IT- Sicherheit nach ISO 27001

Nico Leschnik

- Legal Counsel der GET.ON Online Gesundheitstrainings GmbH
- Zertifizierter ISO 27001 Auditor
- Vormals externer Datenschutzbeauftragter und Consultant für Informationssicherheit

Rechtsgrundlagen

- Art. 32 DSGVO verlangt technische und organisatorische Maßnahmen nach dem Stand der Technik, sowie Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Maßnahmen

- § 4 Abs. 6 i.V.m. Anlage 1 DiGAV, Sektion Datensicherheit:

  „Hat der Hersteller der digitalenGesundheitsanwendung ein Informationssicher-heitsmanagementsystem (ISMS) gemäß ISO 27000-Reihe oder BSI-Standard 200-2 oder ein vergleichbares System umgesetzt und kann auf Verlangen […] ein entsprechendes anerkanntes Zertifikat oder einen vergleichbaren Nachweis vorlegen?“

Die ISO 27000-Normengruppe

- Internationale Industrienormen
- Sicherstellung von Informationssicherheit durch Implementierung eines Informationssicherheitsmanagementsystems (ISMS)
- Festlegung standardisierter technischer und organisatorischer Maßnahmen
  - Hardware/Komponenten
  - Prozesse
  - IT-Systeme
- Ziel: Prozesse definieren, steuern, kontrollieren und stetig verbessern

Die ISO 27000-Normengruppe

- ISO/IEC 27000 – Information security management systems – Overview and vocabulary
- ISO/IEC 27001 – Information security management systems
- ISO/IEC 27002 – Code of practice for information security management;
- ISO/IEC 27005 – Risikomanagement
- ISO/IEC 270017/18 – Datensicherheit im Cloudbereich

Inhalte der ISO 27001

- 114 Controls:
- A.5 Weisungen und Richtlinien zur Informationssicherheit
- A.6 Organisation der Informationssicherheit
- A.7 Personalsicherheit
- A.8 Asset Management
- A.9 Zugangssteuerung
- A.10 Kryptographie
- A.11 Physische und umgebungsbezogene Sicherheit
- A.12 Betriebssicherheit
- A.13 Kommunikationssicherheit
- A.14 Anschaffung, Entwicklung und Instandhalten von Systemen
- A.15 Lieferantenbeziehungen
- A.16 Handhabung von Informationssicherheitsvorfällen
- A.17 Informationssicherheitsaspekte beim BCM
- A.18 Compliance

Dokumentenstruktur eines ISMS

- Leitlinien (z.B. Informationssicherheit)
- Richtlinien (z.B. Kryptographie, Zugangssteuerung, Sicherheitsvorfälle)
- Konzepte (z.B. Anweisungen zur Konfiguration von Systemen)