

6. Informationssicherheit und Datenschutz

Mit der Einführung der Datenschutzgrundverordnung (DSGVO) im Jahr 2018 und dem neuen Bundesdatenschutzgesetz (BDSG) gelten strenge Vorgaben für den Umgang mit den Daten der Patienten in einer Zahnarztpraxis. Dazu zählt die Bestimmung eines Datenschutzbeauftragten (wenn die Praxis verschiedene Kriterien erfüllt), die Information an den Patienten (wie seine Daten verarbeitet werden) und Maßnahmen zur Übermittlung und Speicherung von Daten. Sowie der Vernichtung z.B. von Datenträgern.

Die aktualisierte Fassung der IT-Sicherheitsrichtlinie wurde am 1. Juli 2025 veröffentlicht und ist am 2. Juli 2025 in Kraft getreten, alle Anforderungen sind **seit 2026 verbindlich umzusetzen**. Die Richtlinie verlangt technische und organisatorische Maßnahmen – zum sicheren Umgang mit Geräten, zum Schutz sensibler Daten und zur Absicherung von Netzwerk und Kommunikation. Eine Reihe von Anforderungen sind Aufgaben zur Dokumentation, Vereinbarung oder Schulung. Der Umfang der umzusetzenden Maßnahmen richtet sich nach der Praxisgröße.

Praxisnahe Hilfen für die Umsetzung der IT-Sicherheit in Ihrer Zahnarztpraxis finden Sie unter folgendem Link: <https://www.zahnaerzte-in-sachsen.de/zahnarztpraxis/ti-digitales/it-sicherheit/>

TOM'S

TOM'S sind alle technischen und organisatorischen Maßnahmen, die in der Zahnarztpraxis getroffen werden, um personenbezogene Daten gemäß den Anforderungen der Datenschutz-Grundverordnung zu schützen.

Somit gewährleisten die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und stellen sicher, dass ein dem Risiko angemessene Schutzfunktion eingehalten wird.

Zu den Mindestanforderungen des Qualitätsmanagements gehören insbesondere:

- Zugangs- und Zugriffskontrollen (Berechtigungskonzept, Passwortschutz, Sperrung bei Abwesenheit...)
- Verschlüsselung von Daten bei Speicherung und Übertragung
- Regelmäßige Datensicherung und Wiederherstellbarkeit
- Schutz vor unbefugtem Zutritt zu Praxis – und Serverräumen
- Schulung und Verpflichtung der Mitarbeiter auf den Datenschutz
- Dokumentation und regelmäßige Überprüfung der Maßnahmen

➔ Details dazu finden Sie in der Checkliste „TOM'S“ und „Datensicherheit (DSGVO)“

Checkliste TOM´S - gemäß Art. 32 Abs. 1 DSGVO

Datum	
Durchgeführt von	

Tabellen müssen an die Praxisgegebenheiten angepasst werden.

Empfang	Ja	Nein
Ist das Wartezimmer so abgetrennt, dass Dritte keine Gespräche am Empfang oder in den Behandlungsräumen mithören können?	☐	☐
Ist die ununterbrochene Besetzung des Empfangs während der Öffnungszeiten gewährleistet.	☐	☐
Werden die Anmelde- und Patientendaten des Betroffenen diskret erhoben?	☐	☐
Werden die Patienten auf die Freiwilligkeit des Ausfüllens eines Anamneseformulars hingewiesen?	☐	☐
Sind Bildschirme, Fax, Telefone & Co. vor dem Einblick Dritter geschützt?	☐	☐
Kann kein Unbefugter auf PCs & Co. zugreifen?	☐	☐
Sind die Patientenakten vor unbefugtem Zugriff abgesichert? (abschließbare Schränke)	☐	☐
	☐	☐
	☐	☐

Behandlungsräume	Ja	Nein
Sind Patienten niemals allein in einem Behandlungsraum?	☐	☐
Sind Bildschirme, Fax, Telefone & Co. vor dem Einblick Dritter geschützt?	☐	☐
Alternativ: Ist sichergestellt, dass unter Abwesenheit des Arztes keine Fremdinformationen durch den Patienten eingesehen werden können?	☐	☐
	☐	☐
	☐	☐

