispielsweise durch die Angabe auf der Praxis-Webseite) veröffentlicht werden. Gegenüber der Datenschutzbehörde als Aufsichtsbehörde sind die Kontaktdaten einschließlich des Namens des Datenschutzbeauftragten mitzuteilen.

Die Tätigkeit des Datenschutzbeauftragten darf **in keinem Interessenkonflikt mit der eigentlichen Tätigkeit in der Zahnarztpraxis** stehen. Das führt dazu, dass weder der Praxisinhaber noch der IT-Verantwortliche der Praxis gleichzeitig Datenschutzbeauftragte sein können.

Optimal ist die Bestellung eines angestellten Zahnarztes oder eines anderen Mitarbeiters mit einer gewissen IT-Affinität. Auch die Benennung eines externen Datenschutzbeauftragten ist möglich. 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 Prozesse der Datenverarbeitung in der Praxis, unterrichtet und berät die Praxisleitung, wirkt auf die Einhaltung des Datenschutzrechts hin und sensibilisiert die an den Verarbeitungsvorgängen beteiligten Zahnärzte und Mitarbeiter. Gibt es eine Beschwerde, ist der Datenschutzbeauftragte die erste Anlaufstelle der Datenschutzbehörde in der Praxis.

Mustervorlage: Zuweisung von Verantwortlichkeiten im Datenschutz an Praxismitarbeiter
www.lzkth.de/de/datenschutz-11

Mustervorlage: Schulungsplan im Datenschutz für Praxismitarbeiter
www.lzkth.de/de/datenschutz-12

Mustervorlage: Nachweis über Datenschutzmaßnahmen in der Zahnarztpraxis
www.lzkth.de/de/datenschutz-13

2. Verzeichnis der Datenverarbeitungen erstellen

Das neue Datenschutzrecht schreibt ein Verzeichnis der einzelnen Datenverarbeitungstätigkeiten vor. Dazu zählen beispielsweise die Arbeit mit

- (elektronischen) Patientenakten
- Zahnarztinformationssystemen
- elektronischen Diktier- und Spracherkennungsprogrammen
- Buchhaltungssoftware
- Software zur Versendung und Verwaltung von E-Mails
- Adressdatenbanken
- Software zur Terminverwaltung
- elektronischen Personalakten.

Für die Verzeichnisse der Verarbeitungstätigkeiten ist keine bestimmte Form vorgeschrieben. Die Verzeichnisse können daher als Word- oder Excel-Datei geführt werden. Sie müssen folgende Angaben enthalten:

- Namen und die Kontaktdaten der Praxis
- Namen und die Kontaktdaten des betrieblichen Datenschutzbeauftragten (falls erforderlich)
- Zwecke der Datenverarbeitung
- Art der Personen, deren Daten verarbeitet werden (Patienten, Beschäftigte oder Lieferanten)
- Art der verarbeiteten Daten
- mögliche Empfänger der Daten, an die Daten übermittelt werden (zum Beispiel Krankenkassen und Verrechnungsstellen)
- Übermittlung von Daten in ein Land außerhalb der EU (zum Beispiel bei der Nutzung von E-Mail-Diensten oder Cloud-Diensten)
- Löschfristen
- Maßnahmen der Datensicherheit.

Die Erstellung der Verzeichnisse ist ein mühsamer und zunächst zeitraubender Prozess. Meist gibt es bislang keinen schriftlich fixierten Überblick darüber, welche Datenverarbeitungsprozesse in der Praxis alltäglich laufen. Dies gilt umso mehr, wenn Zahnärzte und Mitarbeiter beruflich Smartphones, Tablets und Notebooks nutzen. Auch Software-Programme auf diesen technischen Geräten können als Datenverarbeitungsverfahren zählen, für die die Pflicht zur Führung eines entsprechenden Verzeichnisses gilt.

Wenn Verzeichnisse von Verarbeitungstätigkeiten erstmalig angelegt werden, ist dies nach aller Erfahrung mit einem hilfreichen Klärungsprozess verbunden: Stets sind die Verarbeitungszwecke zu definieren. Auch die Festlegung von Löschfristen gibt Anlass, Daten nicht unüberlegt für alle Ewigkeit auf Datenträgern aufzubewahren. Das Anlegen dieser Verzeichnisse der Verarbeitungstätigkeiten ist also ein guter Moment, um über Effizienz, Nachvollziehbarkeit und Sinnhaftigkeit der eigenen Datenverwaltung nachzudenken. Dies dient nicht nur dem Schutz der Patientendaten und der Datensicherheit, sondern auch den effizienten Arbeitsabläufen in der Praxis.

