Information zur Datenorganisation
im Rahmen der Umsetzung der DSGVO

Die Datenschutzregelungen verlangen für die Datenverarbeitung von personenbezogenen Daten Sicherheitsvorkehrungen, die das Schutzniveau gewährleisten können, um die Rechte und Freiheiten der betroffenen Personen sicherzustellen. Bei den Schutzvorkehrungen muss der aktuelle Stand der Technik beachtet werden. Datenschutz bedeutet dabei die ständige Anpassung an veränderte Risiken durch die Datenverarbeitung und Möglichkeiten der Datensicherung. Dazu gehört auch, dass ein IT-Sicherheitsmanagement bei Verwendung von EDV-Programmen zur Datenverwaltung berücksichtigt werden muss.

Grundsätzlich sollten sämtliche Maßnahmen und Bemühungen zur technischen und organisatorischen Umsetzung der Datensicherheit und deren Durchführung dokumentiert werden, um diese im Falle einer Überprüfung der Aufsichtsbehörde vorlegen zu können.

Folgende Maßnahmen können die Datensicherheit in der Zahnarztpraxis unterstützen:

Gap Analysis

Die Verfahrensverzeichnisse 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 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 Datenschutzkonformität aller Verfahren.

Datensicherheit

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

- Zuständigkeiten: Festlegung der Zuständigkeiten für den Datenschutz mit Einbindung des ggf. benannten Datenschutzbeauftragten

- Sensibilisierung: Schulung der Mitarbeiter im Datenschutz

- Kontrollen: Durchführung von Stichproben zur Überprüfung der Datenschutzvorgaben

- Verschlüsselung: Soweit möglich, sollen personenbezogene Daten verschlüsselt werden. Es empfiehlt sich daher beispielsweise, die Verschlüsselung von E-Mails mit Verschlüsselungs-programmen 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 wer-den 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 die DSGVO 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 nicht.