Dieser Vorschlag ist nach den klassischen **Kontrollzielen** strukturiert, wie sie in der Praxis zur Einhaltung von Art. 32 DSGVO (Sicherheit der Verarbeitung) üblich sind.

**Technisch-Organisatorische Maßnahmen (TOMs) für die Arztpraxis**

**Dokument: TOM-Konzept der [Name der Praxis]**

Stand: [Aktuelles Datum]

Verantwortlich: [Name des Praxisinhabers / Datenschutzbeauftragten]

**A. Maßnahmen zur Gewährleistung der Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)**

| **Kontrollziel** | **Maßnahme** |
| --- | --- |
| **1. Zutrittskontrolle** (Unbefugten der Zutritt zu Verarbeitungsanlagen verwehren) | **Räumliche Sicherheit:** Praxisräume sind durch abschließbare Türen/Fenster gesichert. Serverraum/Aktenarchiv ist separat abschließbar. **Alarmierung:** Einsatz einer Einbruchmeldeanlage (sofern notwendig). |
| **2. Zugangskontrolle** (Unbefugte Nutzung der Verarbeitungsanlagen verhindern) | **Authentifizierung:** Einsatz von Passwörtern/PINs für alle IT-Systeme. **Passwortrichtlinie:** Mindestlänge von 10-12 Zeichen, Verwendung von Groß-/Kleinbuchstaben, Zahlen und Sonderzeichen; regelmäßige Aufforderung zur Passwortänderung. **Sperrung:** Automatische Sperrung des Bildschirms nach maximal 5 Minuten Inaktivität. |
| **3. Zugriffskontrolle** (Sicherstellen, dass nur Berechtigte auf Daten zugreifen können) | **Rollen- und Rechtekonzept:** Jeder Mitarbeiter (Arzt, MFA, Verwaltung) erhält nur die Berechtigungen, die er für seine jeweilige Aufgabe benötigt (Need-to-know-Prinzip). **Patientenverwaltungssystem (PVS):** Zugriff auf Patientenakten ist nur nach Authentifizierung und mit individueller Benutzerkennung möglich. **Protokollierung:** Zugriffe auf sensible Daten im PVS werden protokolliert (wer hat wann auf welche Akte zugegriffen). |
| **4. Trennungskontrolle** (Getrennte Verarbeitung zu unterschiedlichen Zwecken) | **Systematische Trennung:** Daten, die für unterschiedliche Zwecke erhoben wurden (z.B. Patientendaten vs. Buchhaltungsdaten vs. Personalakten), werden in getrennten Datenbanken oder logisch getrennten Bereichen gespeichert. **Testdaten:** Test- und Produktivsysteme sind strikt voneinander getrennt; Testdaten sind anonymisiert oder pseudonymisiert. |

**B. Maßnahmen zur Gewährleistung der Integrität (Art. 32 Abs. 1 lit. b DSGVO)**

| **Kontrollziel** | **Maßnahme** |
| --- | --- |
| **5. Weitergabekontrolle** (Schutz vor unbefugtem Lesen/Verändern bei Übermittlung/Transport) | **Transportverschlüsselung (Website):** Datenübertragung über die Praxis-Website (Kontaktformular, Terminbuchung) erfolgt ausschließlich mit dem sicheren **TLS-Protokoll (Version 1.2/1.3)**. **E-Mail-Verkehr:** E-Mails, die sensible Patientendaten enthalten, werden nur nach vorheriger Einwilligung des Patienten und unter Verwendung von **Ende-zu-Ende-Verschlüsselung** (z.B. S/MIME, PGP) versandt. |
| **6. Eingabekontrolle** (Protokollierung, ob und von wem Daten eingegeben, geändert oder gelöscht wurden) | **PVS-Protokollierung:** Das Patientenverwaltungssystem protokolliert, wer (Benutzer-ID) wann welche Daten in der Patientenakte **eingegeben, geändert oder gelöscht** hat (revisionssichere Protokollierung). **Datenintegrität:** Die Eingabefelder in Webformularen werden auf Plausibilität und Format geprüft, um unzulässige Eingaben und Angriffe (Injektionen) zu verhindern. |

**C. Maßnahmen zur Gewährleistung der Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)**

| **Kontrollziel** | **Maßnahme** |
| --- | --- |
| **7. Verfügbarkeitskontrolle** (Schutz vor Zerstörung oder Verlust) | **Backup-Konzept:** Tägliche automatische Sicherung aller relevanten Daten (PVS, Bilder, Dokumente) auf ein getrenntes Speichermedium. **Wiederherstellungstest:** Mindestens jährliche Durchführung eines **vollständigen Wiederherstellungstests** (Rückspielen einer gesicherten Version). **USV/Notstrom:** Einsatz einer unterbrechungsfreien Stromversorgung (USV) für kritische Serversysteme. |
| **8. Schnelle Wiederherstellbarkeit** | Dokumentierter **Notfallplan** für den Ausfall des PVS oder des Netzwerkes. Der Plan enthält klare Schritte zur Wiederherstellung der Systeme und zur Fortführung des Praxisbetriebs (z.B. mit Notfallformularen). |

**D. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)**

| **Kontrollziel** | **Maßnahme** |
| --- | --- |
| **9. Auftragskontrolle** (Einhaltung der Weisungen durch Dienstleister) | **AVV-Management:** Abschluss und regelmäßige **Überprüfung der Auftragsverarbeitungsverträge (AVV)** mit allen Dienstleistern, die Zugriff auf personenbezogene Daten haben (Hoster, IT-Wartung, Abrechnungsstelle etc.). **Standort:** Bevorzugte Beauftragung von Dienstleistern, deren Serverstandorte sich in der EU befinden. |
| **10. Zuverlässigkeitskontrolle** (Sicherstellung der Zuverlässigkeit von Mitarbeitern) | **Sensibilisierung und Schulung:** Jährliche **Pflichtschulung** aller Mitarbeiter zum Datenschutz und zur IT-Sicherheit. **Verpflichtung:** Alle Mitarbeiter und externe Dienstleister sind auf das Datengeheimnis verpflichtet. |
| **11. Integrität/Aktualität** | **Patch- und Update-Management:** Zeitnahes Einspielen von Sicherheits-Updates (Patches) für Betriebssysteme, PVS, Firewalls und Virenscanner. **Penetrationstests:** Regelmäßige (z.B. alle 2 Jahre) Überprüfung der IT-Sicherheit durch einen externen IT-Dienstleister (bei größeren Praxen). |

**Hinweis zur Verwendung:**

* Dieses Muster ist eine **Vorlage** und muss an die **spezifischen Gegebenheiten** (z.B. ob Sie eine USV haben, welche Backup-Strategie Sie nutzen) Ihrer Praxis angepasst werden.
* Dieses Dokument dient als **Grundlage** für Ihren Nachweis der Sicherheit gemäß DSGVO.
* Im **Verfahrensverzeichnis** (VV) wird dann, wie zuvor besprochen, nur kurz auf diese detaillierten Maßnahmen verwiesen.