Zugriffskontrolle in der Anwendung Spektor

Dokumentationsbaustein (DSGVO / ISMS)

Zweck und Zielsetzung

Die Anwendung Spektor setzt ein funktions- und objektgruppenbasiertes Berechtigungskonzept um. Ziel ist es, den Zugriff auf Funktionen und Daten auf das erforderliche Minimum zu begrenzen (Need-to-know und minimale Rechtevergabe).

Grundprinzip

Zugriffsrechte werden nicht pauschal vergeben, sondern ergeben sich aus der Kombination von Funktion und Objektgruppe:

- Funktionen definieren, welche Tätigkeiten in Spektor ausgeführt werden dürfen (z.B. Einsicht, Bearbeitung, Administration).
- Objektgruppen definieren den Zuständigkeitsbereich (z.B. Kommune, Einrichtung, Standort).

Schutzwirkung

Durch dieses Modell wird sichergestellt, dass:

- Benutzer ausschließlich auf Daten innerhalb ihres Zuständigkeitsbereichs zugreifen können.
- eine klare Bereichs- bzw. Mandantentrennung gewährleistet ist.
- personenbezogene und sensible Daten vor unbefugtem Zugriff geschützt sind.
- Berechtigungen nachvollziehbar und prüfbar vergeben werden können.

Bezug zu Datenschutz und Informationssicherheit

Das Berechtigungskonzept unterstützt insbesondere Anforderungen aus:

- DSGVO (insb. Art. 5, Art. 25, Art. 32) zur Integrität, Vertraulichkeit und dem Schutz durch Technikgestaltung.
- kommunalen IT-Sicherheitsrichtlinien (Zugriffskontrolle).
- ISO/IEC 27001 (Zugriffskontrolle).

Hinweis: Inhalte können organisationsspezifisch (z.B. Rollenbezeichnungen, Zuständigkeiten) angepasst werden.