2CONSULTING UG

# IT-Sicherheitsrichtlinie

Vorgaben für Praxen durch KBV & KZBV

Auflistung der gesetzlichen Vorgaben auf Seite 2

## Praxissichere IT

Ihre Praxis verwendet ein aktuelles Virenschutzprogramm, nutzt verschlüsselte Internetanwendungen und sendet keine vertraulichen Daten über Apps?
Dann erfüllt sie einen wichtigen Teil der Anforderungen, die durch die IT-Sicherheitsrichtlinie gelten. Der Gesetzgeber hat die KBV und die Kassenzahnärztliche Bundesvereinigung beauftragt, eine IT-Sicherheitsrichtlinie für alle Praxen zu entwickeln (§ 75b SGB V).
Diese Richtlinie beschreibt das Mindestmaß der zu ergreifenden Maßnahmen nach EU-DSGVO, um die IT-Sicherheit zu gewährleisten. . Somit werden viele Anforderungen bereits von den Niedergelassenen umgesetzt.
Die klaren Vorgaben sollen dabei helfen, IT-Systeme und sensible Daten in den Praxen noch besser zu schützen.

# Übersicht der Anforderungen

Bei der Art und Menge der Anforderungen wir in der Größe der Praxen unterschieden.

- Kleine Praxen: **1-5** mit Datenverarbeitung betraute Mitarbeiter
- Mittlere Praxen: **6-20** mit Datenverarbeitung betraute Mitarbeiter
- Große Praxen: **Über 21** mit Datenverarbeitung betraute Mitarbeiter, oder es werden **überdurchschnittlich viele Daten** verarbeitet (z.B. Labor, klinikähnliches MVZ)

## Alle Praxen

- Nutzung sicherer Apps
- Verhinderung von Datenabfluss
- Schutz vertraulicher Daten
- Kryptografische Sicherung vertraulicher Daten
- Abmelden oder Sperren
- Einsatz von Virenschutzprogrammen
- Zugriffschutz verwenden
- Dokumentation des Netzes
- Verhinderung der unautorisierten Nutzung von Rechnermikrofonen und Kameras
- Updates von Mobiltelefonen
- Sichere Speicherung lokaler App-Daten
- Benutzung einer Firewall
- Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen
- Regelmäßige Datensicherung
- Sperrmaßnahmen bei Verlust eines Mobiltelefons
- Schutz vor Schadsoftware
- Zeitnahes Installieren verfügbarer Aktualisierungen
- Sicheres Aufbewahren von Administrationsdaten

"Mit Datenverarbeitung betraute Mitarbeiter"

Unter dem Begriff „Datenverarbeitung“ werden Tätigkeiten zusammengefasst wie Erheben und Abfragen, Ordnen, Speichern, Anpassen und Ändern, Auslesen und Weiterleiten, Löschen und Vernichten der Daten. In den Praxen beginnt dieser Prozess quasi bei der Terminvereinbarung am Telefon oder dem Einlesen der elektronischen Gesundheitskarte.

zusätzlich gilt für..

## mittlere Praxen

- Minimierung und Kontrolle von App-Berechtigungen
- Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung
- Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten
- Regelungen zur Mitnahme von Wechseldatenträgern

*Weitere Informationen finden Sie auf www.2consulting.eu/praxissichere-it.de*

zusätzlich gilt für..

## Praxen mit Großgeräten

- Einschränkung des Zugriffs für Konfigurations- und Wartungsschnittstellen
- Nutzung sicherer Protokolle für die Konfiguration und Wartung
- Netzsegmentierung

zusätzlich gilt für..

## große Praxen

- Festlegung einer Richtlinie für den Einsatz von Smartphones und Tablets
- Auswahl und Freigabe von Apps