Datensicherheit und -verwaltung	Ja	Nein
Sind die Datenverarbeitungssysteme physisch geschützt? (Beschränkung des Zugangs zum Server usw.)	☐	☐
Ist der Zugriff auf den Rechner durch sichere Passwörter geschützt?	☐	☐
Werden die Passwörter regelmäßig gewechselt?	☐	☐
Sind unbeaufsichtigte PCs stets gesperrt / ausgeschaltet (inkl. Passwortschutz)?	☐	☐
Sind Virenschutzprogramme und ggf. auch Firewalls installiert und auf dem aktuellsten Stand?	☐	☐
Werden regelmäßig Sicherungen der Daten erstellt? Und werden diese extern aufbewahrt?	☐	☐
Ist eine verschlüsselte und / oder sichere Übertragung von Daten (auch physischen) gewährleistet?	☐	☐
Werden nicht mehr benötigte Patientenakten, Informationen und Datenträger gemäß Datenschutzbestimmungen korrekt entsorgt?	☐	☐
Sind alle Angestellten auf das Datengeheimnis verpflichtet worden?	☐	☐
Wurden sie darüber hinaus auch auf die besondere Verschwiegenheitspflicht hingewiesen und entsprechend belehrt?	☐	☐
	☐	☐
	☐	☐

Recht des Betroffenen	Ja	Nein
Ist sichergestellt, dass die Betroffenen ihr Auskunftsrecht geltend machen können?	☐	☐
Sind Bildschirme, Fax, Telefone & Co. vor dem Einblick Dritter geschützt?	☐	☐
Alternativ: Ist sichergestellt, dass unter Abwesenheit des Arztes keine Fremdinformationen durch den Patienten eingesehen werden können?	☐	☐
Werden Betroffene über den Umfang einer Einwilligungserklärung in die Datenübertragung aufgeklärt?	☐	☐
	☐	☐
	☐	☐

Zusammenfassung / Bemerkungen

Ort, Datum: _____

Unterschrift Praxisinhaber/QM-Beauftragter: _____

Checkliste zur Informationssicherheit und Datenschutz

Datum	
Durchgeführt von	

- ☐ Verzeichnis der Verarbeitungstätigkeiten ist aktuell und vollständig
- ☐ Datenschutzhinweise / Informationspflichten gegenüber Patienten sind umgesetzt
- ☐ Einwilligungen (z. B. für Foto, Newsletter, Weitergabe) werden korrekt eingeholt und dokumentiert
- ☐ Zugriffsberechtigungen auf Patientendaten sind rollenbasiert und nach dem Need-to-know-Prinzip geregelt.
- ☐ Technische und organisatorische Maßnahmen (TOM'S) sind dokumentiert und wirksam (Verschlüsselung, Backup, Zugangskontrolle).
- ☐ Mitarbeiter sind zum Datenschutz geschult und verpflichtet
- ☐ Löschkonzepte und Aufbewahrungsfristen werden eingehalten
- ☐ IT-Sicherheits-RL zur Kenntnis genommen

Zusammenfassung / Bemerkungen

Ort, Datum: _____

Unterschrift Praxisinhaber/QM-Beauftragter: _____

VERHALTEN BEI IT-NOTFÄLLEN



Ruhe bewahren & IT-Notfall melden

Lieber einmal mehr als einmal zu wenig anrufen!



IT-Notfallrufnummer:



Wer meldet?



Welches IT-System ist betroffen?



Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?



Wann ist das Ereignis eingetreten?



Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

Weitere Arbeit
am IT-System
einstellen

Beobachtungen
dokumentieren

Maßnahmen nur
nach Anweisung
einleiten

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

- ➔ Informationen zum Einsatz der IT-Notfallkarte „Verhalten bei IT-Notfällen“ sowie der ergänzenden Dokumente „Maßnahmenkatalog zum Notfallmanagement - Fokus IT-Notfälle“ und „TOP 12 Maßnahmen bei Cyber-Angriffen“ finden Sie unter nachfolgendem Link auf den Internetseiten der Allianz für Cyber-Sicherheit des Bundesamtes für Sicherheit in der Informationstechnik:

<https://www.allianz-fuer-cybersicherheit.de/ACS/IT-Notfallkarte>