ISDS-Konzept

Kopf \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Bezeichnung des Informatikprojekts
* Zuständige Stelle der Gemeinde
* Projektverantwortlicher, inkl. Kontaktinformationen
* Version/Datum (Versionenkontrolle)
* Visum des Projektauftraggebers

1. Angaben zum Projekt

(es kann auch auf bereits bestehende Projektdokumente verwiesen werden)

* Detaillierte Beschreibung des Prozesses oder der Prozesse, die mit der geplanten Informatiklösung unterstützt werden sollen.
* Beschreibung der Input- und Output-Schnittstellen, insbesondere der Online-Zugriffe für Dritte (Abrufverfahren).
* Beschreibung der zur Wahl stehenden IT-Lösung(en).

2. Datenschutz

* Benennung der für den Prozess bzw. die Prozesse massgeblichen Rechtsgrundlagen, insbesondere auch der Rechtsgrundlagen für Online-Zugriffe von Dritten (Abrufverfahren), vgl. Checkliste Datenschutzbeurteilung.
* Gegebenenfalls Ausführungen zu den Möglichkeiten, noch fehlende oder ungenügende Rechtsgrundlagen bis zur Inbetriebnahme des Systems schaffen zu können.
* Datenarchivierung und -vernichtung.
* Beschreibung der Verfahren zur Gewährleistung der Datenschutzrechte der betroffenen Personen (Auskunft/Einsicht, Berichtigung und Sperrung).
* Benutzerberechtigungskonzept
* Anmeldung der Datensammlung(en) bei der Datenschutzaufsichtsstelle (als Anlage).

3. Informationssicherheit

Grundschutz

Anhand der Checkliste Grundschutz[[1]](#footnote-1) ist darzulegen, welche Grundrisiken der Infrastruktur und der Daten- und Benutzerverwaltung bestehen und welche Massnahmen getroffen worden sind, um den Grundschutz zu gewährleisten.

Erhöhter Schutzbedarf / Applikationsschutz

Es sind sodann Aussagen darüber zu machen, ob ein erhöhter Schutzbedarf, über den Grundschutz hinaus, besteht und welche Massnahmen hierzu getroffen werden. Anhaltspunkte ergeben sich aus der Risikobeurteilung:

Die Risikobeurteilung für eine Applikation beinhaltet:

* 1. Eine *Informationswertanalyse* zeigt auf, welcher materielle Schaden bei einem Teil- oder Gesamtverlust der Informationen entstehen würde.
  2. Eine *Bedrohungsanalyse* deckt auf, wer allenfalls an einem (illegalen) Zugang zu den Informationen ein Interesse haben könnte und welches kriminelle Potential ein Missbrauch der Informationen darstellen könnte.
  3. Mittels einer *Klassifizierung*, wird die Applikation punkto Verfügbarkeit und Vertraulichkeit der Daten eingeordnet.

4. Massnahmen

Auflistung der bis zur Inbetriebnahme erforderlichen technischen und organisatorischen Massnahmen, wobei obligatorisch sind:

* Benutzerberechtigungskonzept
* Grundschutzmassnahmen Informationssicherheit gemäss Checkliste Grundschutz
* Massnahmen, die allenfalls einen erhöhten Schutzbedarf abdecken.
* Angaben zur Umsetzung der Massnahmen bis zur Systemeinführung (Massnahmenplan)

1. Zum Erstellen dieser Liste ist ein anerkannter Standard anzuwenden [z. B: Best practices aus ISO 27000 ([www.iso.org/iso/catalogue\_detail?csnumber=41933](http://www.iso.org/iso/catalogue_detail?csnumber=41933) ), BSI-Handbuch (<https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html;jsessionid=289D252805C9E8B063DA1BCA72CE0418.2_cid241> ), WiSB (<https://www.isb.admin.ch/isb/de/home/themen/sicherheit.html>)] [↑](#footnote-ref-1)