Mustervorlage: Verzeichnis der Datenverarbeitungen
www.lzkth.de/de/datenschutz-14

3. Schwachstellen im Datenschutz aufdecken

Zugleich können diese Verzeichnisse der Datenverarbeitungstätigkeiten ein Ausgangspunkt für die Suche nach Schwachstellen im Datenschutz der Zahnarztpraxis sein. Dazu 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 anderer Löschfristen gewährleistet?
- **Zugriffsrechte:** Haben Mitarbeiter ausschließlich Zugriff auf jene 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 Schadsoftware:** Gibt es eine Firewall? Sind aktuelle Virenscanner installiert?

Am Ende dieser Analyse steht ein **Maßnahmenplan mit dem Ziel der möglichst umfassenden Datenschutzkonformität** aller Verfahren.

Informationen zur Datenorganisation
www.lzkth.de/de/datenschutz-15

Mustervorlage: Risikobeurteilung für Datenschutz-Folgenabschätzungen
www.lzkth.de/de/datenschutz-16

Rechtliche Hinweise zur Datenschutz-Folgenabschätzung
www.lzkth.de/de/datenschutz-17

4. Datensicherheit gewährleisten

Mit technischen und organisatorischen Maßnahmen muss die Praxis die Sicherheit der verarbeiteten Personendaten gewährleisten. Folgende Maßnahmen sind vorgeschrieben:

- **Verschlüsselung:** Soweit möglich, sollen personenbezogene Daten verschlüsselt werden. Dabei empfiehlt sich beispielsweise die Verschlüsselung von E-Mails mit Verschlüsselungsprogrammen.
- **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 eines IT-Fachdienstleisters oder eines fachkundigen Mitarbeiters.
- **Wiederherstellbarkeit:** Verarbeitungsprozesse müssen durch eine fachgerechte Datensicherung gegen Datenverlust geschützt werden. 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 hundertprozentige 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 zur Größe der Praxis stehen, fordert die DSGVO nicht.

Dokumentationspflichten werden im neuen Recht großgeschrieben. Es sollte daher ein Papier geben, das die fortlaufenden Bemühungen der Praxis um „technische und organisatorische Maßnahmen“ der Datensicherheit und deren Durchführung belegt.

Mustervorlage: Praxisinterne Richtlinien zum allgemeinen Datenschutz
www.lzkth.de/de/datenschutz-18

5. Verträge mit praxisexternen Dienstleistern zur Auftragsdatenverarbeitung aktualisieren

Bei der Datenverarbeitung bedienen sich Zahnarztpraxen der Unterstützung durch externe Dienstleister aller Art. Dies können IT-Dienstleister sein, Dentallabore, Abrechnungs- oder Buchhaltungsbüros oder auch Cloud-Dienstleister für die Textverarbeitung, Terminverwaltung oder Spracherkennung.

All diese Arbeiten wurden bereits nach bisherigem Recht als Auftragsdatenverarbeitung angesehen, für die zwischen der Praxis und jedem Dienstleister schriftliche Verträge notwendig waren. Auch nach dem neuem Datenschutzrecht bleibt das so, allerdings **müssen bestehende Verträge an das neue Recht angepasst werden**. Selbstverständlich müssen dabei auch weiterhin zusätzliche rechtliche Anforderungen eingehalten werden, die sich zum Beispiel aus dem jeweiligen Berufsrecht ergeben. Sofern noch keine Verträge existieren, sollte jede Praxis diese Vertragsschlüsse vor dem 25. Mai 2018 nachholen.

Mustervorlage: Vertrag zur Auftragsdatenverarbeitung mit einem Dentallabor
www.lzkth.de/de/datenschutz-19

6. Datenschutzinformationen veröffentlichen

Die Informationspflichten zum Datenschutz sind nach neuem Recht wesentlich umfangreicher als bisher. Zugleich verfügen viele Zahnarztpraxen über eine eigene Webseite oder eine Präsenz in sozialen Medien. Terminerinnerungen per SMS oder Patienten-Newsletter gehören zunehmend zum Serviceangebot. **Praxen sollten daher in Abstimmung mit ihrem Webmaster bis spätestens zum 25. Mai 2018 prüfen, ob auf ihrer Internet- und/oder Facebook-Seite eine gültige Datenschutzerklärung mit allen nötigen Angaben veröffentlicht ist. Zudem empfehlen sich allgemeine Hinweise zur Datenverarbeitung, die jeder Patient erhalten und unterschreiben sollte.**

Mustervorlage: Datenschutzerklärung für Praxis-Webseite
www.lzkth.de/de/datenschutz-20

Mustervorlage: Datenschutzerklärung an Patienten
www.lzkth.de/de/datenschutz-21

Mustervorlage: Datenschutzerklärung an Praxispersonal
www.lzkth.de/de/datenschutz-22

