DSGVO-Checkliste für Arzt-, Therapie- und sonstige Gesundheitspraxen

Österreich, Stand Juli 2025 – ohne Gewähr, ersetzt keine Rechtsberatung.

- [ ] Verantwortlicher & ggf. Datenschutzbeauftragter (DSB)
- [ ] Ist-Analyse & Dateninventar
- [ ] Verzeichnis der Verarbeitungstätigkeiten (VVT)
- [ ] Rechtsgrundlage prüfen (Art. 6 & 9 DSGVO)
- [ ] Informationspflichten (Art. 13/14)
- [ ] Betroffenenrechte
- [ ] Auftragsverarbeitungsverträge (AVV)
- [ ] Technische & organisatorische Maßnahmen (TOMs)
- [ ] Datenschutz-Folgenabschätzung (DSFA)
- [ ] Incident- & Data-Breach-Management
- [ ] Speicher- & Löschfristen
- [ ] Schulung & Vertraulichkeit der Mitarbeitenden
- [ ] Website & Online-Terminsystem

Kurzbeschreibung (1/2)

Verantwortlicher & ggf. Datenschutzbeauftragter (DSB)

Verantwortliche Person festlegen; DSB ist Pflicht, sobald umfangreich Gesundheitsdaten verarbeitet werden oder Art. 37 DSGVO greift.

Ist-Analyse & Dateninventar

Welche (Gesundheits-)Daten werden wo, wie lange, auf welcher Rechtsgrundlage verarbeitet und an wen übermittelt? Ergebnis fließt ins Verarbeitungsverzeichnis.

Verzeichnis der Verarbeitungstätigkeiten (VVT)

Für jede Verarbeitung (Patientenverwaltung, Personalverwaltung, Labor etc.) Art 30 DSGVO-konformes VVT führen. Muster stellt z. B. die Ärztekammer NÖ bereit.

Rechtsgrundlage prüfen (Art. 6 & 9 DSGVO)

Standard bei Behandlung: Art. 9 Abs. 2 h DSGVO + Art. 6 Abs. 1 b (Behandlungs vertrag). Einwilligung nur nötig für Zusatzservices (Newsletter, Marketing, Angehörigenauskunft).

Informationspflichten (Art. 13/14)

Datenschutzerklärung (Praxis & Website) in klarer Sprache; Aushang oder Hand-out; Patienten bei Erstkontakt informieren. Muster siehe Ärztekammer-Downloads.

Betroffenenrechte

Verfahren & Fristen für Auskunft, Berichtigung, Löschung, Einschränkung, Daten übertragbarkeit, Widerspruch definieren; Dokumentation jeder Anfrage.

Auftragsverarbeitungsverträge (AVV)

Schriftliche AVV nach Art. 28 DSGVO mit IT-Dienstleistern, Cloud-Anbietern, Abrechnungsstellen, Laboren etc. Regelmäßig prüfen.

Technische & organisatorische Maßnahmen (TOMs)

Zutritts-/Zugangs-/Zugriffskontrolle, Verschlüsselung (E-Mail nur verschlüsselt; unverschlüsselt reicht Einwilligung nicht aus), Backup, Updates, Lösch-/Schredder-Konzept.

Datenschutz-Folgenabschätzung (DSFA)

Wenn hohes Risiko (meist bei elektronischer Patientenakte, Telemedizin, Video sprechstunde), DSFA nach Art. 35 durchführen und dokumentieren.

Kurzbeschreibung (2/2)

Incident- & Data-Breach-Management

Meldeprozess: binnen 72 h an die Datenschutzbehörde (§ DSG) und ggf. Betroffene (Art. 33/34). Formblätter bereithalten.

Speicher- & Löschfristen

Mind. 10 Jahre Aufbewahrung (§ 51 ÄrzteG); medizinische Großbilddaten u. U. 30 Jahre (§ 48 SpitalG Tirol). Danach sichere Löschung/Anonymisierung.

Schulung & Vertraulichkeit der Mitarbeitenden

Einstiegsschulung + jährliche Auffrischung; Schriftliche Vertraulichkeits erklärungen (§ 6 DSGVO).

Website & Online-Terminsystem

TLS-Verschlüsselung, Cookie-Banner (TTDSG/TKG), Auftragsverarbeitung mit Dienstleistern, Formular-Double-Opt-In.