Projektbüro Digitale Tools

Stand: 23.05.2024

Informationsblatt für Anbieter:innen & Beiräte – Datenschutz & IT-Sicherheit

Vertrauliche Inhalte in den eingereichten Dokumenten dürfen, wenn nötig, geschwärzt werden.

Das Datenschutzkonzept sollte Angaben zu folgenden Aspekten enthalten:

- Datenschutz-Grundverordnung (DSGVO)-Konformität in Konzept und Inhalten
- Klar definierte, zweckgebundene Verarbeitungstätigkeit der gesammelten Daten
- Datenschutzfolgenabschätzung der erhobenen Daten
- Auftragsverarbeitungsvertrag mit zuständigen Dienstleistenden
- Verzeichnis der getroffenen technisch-organisatorischen Maßnahmen (TOM)
- Rollen- und Rechtekonzept (Nutzer:innen greifen nur auf für sie/ihn relevante Daten zu)
- Authentifizierungskonzept (2-Faktor-Authentifizierung)
- Ausgearbeitetes Löschkonzept (unter Beachtung der gesetzlichen Aufbewahrungsfristen)
- DSGVO-konformes Standarddatenschutzmodell (z.B. nach Standard-Datenschutz (SDMv2) Modell)
- Datentransfer in Drittstaaten
- Für Webseiten: Verfahrensverzeichnis (Impressum, Datenschutzangaben, Cookies, usw.)

Das IT-Sicherheitskonzept sollte Angaben zu folgenden Aspekten enthalten:

- IT-Grundschutz nach ISO2700x Normen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) aus Anwender:innen- und Anbieter:innensicht
- Anwendung des BSI Cloud Computing Compliance Criteria Catalogue (BSI C5 Kriterien) und Standardverträge zu den Ergänzenden Vertragsbedingungen für die Beschaffung von IT-Leistungen (EVB-IT)
- Ergebnisbericht durchgeführter Penetrationstests (PEN-Tests)
- Inhaltlich korrekte und extern geprüfte Schutzbedarfsanalyse (siehe Leitfaden BSI)
- Sichere Infrastruktur für Datentransfers
- Authentifizierung der Systeme untereinander (z.B. Verwendung Public Key Infrastruktur (PKI), Virtual Private Network (VPN) Tunnel)
- Verschlüsselungs-/Kryptokonzept (verwendete Standards)
- Schlüssige Auskünfte über Back-Up- und Archivierungsstrategien
- Pseudonymisierungskonzept (Identifikationsnummer (ID) oder Klarnamen zwingend nötig?)

Projektbüro Digitale Tools

Stand: 23.05.2024

Zu beachtende **rechtliche Vorgaben:**

- Datenschutzgrundverordnung der Europäischen Union (EU-DSGVO)
- Bundesdatenschutzgesetz (BDSG)
- Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG)
- Technische und organisatorische Maßnahmen (TOM): Backups für Daten, Protokollierung von Zugriffen

Anwendbare **Rahmenwerke:**

- IT-Grundschutz-Kompendium und IT-Grundschutz Profile des BSI:
  - BSI-Standard 200-1: Managementsysteme für Informationssicherheit
  - BSI-Standard 200-2: IT-Grundschutz Methodik
  - BSI-Standard 200-3: Risikomanagement
  - BSI-Standard 200-4: Business Continuity Management

- BSI-Standard 100-4: Notfallmanagement

- Sicherheitszertifizierungen:
  - International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 25000: Software-Engineering – Qualitätskriterien und Bewertung von Softwareprodukten (SQuaRE) – Leitfaden für SQuaRE
  - ISO / IEC 25010: Qualitätskriterien von Software, IT-Systemen und Software-Engineering
  - ISO / IEC 27001: Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmanagementsysteme – Anforderungen
  - ISO / IEC 27002: IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management

- Schutz vor Angriffen und Sicherheitsrisiken:
  - Open Web Application Security Project (OWASP) Top 10: Sensibilisierungsdokument zum Minimieren von Sicherheitsrisiken mit Informationen zu den zehn kritischsten Risiken
  - Penetrationstest und Schwachstellenanalyse entsprechend des Security Assurance Levels (SEAL)