# Checkliste IT-Sicherheit für Praxen

Selbsttest zur IT-Sicherheitsrichtlinie nach § 390 SGB V für Arzt-, Zahnarzt- und Psychotherapiepraxen

Arztpraxen verwalten besonders schützenswerte Daten: Diagnosen, Befunde, Medikationspläne. Seit 2021 gibt es deshalb eine verbindliche IT-Sicherheitsrichtlinie für vertragsärztliche, vertragspsychotherapeutische und vertragszahnärztliche Praxen, 2025 wurde sie überarbeitet. Mit dieser Checkliste prüfen Sie in wenigen Schritten, wo Ihre Praxis steht.

## Welche Anlage gilt für Ihre Praxis?

Maßgeblich ist, wie viele Personen ständig mit der Datenverarbeitung betraut sind, also regelmäßig mit Praxissoftware und Patientendaten arbeiten. Die Anforderungen bauen aufeinander auf: Wer unter Anlage 2 fällt, erfüllt auch Anlage 1.

| | |
|---|---|
| **Anlage 1** | Praxen mit bis zu fünf Personen, die ständig mit der Datenverarbeitung betraut sind. Das ist die Mehrheit der Einzel- und kleineren Gemeinschaftspraxen. |
| **Anlage 2** | Praxen mit sechs bis zwanzig Personen. Mit zusätzlichen Anforderungen. |
| **Anlage 3** | Praxen mit mehr als zwanzig Personen sowie Großlabore und große MVZ mit krankenhausähnlichen Strukturen. |
| **Anlage 4** | Praxen mit medizinischen Großgeräten wie CT oder MRT. |
| **Anlage 5** | Die dezentralen Komponenten der Telematikinfrastruktur, etwa Konnektor und Kartenterminals. |

## Zehn Fragen an Ihre Praxis-IT

Die Liste ist kein Ersatz für den Wortlaut der Richtlinie, deckt aber die Punkte ab, an denen es in Praxen am häufigsten hakt. Wenn Sie eine Frage nicht sicher mit Ja beantworten können, lohnt sich ein genauerer Blick.

**1. Überblick** ☐ Ja ☐ Nein
Gibt es eine aktuelle Liste aller Geräte, Programme und Zugänge der Praxis?

**2. Updates** ☐ Ja ☐ Nein
Werden Betriebssysteme, Praxissoftware, Browser und Netzwerkgeräte regelmäßig aktualisiert?

**3. Altgeräte** ☐ Ja ☐ Nein
Bekommen alle Rechner noch Sicherheitsupdates für ihr Betriebssystem?

**4. Virenschutz und Firewall** ☐ Ja ☐ Nein
Sind sie auf allen Geräten aktiv und aktuell?

**5. Datensicherung** ☐ Ja ☐ Nein
Läuft sie automatisch, liegt eine Kopie getrennt vom Praxisnetz, und wurde die Wiederherstellung schon einmal getestet?

**6. Zugänge** ☐ Ja ☐ Nein
Hat jede Person ein eigenes Benutzerkonto, und werden Konten ausgeschiedener Mitarbeitender gesperrt?

**7. WLAN** ☐ Ja ☐ Nein
Ist das Gäste-WLAN für Patientinnen und Patienten vom Praxisnetz getrennt?

**8. Schulung** ☐ Ja ☐ Nein
Weiß das Team, wie Phishing-Mails aussehen und was bei einem Verdacht zu tun ist?

**9. Notfall** ☐ Ja ☐ Nein
Ist festgelegt, wer im Ernstfall informiert wird und wie die Praxis ohne IT weiterarbeitet?

**10. Dokumentation** ☐ Ja ☐ Nein
Ist festgehalten, welche Maßnahmen umgesetzt sind und wer sie betreut?

### Der wichtigste Einzelpunkt: die Datensicherung

Wenn nur Zeit für eine Maßnahme ist, dann für die Datensicherung. Eine externe Festplatte, die dauerhaft am Server hängt, schützt nicht vor Verschlüsselungstrojanern, denn sie wird oft gleich mitverschlüsselt. Bewährt hat sich, mehrere Kopien auf unterschiedlichen Medien vorzuhalten, davon mindestens eine getrennt vom Praxisnetz. Genauso wichtig ist der regelmäßige Test, ob sich die Daten tatsächlich zurückspielen lassen.

## Kostenloser Praxis-IT-Check

Sie möchten wissen, wo Ihre Praxis steht? DigiVillage GmbH prüft kostenlos und unverbindlich Datensicherung, Updates, Virenschutz, Zugänge und Benutzerkonten sowie Netzwerk und WLAN. Sie erhalten eine kurze schriftliche Übersicht mit Prioritäten.

**Anfrage: digivillage.de/praxis-it-check**

## Quelle und Hinweis

Grundlage ist die IT-Sicherheitsrichtlinie nach § 390 SGB V in der Fassung der KBV beziehungsweise für Zahnarztpraxen der KZBV. Die aktuelle Fassung mit allen Anlagen steht kostenlos auf den Seiten der KBV und der KZBV. Maßgeblich ist allein der Wortlaut der Richtlinie. Diese Übersicht ist keine Rechtsberatung.