Cloud-spezifische Risiken und Massnahmen

Überarbeitetes Merkblatt von privatim

Fachgruppe von Jurist:innen im E-Government vom 6. April 2022

Ueli Buri, Datenschutzbeauftragter des Kantons Bern

Auftragsbearbeitung: Begriff und Verantwortung

z.B. Art. 16 DSG:

«[1] Für den Datenschutz ist das Bundesorgan verantwortlich, das die Personendaten in Erfüllung seiner Aufgaben bearbeitet oder bearbeiten lässt.»

→ Auftragsbearbeitung = Beizug von Hilfspersonen bei der Erfüllung der *eigenen* öffentlichen Aufgabe

→ öffentliches Organ bleibt für den Datenschutz verantwortlich, und zwar für alle Aspekte des Gesetzes:

- Grundsätze (Legalitätsprinzip, Zweckbindung, Verhältnismässigkeit)
- Datensicherheit
- Gewährung der Betroffenenrechte

Auftragsbearbeitung: Leitlinien

- Übertragung von Datenbearbeitung an Dritte darf für die Rechte der betroffenen Personen nicht nachteilig sein

  Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23. März 1988, BBl 1988 II 413

- Verfassungsmässige Garantien dürfen nicht dadurch umgangen werden, dass Datenbearbeitung aus Schweiz ausgelagert wird

- Schranken aus der übrigen Rechtsordnung (insbes. gesetzliche Geheimhaltungspflichten) sind zu beachten

Auftragsbearbeitung: Gesetzlicher Rahmen

Allgemeine Grundsätze zur Auslagerung von Datenbearbeitungen:

- Auftragsbearbeiter darf Daten nur so bearbeiten, wie das öffentliche Organ selbst es dürfte (insbes. nicht für eigene Zwecke)
- Es dürfen keine Geheimhaltungspflichten entgegenstehen
- Auftragsbearbeiter muss die Datensicherheit gewährleisten
- Beizug von Unterbeauftragten nur mit vorgängiger Zustimmung des öffentlichen Organs

Und: keine Übermittlung von Daten in Staaten ohne angemessenen Datenschutz

→ Regelung in geeigneter vertraglicher Vereinbarung notwendig !

Einsatz von Online-Diensten («Cloud»)

Kernrisiko = Kontrollverlust beim Schutz von Grundrechten !

- Gestaltungsspielraum Vertragsbedingungen
  - ISDS-Verhaltens- und Sorgfaltspflichten des Auftragsbearbeiters
  - Kontrollrecht und -möglichkeit
  - Durchsetzbarkeit (Rechtswahl und Gerichtsstand)
- Ort(e) der Datenbearbeitungen → ausl. Behördenzugriffe
- Vertraulichkeit / Geheimnisschutz
- Umgang mit Daten über Nutzer:innen
- Einsatz von Unterbeauftragten

Bearbeitungsort(e) und ausländische Behördenzugriffe

- Keine Datenübermittlung *in* Länder ohne angemessenen Datenschutz (und kein Zugang von Personen *aus* solchen Ländern)

  → wo eine genügende Gesetzgebung fehlt, kann ein angemessener Datenschutz vertraglich – insbes. mit anerkannten Standardvertragsklauseln – erreicht werden, AUSSER wenn Zugriffe ausländischer Behörden möglich sind, welche den folgenden Grundrechtsgarantien nicht genügen («Schrems II»/Anleitung EDÖB):

  - Legalitätsprinzip
  - Verhältnismässigkeit
  - Betroffenenrechte
  - Rechtsweggarantie

- Übermittlung innerhalb CH/EU an Cloud-Anbieter, der dem CLOUD Act o.ä. untersteht, ist m.E. (noch) nicht unzulässig und damit einer Risikobeurteilung zugänglich

Vertraulichkeit

z.B. Art. 8 revDSG:

«[1] Der Verantwortliche und der Auftragsbearbeiter gewährleisten durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit.»

