

CHECKLISTE: BIN ICH BEREIT FÜR §390 SGB V?

Diese Checkliste hilft Ihnen einzuschätzen, ob Ihre Praxis die Anforderungen der neuen IT-Sicherheitsrichtlinie nach §390 SGB V bis zum 01.10.2025 erfüllt.



Die Liste basiert auf dem aktualisierten gesetzlichen Rahmen (gültig seit 01.04.2025) und berücksichtigt auch bestehende Pflichten nach §75b SGB V.

Grundschutz für alle Praxen (Pflicht seit 01.07.2022, §75b SGB V)

Netzplan: Gibt es eine aktuelle, verständliche Darstellung Ihres Praxisnetzwerks?

Tipp: Der Netzplan sollte alle PCs, Router, Drucker, Konnektoren etc. enthalten.

Virenschutz: Wird auf allen Systemen ein aktueller, automatisierter Virenschutz eingesetzt?

Beispiel: Auf dem Empfangs-PC läuft z. B. Windows Defender mit Echtzeitschutz.

Datensicherung: Erfolgt eine regelmäßige und dokumentierte Sicherung Ihrer Daten?

Praxisbeispiel: Tägliches Backup auf ein externes verschlüsseltes NAS.

Passwortschutz: Werden sichere, individuelle Passwörter vergeben und regelmäßig geändert?

Empfehlung: Mindestens 12 Zeichen oder lange Merksätze wie „MeineP@sswörter2025!“

Systemaktualität: Werden Betriebssysteme, Praxissoftware und Medizingeräte regelmäßig aktualisiert?

Tipp: Software-Wartungsvertrag oder Update-Plan mit dem IT-Dienstleister.

Neue Pflicht bis 01.10.2025 (gültig ab 01.04.2025, §390 SGB V)

IT-Einweisung: Werden neue Mitarbeitende beim Eintritt geschult – auch zur IT-Sicherheit?

Beispiel: Kurzanleitung + PDF mit Verhaltensregeln bei E-Mails, USB-Nutzung etc.

Schulungen: Gibt es regelmäßige Fortbildungen zu Cybergefahren und sicherem Verhalten?

Empfehlung: 1x jährlich – viele Versicherer stellen kostenloses Material bereit.

Offboarding: Ist geregelt, wie bei Personalabgängen Zugänge gesperrt und Daten gelöscht werden?

Tipp: Checkliste für Praxisleitung + Löschermerk in der Personalakte.

Cloud-Dienste: Nutzen Sie ausschließlich Anbieter mit C5-Testat des BSI?

Erklärung: Das C5-Testat bestätigt IT-Sicherheit und DSGVO-Konformität.

App-Regelung: Gibt es interne Vorgaben zur App-Nutzung auf Praxisgeräten?

Beispiel: Nur Nutzung über Apple/Google-Store & keine Datenweitergabe über Apps.



Je nach Praxisgröße zusätzlich erforderlich

Ab 6 Mitarbeitenden

Mobile-Richtlinie: Gibt es eine schriftliche Nutzungsregel für dienstliche Mobilgeräte?

Beispiel: „WhatsApp dienstlich verboten“, Automatische Bildschirmsperre nach X Minuten, kein Privatgebrauch.

Ab 21 Mitarbeitenden oder komplexe Praxis

Netzwerksegmentierung: Sind medizinische Geräte vom Verwaltungsnetz getrennt?

Ziel: Angriffe auf Empfangs-PC dürfen nicht das EKG oder Röntgengerät lahmlegen.

Ab 21 Mitarbeitenden oder komplexe Praxis

MDM: Wird die Nutzung mobiler Endgeräte zentral überwacht?

Empfehlung: Microsoft, Cisco oder vergleichbare Lösung mit Fernlöschung für gestohlene Geräte oder zur Überwachung von Aktivitäten.

Bei Großgeräten

Zugriffsschutz: Ist die Wartung von CT/MRT nur durch autorisierte Personen möglich?

Empfehlung: Zugang nur mit Kennwort, keine offenen Fernwartungsports.

Selbsttest-Auswertung

10–12 x [✓]

Ihre Praxis ist gut vorbereitet

7–9 x [✓]

Handlungsbedarf in mehreren Bereichen

<7 x [✓]

Kritische Lücken – prüfen Sie gezielt mit externer Hilfe

Hintergrund zur Gesetzesänderung

Die neue IT-Sicherheitsrichtlinie (§390 SGB V) ersetzt die alte aus §75b.

Das Ziel besteht darin, einheitliche und prüfbare Standards zu schaffen – insbesondere zu Awareness, Dokumentation und technischer Sicherheit. Verstöße können haftungs- oder versicherungsrechtlich relevant werden.

Unser Angebot

- Risikoevaluierung, die den §390 SGB V mit abdeckt
- Musterdokumente (Netzplan, Richtlinien, Schulungsvorlagen)
- Unterstützung bei Cyberversicherbarkeit & Prävention)

Kontakt

eccyber-Team: team@ecclesia-cyber.de



Ihre Dienstleistungen und Versicherungslösungen aus einer Hand

Von der Evaluierung bis zum Incident Response: Unsere Spezialeinheit **eccyber** bietet Ihnen alle Versicherungslösungen und Dienstleistungen, die Sie für ein ganzheitliches Risikomanagement benötigen. Alle Informationen dazu finden Sie hier: qr.ecclesia.de/r/hierbistdu richtig

