

EINFÜHRUNG DIGITALER LÖSUNGEN IN DER PRAXIS – ORIENTIERUNGSHILFE

DATENSCHUTZ UND INFORMATIONSSICHERHEIT

Gesundheitsdaten zählen zu besonders schützenswerten personenbezogenen Daten. Datenschutz und Informationssicherheit sollten daher bereits vor Einführung digitaler Lösungen geprüft, aktualisiert und dokumentiert werden. Die nachfolgende Checkliste soll eine Orientierung geben.

Kriterium

Wichtige Prüfpunkte

1 **Transparenz & Informationspflichten nach Art. 13 DSGVO**

- Datenschutzerklärung der Praxis aktualisieren und um Inhalte des neuen Systems ergänzen
- Hinweise zu Zweck, Datenarten, Empfängern und Speicherdauer bereitstellen
- Informationen auch in den Praxisräumen verfügbar machen

- Patienten verständlich über die digitale Lösung informieren

2 **Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO**

- Technische und Organisatorischen Maßnahmen (TOM) prüfen
- Verschlüsselte Kommunikation zwischen dem Patienten und der Webseite oder Anwendung sicherstellen (TLS)
- Datenverarbeitung in Deutschland/EU bzw. akzeptiertem Drittland

- AVV mit dem Dienstleister abschließen

3 **Praxisinterne DSGVO-Dokumentation**

- Interne Datenschutzrichtlinie ergänzen
- Zuständigkeiten festlegen
- Mitarbeitende zu Datenschutz und IT-Sicherheit schulen

- Verarbeitung im Verzeichnis nach Art. 30 DSGVO dokumentiert

4 **Absicherung der Informationssicherheit**

- Regelmäßige Updates, Firewall und Virenschutz vorhanden
- Sichere Passwörter und Zugriffsrechte regeln
- Datensicherungen (Backups) einrichten
- Anforderungen der KBV-IT-Sicherheitsrichtlinie berücksichtigen

- Sichere Website- und Kontaktformulare (TLS/HTTPS)

5 **Datenverarbeitung, Datensparsamkeit & Zweckbindung**

- Keine unnötigen Pflichtangaben abfragen
- Daten nur für den vorgesehenen Zweck verwenden
- Keine Kommunikation über unsichere Kanäle (z. B. WhatsApp)

- Nur erforderliche Gesundheitsdaten verarbeiten