Öffentliche Beschaffung und Informationssicherheit

Julia Bhend – Vergabetagung 2024

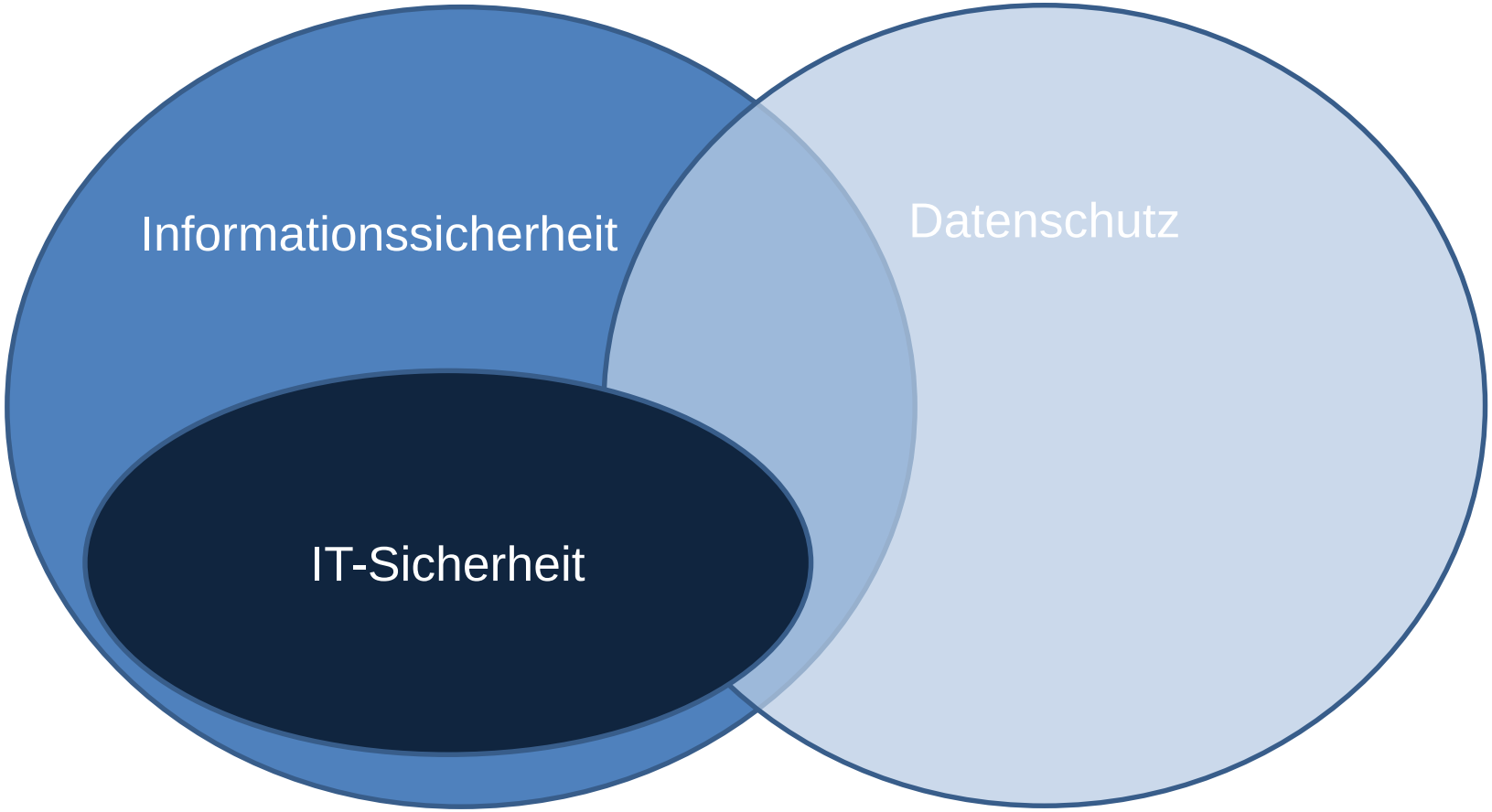
PROBSTPARTNER

Einleitung

Was ist Informationssicherheit?

- Schutz von Informationen in Bezug auf
  - Vertraulichkeit
  - Verfügbarkeit
  - Integrität
  - Nachvollziehbarkeit der Bearbeitung

Informationssicherheit vs. Datenschutz



Was bezweckt Informationssicherheit?