→ Schutz aller Personendaten gegen unbefugten Zugang durch Dritte

Transportverschlüsselung zwingend, angemessener Schutz von «data at rest»

→ Schutz von besonderen Personendaten vor erhöhten Risiken beim Cloud-Anbieter

- Verschlüsselung durch das öffentliche Organ
- Verschlüsselung durch Cloud-Anbieter, sofern angemessener Schutz durch übrige Massnahmen gewährleistet ist

Geheimnisschutz

Pro memoria: Outsourcing zulässig, sofern keine Geheimhaltungspflicht entgegensteht

- Datenschutz folgt Zulässigkeit gemäss einschlägiger Gesetzgebung (insbes. Art. 320 und 321 StGB)

  → jeweilige Geheimhaltungsvorschrift (inkl. Rechtsprechung) legt fest, inwieweit Bekanntgabe an Hilfsperson datenschutzrechtlich zulässig ist

- Datenschutz und Geheimnisschutz sind unterschiedliche Konzepte
- Verschiedene Auffassungen zum Outsourcing von Geheimnissen
  - BRat (Botschaft ISG): nur an Hilfsperson, die selbst (Amts-) Geheimnis untersteht
  - BGE 145 II 229 E. 7.4: Berufsgeheimnis (des Anwalts) erlaubt keine Subdelegation
  - Lehre: höchst unterschiedliche Meinungen, von sehr streng bis sehr liberal …

Daten über Nutzer:innen / Unterbeauftragte

- Daten über Nutzer:innen dürfen nur so erhoben und ausgewertet werden, wie das öffentliche Organ selbst es dürfte
  - Umfang und Bearbeitungszwecke sind offenzulegen
  - Sind gleich zu schützen wie Inhaltsdaten
  - Weitergehende Bearbeitung nur mit mindestens pseudonymisierten Daten
- Unterbeauftragte sind einzeln so auszuweisen, dass Zulässigkeit und Risiken beurteilt werden können
  - Pflichten zur Steuerung und Kontrolle sind in Vertrag festzuhalten
  - Kündigungsrecht anstatt vorgängiger Zustimmung zulässig, aber …

Umfassende Risikobeurteilung

z.B. Art. 22 revDSG:

«[3] Die Datenschutz-Folgenabschätzung enthält eine Beschreibung der geplanten Bearbeitung, eine Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen zum Schutz der Persönlichkeit und der Grundrechte.»

Nutzungskonzept:

→ «Welche Daten müssen/sollen durch wen (alles) wozu bearbeitet werden können?»

ISDS-Konzept:

- Risiken: Beschreibung und Bewertung der Risiken für alle Betroffenen (differenziert nach Inhalten und ev. Services)
- Massnahmen: technisch (insbes. 🔒), organisatorisch und (soweit mögl.) vertraglich

  → müssen Risiken beseitigen oder auf ein tragbares Mass reduzieren

Risikoentscheid

- Zusätzliche Risiken müssen durch unverzichtbare Vorteile
  - des Online-Dienstes gegenüber einer gleichwertigen Variante *on premise* und
  - des Produkts gegenüber risikoärmeren Produkten anderer Anbieter

  aufgewogen werden
- Auf Datenbearbeitungen mit hohen Restrisiken ist zu verzichten
- Es muss ein «Plan B» für untragbare Veränderungen bestehen
- Entscheid muss vom obersten Leitungsorgan getroffen werden
- Bei Daten unter gesetzlicher Geheimhaltungspflicht: Beizug vorgesetzte Behörde bzw. Aufsichtsbehörde empfohlen

Kontakt

Ueli Buri, Datenschutzbeauftragter
+41 31 636 64 46 (direkt), ueli.buri@be.ch

Datenschutzaufsichtsstelle des Kantons Bern (DSA)
Poststrasse 25, 3072 Ostermundigen
+41 31 633 74 10, www.be.ch/dsa