Mustervorlage: Einwilligung von Praxismitarbeitern für Porträtfotos auf Praxis-Webseite
www.lzkth.de/de/datenschutz-23

Mustervorlage: Einwilligung von Patienten zum Empfang von Praxisinformationen
www.lzkth.de/de/datenschutz-24

Mustervorlage: Einwilligung von Patienten zum Empfang des Recalls
www.lzkth.de/de/datenschutz-25

Mustervorlage: Einwilligung von Patienten zur Datenverararbeitung
www.lzkth.de/de/datenschutz-26

Die neuen Informationspflichten umfassen unter anderem:

- Namen und die Kontaktdaten der Praxis
- Kontaktdaten des betrieblichen Datenschutzbeauftragten
- Art der verarbeiteten Daten
- Zwecke der Datenverarbeitung
- Art der Personen, deren Daten verarbeitet werden (Patienten, Beschäftigte oder Lieferanten)
- mögliche Empfänger der Daten, an die die Daten übermittelt werden (zum Beispiel Krankenkassen und Verrechnungsstellen)
- Übermittlung von Daten in ein Land außerhalb der EU (zum Beispiel bei der Nutzung von E-Mail-Diensten oder Cloud-Diensten)
- Löschfristen
- datenschutzrechtlichen Ansprüche des Patienten (Auskunft, Berichtigung, Löschung, Sperrung, Widerspruchsrecht, Datenübertragbarkeit)
- Recht des Patienten auf Widerruf einer Einwilligung
- Recht des Patienten auf Beschwerde bei einer Datenschutzbehörde.

7. Betroffenenrechte sichern

Zusätzlich zum allgemeinen Informationsanspruch stehen den von der Datenverarbeitung betroffenen Personen weitere Rechte zu. Eine Reaktion seitens der Praxis muss innerhalb der Frist eines Monats erfolgen, da ansonsten Bußgelder drohen können. Daher sollten **je nach Organisation und Struktur der Praxis folgende Betroffenenrechte rechtzeitig gewährleistet** werden:

- Information über Datenerhebung bei Dritten
- Auskunftsanspruch
- Recht auf Datenberichtigung
- Recht auf Datenlöschung
- Recht auf Einschränkung der Datenverarbeitung
- Recht auf Datenübertragung

Die benannten Rechte eines Patienten auf Berichtigung, Löschung, Einschränkung der Verarbeitung bzw. Widerspruch gegen die Verarbeitung patientenbezogener Daten gelten nicht uneingeschränkt. Insbesondere Behandlungsdaten sind aufgrund der gesetzlichen Dokumentationspflicht des Zahnarztes von diesen Rechten ausgeschlossen.

In der Praxis sollte es zudem klare Regeln zum Verfahren geben, 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.

Informationen zu Betroffenenrechten
www.lzkth.de/de/datenschutz-27

8. Meldepflichten berücksichtigen

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 beispielsweise sein Dienst-Handy und befinden sich auf dem Handy auch Patientendaten, kann dies zu einer Meldepflicht führen. Bereits der bloße Verstoß gegen die Meldepflicht kann ein Bußgeld nach sich ziehen. Daher **muss in jedem Fall gewährleistet werden, dass die Praxisleitung oder der Datenschutzbeauftragte zeitnah von jeder „Datenpanne“ erfahren**.

Mustervorlage: Verfahrensanweisung für die Reaktion auf Anfragen der Aufsichtsbehörden
www.lzkth.de/de/datenschutz-28

Mustervorlage: Verfahrensanweisung für das interne Vorgehen bei einem Datenschutzverstoß
www.lzkth.de/de/datenschutz-29

Achtung, Bußgelder!

Bei Verstößen gegen das neue Datenschutzrecht drohen Bußgelder bis zu 20 Mio. Euro. Eine Übergangsfrist nach dem 25. Mai 2018 gibt es nicht. Zahnarztpraxen, deren Datenverarbeitung nach diesem Stichtag nicht dem neuen Recht entspricht, müssen also mit Bußgeldern rechnen.

Dies gilt umso mehr, da neue, förmliche Beschwerdebefugnisse der Betroffenen eingeführt werden. Beschweren sich in Zukunft Mitarbeiter oder Patienten bei der zuständigen Datenschutzbehörde, darf die Behörde nicht untätig bleiben und muss der Beschwerde nachgehen. Auch strafbewehrte Sanktionen sind bei Verstößen gegen das Datenschutzrecht möglich. Das Ausmaß der Strafe richtet sich vor allem nach Schwere und Dauer des Vorfalls sowie nach dessen Auswirkungen auf Patienten.

(Stand: Mai 2018)