Schutzobjekte:

- Infrastruktur, Anwendungen, Informationssysteme, Datensammlungen, Produkte und Dienste zur elektronischen Verarbeitung von Informationen
- Personendaten, andere Daten und Informationen gleich welcher Art und Form

Zweck:

- Schutz der Entscheidungs- und Handlungsfähigkeit der öffentlichen Organe
- Schutz der öffentlichen Sicherheit
- Schutz der wirtschaftspolitischen Interessen der Schweiz
- Schutz der Persönlichkeits- und Grundrechte der betroffenen Personen

Rechtsgrundlagen

- Datenschutz- und Informationssicherheit:
  - Datenschutzgesetz (DSG), Informationssicherheitsgesetz (ISG) und zugehörige Verordnungen des Bundes
  - kantonale Datenschutz- und Informationsschutzgesetze
  - bereichsspezifische Regelungen (u.a. Personal, Gesundheitsbereich)
  - Verwaltungsverordnungen und Weisungen

- Besondere Geheimhaltungspflichten
  - Amts- und Berufsgeheimnis (Art. 320 / 321 StGB)
  - Weitere Geheimhaltungspflichten (u.a. Sozialversicherungen, Steuergesetze, Gesundheitsbereich)

- BöB / IVöB

Informationssicherheitsgesetz des Bundes (ISG)

- Persönlicher Geltungsbereich:
  - verpflichtete Behörden und Organisationen des Bundes gemäss Art. 2 Abs. 1 und 2 ISG
  - Teilweise: öffentliche und private Betreiber kritischer Infrastrukturen (Art. 2 Abs. 5 ISG)
  - Teilweise: Kantone, soweit sie klassifizierte Informationen des Bundes bearbeiten oder auf Informatikmittel des Bundes zugreifen und nicht eine mind. gleichwerte Informationssicherheit gewährleisten (Art. 3 ISG)

- Personensicherheitsprüfungen / Betriebssicherheitsverfahren nach ISG:
  - Kantone können dazu für ihre eigene Informationssicherheit unter bestimmten Voraussetzungen Leistungen der Fachstellen des Bundes in Anspruch nehmen (Art. 86 Abs. 4 ISG i.V.m. Art. 35 VPSP bzw. Art. 24 VBSV).

Warum muss sich die öffentliche Auftraggeberin mit Informationssicherheit befassen?

- Informationssicherheit muss durch geeignete technische und organisatorische Massnahmen gewährleistet werden (Art. 6 ISG und Art. 3 ISV / Art. 8 Abs. 1 DSG und Art. 1 DSV).

- Die Massnahmen müssen angemessen sein angesichts
  - Zweck, Art und Umfang der Datenbearbeitung
  - Schutzbedarf und möglicher Risiken für die betroffenen Personen
  - Stand der Technik
  - Kosten

Warum muss sich die öffentliche Auftraggeberin mit Informationssicherheit befassen?

- Zusammenarbeit mit Auftragnehmern ist nur unter bestimmten Voraussetzungen zulässig (Art. 9 ISG / Art. 9 DSG):
  - Übertragung der Bearbeitung durch Vereinbarung oder Gesetz
  - Informationssicherheit muss im Vertrag geregelt werden
  - keine widersprechenden Geheimhaltungsverpflichtungen.

- Bei Bearbeitung von Informationen durch einen Auftragnehmer verbleibt die Verantwortung für die Informationssicherheit (auch) bei der Auftraggeberin.

Warum müssen sich die Anbieter mit Informations-sicherheit befassen?

- Unterstehen selbst den Datenschutzgesetzen und damit auch direkt Datensicherheitspflichten

- Bei Zusammenarbeit mit öffentlichen Auftraggebern müssen sich Anbieter an die Anforderungen und Massnahmen der Informationssicherheitsgesetzgebung und der Ausschreibung bzw. des Vertrags halten

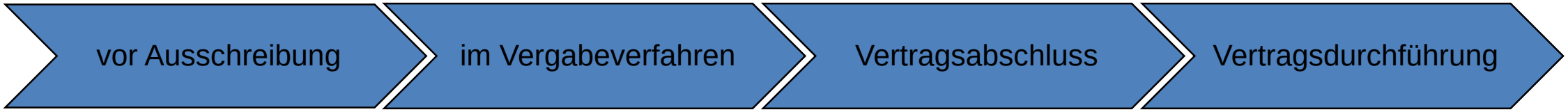
Vor der Ausschreibung zu klären

- Welche Daten und Systeme sind betroffen?
- Was ist deren Schutzbedarf?
- Was sind die möglichen Folgen einer Verletzung der Informationssicherheit?
- Welche Mindestvorgaben gelten?

