Projektbüro
Digitale Tools

Stand: 17.07.2023

Informationsblatt für Anbieter & Beiräte – Datenschutz & IT-Sicherheit

Vertrauliche Inhalte können bei allen Konzepten, wenn nötig, geschwärzt werden.

Das Datenschutzkonzept sollte Angaben zu folgenden Aspekten enthalten:

- DSGVO-Konformität von Konzept und Inhalten
- Klar definierte, zweckgebundene Verarbeitungstätigkeit der gesammelten Daten
- Datenschutzfolgenabschätzung der erhobenen Daten
- Auftragsverarbeitungsvertrag mit dem zuständigen Dienstleister
- Verzeichnis der getroffenen TOM (technisch-organisatorische Maßnahmen)
- Rollen- und Rechtekonzept (Nutzer greift nur auf für ihn relevante Daten zu)
- Authentifizierungskonzept (2-Faktor-Authentifizierung)
- Ausgearbeitetes Löschkonzept (unter Beachtung der gesetzlichen Aufbewahrungsfristen)
- DSGVO-konformes Standarddatenschutzmodell (z.B. nach SDMv2-Modell)
- Datentransfers in Drittstaaten
- Verfahrensverzeichnis für Webseiten (Impressum, Datenschutzangaben, Cookies, usw.)

Das IT-Sicherheitskonzept sollte Angaben zu folgenden Aspekten enthalten:

- IT-Grundschutz nach ISO2700x Normen (BSI) aus Anwender- und Herstellersicht
- Anwendung der C5-Kriterien und EVB-IT-Standardverträge
- Bericht und Ergebnisse durchgeführter PEN-Tests
- Inhaltlich korrekte und extern geprüfte Schutzbedarfsanalyse (siehe Leitfaden BSI)
- Sichere Infrastruktur für Datentransfers
- Authentifizierung der Systeme untereinander (z.B. Verwendung PKI, VPN-Tunnel)
- Verschlüsselungs-/Krypto-Konzept (verwendete Standards)
- Schlüssige Auskünfte über Back-Up- und Archivierungsstrategien
- Pseudonymisierungskonzept (IDs, oder Klarnamen zwingend nötig?)