Österreichische Zahnärztekammer

# Datenschutz und Datensicherheit

# Technische Tipps zur Umsetzung in der zahnärztlichen Ordination:

1) Ordinationszutritt und Räumlichkeiten: Der erste Weg in die Ordination führt bekanntlich durch die Tür, die nach dem heutigen Stand der (Türschloss-)Technik abzusichern ist und somit den ersten Schutz auch für die Daten bieten soll. Die Ordination sollte möglichst vor Einbruch, Diebstahl und unberechtigten Zugriffen sicherheitstechnisch (evt. auch durch elektronische Sicherheitsmaßnahmen) abgesichert sein.

WICHTIG: Achten Sie auf eine räumliche Trennung zwischen Wartebereich und Behandlungsräumen, aber auch der Bereich zur Anmeldung sollte so liegen, dass Wartende nicht Gespräche über personenbezogene Daten, insb. Gesundheitsdaten mithören können.

2) Datenserver: sollte in einem Bereich stehen, in dem er für Patienten nicht direkt zugänglich ist (jedenfalls NICHT unversperrt im Eingangs-/Garderobe- oder Wartebereich) und vor unbefugten Zugriffen geschützt sein. Er muss weiters vor unbeabsichtigter Beschädigung/Zerstörung (z.B. Flüssigkeiten, die über die Hardware rinnen könnten) geschützt werden.

**Die folgenden Punkte sind gleichermaßen für Ihren PC und mobile Endgeräte (Handy, Laptop, Tablet,...) zu beachten:**

a) Computer-Arbeitsplatz: die verwendete Hard- und Software sollte dem aktuellen Stand entsprechen, damit die Sicherheit und Zuverlässigkeit gewährleistet ist (Passwortschutz, aktuelle Sicherheits-Updates). In Anbetracht der Strafdrohungen für Datenverlust/Datenschutzverletzungen ist eine regelmäßige Investition in die Sicherheit sicherlich vorteilhaft. Vergewissern Sie sich, dass Ihr Benutzerprofil keine Administratorenrechte hat (mit Ihrem IT-Berater klären!).

b) Schutz von Patientendaten: achten Sie auf eine sichere Speicherung von Patientendaten! Die Weitergabe von personenbezogenen Daten auf elektronischem Weg per E-Mail, USB-Stick etc. (z.B. an Zahntechniker) hat verschlüsselt zu erfolgen! Papieraufzeichnungen sind sicher zu verwahren und mittels Schredder zu vernichten. Wird für die elektronische Befundübermittlung eine externe Firma beauftragt, sollte diese jedenfalls die Grundsätze der DSGVO einhalten und von Ihnen sorgfältig ausgewählt sein.

c) Internetproblematik – Viren, Trojaner, Spam: Achten Sie bei einer Internet-Anbindung, die nicht über das GIN-Netz führt, auf die Installation einer Firewall. Jedenfalls nötig ist ein aktueller Spam- und Virenschutz. Sowohl Sie als auch Ihre MitarbeiterInnen sollten keine Anhänge von E-Mails öffnen, die von unbekannten Personen gesendet wurden. Diese könnten Trojaner oder Viren in Form von Schadprogrammen enthalten. Auch (private) USB-Sticks können über darauf gespeicherte Inhalte Trojaner, Viren etc. übertragen.

d) (Fern-)Wartung: zur Erhöhung der Sicherheit ist eine regelmäßige Wartung angeraten. Eine Fernwartung sollte nur auf Ihren Auftrag hin erfolgen.

e) Datensicherung: Sie sollten die Daten regelmäßig auf aktuellen Sicherheitsmedien sichern. Vergewissern Sie sich, dass die Lesbarkeit der gesicherten Informationen weiterhin gegeben ist z.B. durch probeweises Wiedereinspielen.

f) Hardware-Reparatur, Festplattentausch: zur Reparatur wenden Sie sich ausschließlich an Fachleute Ihres Vertrauens, die vertraglich gebunden sind. Bezüglich Festplatten, die die Ordination verlassen oder auf die Sicherheits-Back-Ups gespeichert werden, lassen Sie sich schriftlich bestätigen, dass die Daten **sicher** gelöscht wurden oder die Backup-Festplatte/kaputte Festplatte übergeben. Bei alleinigem Löschen oder Formatieren sind die Daten wiederherstellbar!

g) Hardware-Entsorgung: sollte durch einen Fachmann erfolgen, der Ihnen die sichere Löschung/Vernichtung bestätigt (ein einfaches Format-Kommando ist zu wenig). In Hinblick auf die Dokumentationspflicht sichern Sie die Daten zuvor (Patientendaten mind. 10 - max. 30 Jahre aufzubewahren).

h) Verschwiegenheitsvereinbarung und Dokumentation: auch mit Ihrem IT-Berater sollten Sie schriftlich eine Vereinbarung betreffend Verschwiegenheit über die Daten abschließen. Jegliche EDV-Vorkommnisse wie Wartungen, Störfälle, Reparaturen, automatische Protokollierungen, etc. sollten dokumentiert werden.

**Kontaktieren Sie den IT-Berater Ihres Vertrauens, um die angeführten Punkte gegebenenfalls durchzusprechen und lassen Sie Ihr Computer-System regelmäßig auf Sicherheit und Zuverlässigkeit überprüfen!**