Instrumentarium im Beschaffungsprozess

- Rechtsgrundlagenanalyse (RGA)
- Schutzbedarfsanalyse (Schuban)
- Abklärungen Risiken und Alternativen
- ISDS-Konzept
- Datenschutz-Folgenabschätzung (DSFA) / Vorabkontrolle
- Personensicherheitsprüfungen (PSP) / Betriebssicherheitsverfahren (BSV)
- Vertrag

Ablauf


vor Ausschreibung
im Vergabeverfahren
Vertragsabschluss
Vertragsdurchführung

Informationssicherheit im Beschaffungsprozess

Vergabeverfahren

- Selektives Verfahren
- Dialog
- Geheimhaltungsvereinbarungen für Vergabeverfahren
- Optionen und Varianten in Bezug auf Informationssicherheit
- Mindestanforderungen (EK/TS)
- Bewertung der Angebote in Bezug auf Informationssicherheit (als ZK vorsehen)

Informationssicherheit im Beschaffungsprozess

Ausnahmen vom Beschaffungsrecht aus Sicherheitsinteressen

- Nach Art. 10 Abs. 3 lit. a IVöB 2019 bzw. Art. 10 Abs. 4 lit. a BöB findet Beschaffungsrecht keine Anwendung, wenn dies für den Schutz und die Aufrechterhaltung der äusseren oder inneren Sicherheit oder der öffentlichen Ordnung als erforderlich erachtet wird.

- Staatsvertragskonforme Auslegung verlangt differenzierte Anwendung (vgl. Art. III Ziff. 1 vs. Art. III Ziff. 2 lit. a GPA 2012).

- Unterscheidung zwischen
  - Aufträgen für nationale Sicherheits- und Verteidigungszwecke → integral ausgenommen
  - Anderen Aufträgen, die öffentliche Sicherheitsinteressen tangieren →nur ausgenommen, wenn und soweit keine weniger wettbewerbsbeschränkenden Massnahmen möglich

Informationssicherheit im Beschaffungsprozess

Betriebssicherheitsverfahren (BSV) nach ISG

- Einleitung auf Antrag der Auftraggeberin, die sicherheitsempfindlichen Auftrag vergeben möchte
  - Bearbeitung von "vertraulich" oder "geheim" klassifizierten Informationen
  - Verwaltung, Betrieb, Wartung und Überprüfung von Informatikmitteln der Sicherheitsstufe "hoher Schutz" oder "sehr hoher Schutz"
  - Zugang zu Sicherheitszonen
- Als EK vorsehen / Ausschluss aus Vergabeverfahren, wenn Sicherheitsrisiko festgestellt wird (Art. 58 Abs. 2 ISG)
- Gültigkeit Betriebssicherheitserklärung:
  - Grds. fünf Jahre
  - auch für weitere sicherheitsempfindliche Aufträge (ggf. Anpassung Sicherheitskonzept nötig)
  - Widerruf möglich, wenn Pflichten (insb. Sicherheitskonzept und Meldepflichten) nicht eingehalten werden

Informationssicherheit im Beschaffungsprozess

Vertrag: mögliche Regelungspunkte

- Verfügungsbefugnis über die Daten
- Einhaltung der Vorgaben betr. Geheimhaltung, Datenschutz und Informationssicherheit
- Vereinbarung von konkreten technischen und organisatorischen Massnahmen und Aktualisierung der Massnahmen
- Ort der Bearbeitungsaktivitäten und Datenspeicherung
- Einsatz und Wechsel von Subunternehmen
- Umgang mit Herausgabebegehren von Dritten
- Melde- und Unterstützungspflichten bei Sicherheitsvorfällen
- Kontrollen
- Export der Daten, Löschung und Unterstützung bei Beendigung
- Ausstiegsmöglichkeiten

Informationssicherheit im Beschaffungsprozess

Überprüfung

91. Die Umsetzung und Einhaltung der Sicherheitsmassnahmen sind zu prüfen. Der Auftragsbearbeiter selbst hat Audits durchzuführen und ungewöhnliche Sicherheitsvorfälle dem Verantwortlichen zu melden. Dies ergibt sich bereits aus den Grundschutzmassnahmen von Art. 7 aDSG und aus dem Grundsatz von Treu und Glauben. Der Verantwortliche kann sich ein Auditrecht ausbedingen und sich auch Auditberichte des Auftragsbearbeiters vorlegen lassen.

Auszug aus Schlussbericht des EDÖB vom 25. April 2024 in Sachen Xplain AG

Kontakt

Julia Bhend
julia.bhend@probstpartner.ch

Probst Partner AG, Winterthur/Zürich
+41 52 269 14 00
www.probstpartner.ch
swissdataprotectionlaw.ch