Hausärztinnen- und Hausärzteverband

Umsetzung technischer und organisatorischer Maßnahmen (TOMs) nach Art. 32 DSGVO unter Berücksichtigung der KBV-IT-Sicherheitsrichtlinie

Stand Juli 2026

Hausarztpraxen sind verpflichtet, geeignete technische und organisatorische Maßnahmen (TOMs) zu treffen, um die Vertraulichkeit, Integrität und Verfügbarkeit der personenbezogenen Daten, insbesondere Gesundheitsdaten, die Inhalt ihrer täglichen Arbeit sind, sicherzustellen.

Diese Übersicht bietet eine Hilfestellung und einen Überblick dafür, welche technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit in einer Hausarztpraxis ergriffen bzw. umgesetzt werden können. Wesentliche rechtliche Grundlagen finden sich in der DSGVO als auch in der KBV-IT-Sicherheitsrichtlinie: während die DSGVO die rechtlichen Anforderungen formuliert, konkretisiert die KBV-IT-Sicherheitsrichtlinie die Anforderungen an die Informationssicherheit für vertragsärztliche Praxen. Beide entfalten Relevanz für die hausärztliche Tätigkeit.

1. Was sind technische und organisatorische Maßnahmen?

Technische und organisatorische Maßnahmen (TOMs) dienen dem Schutz personenbezogener Daten vor

- unbefugter Offenlegung,
- Verlust,
- Manipulation,
- Zerstörung sowie
- unbefugtem Zugriff.

Die Maßnahmen müssen dem jeweiligen Risiko angemessen sein. Eine kleine Einzelpraxis benötigt regelmäßig andere Schutzmaßnahmen als ein Medizinisches Versorgungszentrum mit mehreren Standorten.

2. Welches sind relevante organisatorische Maßnahmen aus datenschutzrechtlicher Sicht?

Organisatorische Maßnahmen dienen der Gewährleistung des Schutzes der Verarbeitung und der Daten durch Anweisungen und Vorgaben. Das sind in der Regel Dokumente wie Richtlinien, Anweisungen oder Verpflichtungserklärungen. Aber auch Datenschutzschulungen, Prozessanleitungen und Anwendungsschulungen zu einer konkreten Software oder eine externe Datenschutzberatung gehören dazu. Folgende organisatorische Maßnahmen sind insbesondere zu treffen:

2.1 Berechtigungs- und Rollenkonzepte (Art. 32 DSGVO, Art. 5 DSGVO, KBV-IT-Sicherheitsrichtlinie)

Jede Mitarbeiterin bzw. jeder Mitarbeiter sollte ausschließlich Zugriff auf diejenigen Daten erhalten, die zur Erfüllung der jeweiligen Aufgaben erforderlich sind (Need-to-know-Prinzip).

Empfohlen werden daher individuelle Benutzerkonten, keine Sammelaccounts, regelmäßige Überprüfung der Berechtigungen sowie sofortige Sperrung ausgeschiedener Beschäftigter.

2.2 Verpflichtung auf Vertraulichkeit (Art. 5 DSGVO, Art. 32 DSGVO, § 203 StGB)

Alle Mitarbeitenden sollten vor Aufnahme ihrer Tätigkeit über Datenschutz und Schweigepflicht informiert und entsprechend verpflichtet werden.

2.3 Mitarbeiterschulungen (Art. 24 DSGVO, Art. 32 DSGVO, KBV-IT-Sicherheitsrichtlinie)

Schulungen sollten mindestens folgende Themen umfassen: Datenschutz, Phishing, Passwortsicherheit, Social Engineering, sichere E-Mail-Kommunikation, Umgang mit Patientendaten, Verhalten bei Sicherheitsvorfällen.

2.4 Clean-Desk- und Clear-Screen-Prinzip

Patientenakten sollten nicht offen ausliegen. Computer sollten beim Verlassen des Arbeitsplatzes automatisch oder manuell gesperrt werden.

2.5 Notfallmanagement

Jede Praxis sollte dokumentieren, wer im Notfall verantwortlich ist, wie Backups eingespielt werden, wie bei Cyberangriffen vorzugehen ist, wie Datenschutzverletzungen erkannt und gemeldet werden.

3. Welches sind wichtige technische Maßnahmen?

Technische Maßnahmen sollen dazu geeignet sein, die Gewährleistung des Schutzes der Verarbeitung und der Daten durch physische und IT-technische Maßnahmen zu unterstützen. Hierbei kann es sich insbesondere um folgende Maßnahmen handeln:

3.1 Passwortmanagement (Art. 32 DSGVO, KBV-IT-Sicherheitsrichtlinie)

Empfohlen werden in diesem Zusammenhang individuelle Passwörter, lange Passphrasen, Passwortmanager sowie Mehr-Faktor-Authentifizierung, soweit verfügbar.

3.2 Benutzerverwaltung

Jeder Beschäftigte sollte ein eigenes Benutzerkonto erhalten. Administratorrechte sollten nur wenigen Personen eingeräumt werden.

3.3 Software-Updates

Betriebssysteme, Praxisverwaltungssysteme und Sicherheitssoftware sollten regelmäßig aktualisiert werden. Automatische Updates sind empfehlenswert.

3.4 Virenschutz

Alle Endgeräte sollten aktuelle Antivirensoftware, automatische Updates sowie regelmäßige Scans verwenden.

3.5 Firewall

Das Praxisnetzwerk sollte durch geeignete Firewalls gegen Angriffe geschützt werden.

3.6 Datensicherung

Backups sollten täglich erfolgen, verschlüsselt sein, regelmäßig getestet werden und räumlich getrennt aufbewahrt werden.

3.7 Verschlüsselung

Gesundheitsdaten sollten insbesondere auf mobilen Geräten, bei Datenträgern und auch bei elektronischer Übermittlung verschlüsselt werden.

3.8 Mobile Endgeräte

Laptops und Tablets sollten verschlüsselt, passwortgeschützt und fernlöschbar sein.

3.9 Protokollierung

Die Protokollierung von Zugriffen ermöglicht die Nachvollziehbarkeit und Aufklärung möglicher Datenschutzverletzungen.

4. Einordnung der KBV-IT-Sicherheitsrichtlinie

Die KBV-IT-Sicherheitsrichtlinie konkretisiert die Anforderungen des Art. 32 DSGVO für vertragsärztliche Praxen. Sie enthält überwiegend technische, aber auch organisatorische Vorgaben (z. B. Benutzerverwaltung, Verantwortlichkeiten, Dokumentation und Schulungen). Während die DSGVO lediglich fordert, dass geeignete TOMs getroffen werden, beschreibt die Richtlinie zahlreiche konkrete Maßnahmen für den Praxisalltag.

Die Anforderungen orientieren sich insbesondere an

- der Größe der Praxis,
- der Anzahl der Beschäftigten,

- der vorhandenen IT-Infrastruktur.

Je digitaler die Praxis arbeitet und je mehr digitale Komponenten und Anwendungen zum Einsatz kommen, desto mehr beziehungsweise höhere Anforderungen gelten. Dadurch soll sichergestellt werden, dass die Sicherheitsmaßnahmen angemessen und praktikabel ausgestaltet sind.

4.1 Welcher Praxistyp liegt vor?

Die Anforderungen unterscheiden sich nach Art der Praxis. Dabei gilt:

- **Praxis**: Eine Praxis ist eine vertragsärztliche Praxis mit bis zu fünf ständig mit der Datenverarbeitung betrauten Personen. Hier gelten die Anlagen 1, 5 (und 4 bei medizinischen Großgeräten).

- **Mittlere Praxis**: Eine mittlere Praxis ist eine vertragsärztliche Praxis mit 6 bis 20 ständig mit der Datenverarbeitung betraute Personen. Hier gelten die Anlagen 1, 2, 5 (und 4 bei medizinischen Großgeräten)

- **Großpraxis**: oder Praxis mit Datenverarbeitung im erheblichen Umfang: Eine Großpraxis oder Praxis mit Datenverarbeitung im erheblichen Umfang ist eine Praxis mit über 20 ständig mit der Datenverarbeitung betrauten Personen oder eine Praxis, die in über die normale Datenübermittlung hinausgehenden Umfang in der Datenverarbeitung tätig ist (z. B. Groß-MVZ mit krankenhausähnlichen Strukturen, Labore). Hier gelten die Anlagen 1, 2,3, 5 (und 4 bei medizinischen Großgeräten).

Je nach Praxisgröße unterscheidet die KBV-IT-Sicherheitsrichtlinie in unterschiedliche Anforderungen, die in einzelnen Anlagen geregelt werden (vgl. https://hub.kbv.de/spaces/itsrl/pages/63537214/Praxishinweise)

Anlagen zur IT-Sicherheitsrichtlinie

Anlage 1: Anforderungen für Praxen

Die Basisanforderungen an Technik und Personal gelten für alle Praxen, in denen bis zu fünf Beschäftigte ständig mit der Datenverarbeitung betraut sind.

Anlage 2: Zusätzliche Anforderungen für mittlere Praxen

Sind in der Praxis sechs bis zwanzig Personen ständig mit der Datenverarbeitung betraut, müssen einige Zusatzanforderungen erfüllt werden.

Anlage 3: Zusätzliche Anforderungen für große Praxen

In manchen Praxen sind mehr als zwanzig Personen ständig mit der Datenverarbeitung betraut oder es handelt sich um ein Groß-MVZ mit krankenhausähnlichen Strukturen, in dem die Datenverarbeitung über die normale Datenübermittlung hinausgeht. In diesem Fall müssen nochmals weitere Zusatzanforderungen erfüllt werden.