Datenschutz bei Cloud Services

Rechtliche Einordnung und Herausforderungen

IT-Beschaffungskonferenz vom 26. August 2021

Ueli Buri, Datenschutzbeauftragter des Kantons Bern

Grundrecht auf Privatsphäre und Schranken

Art. 13 BV Schutz der Privatsphäre

[1] Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs.

[2] Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.

Art. 36 BV Einschränkungen von Grundrechten

[1] Einschränkungen von Grundrechten bedürfen einer gesetzlichen Grundlage. […]

[2] Einschränkungen von Grundrechten müssen durch ein öffentliches Interesse oder durch den Schutz von Grundrechten Dritter gerechtfertigt sein.

[3] Einschränkungen von Grundrechten müssen verhältnismässig sein.

[4] Der Kerngehalt der Grundrechte ist unantastbar.

Anwendbares Datenschutzrecht

Bundesgesetz über den Datenschutz (DSG):

Gilt für die Bearbeitung von Personendaten durch

a. private Personen; → *Persönlichkeitsschutz*

b. Bundesorgane.

Kantonale Datenschutzgesetze:

Gelten für die Bearbeitung von Personendaten durch kantonale öffentliche Organe → *Grundrechtsschutz*

Öffentliches Organ = Verwaltung & Dritte, die mit öffentlicher Aufgabe betraut sind

Allgemeine Grundsätze

Gelten für *jede* Bearbeitung von Personendaten:

- Rechtmässigkeit
- Zweckbindung
- Verhältnismässigkeit
- Richtigkeit
- Transparenz
- Datensicherheit

Verantwortung

«Für den Datenschutz ist das [Bundes-] Organ verantwortlich, das die Personendaten in Erfüllung seiner Aufgaben bearbeitet oder bearbeiten lässt» (Art. 16 DSG).

Verantwortung umfasst alle Aspekte des Gesetzes, d.h.

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

Datenbearbeitung im Auftrag («Outsourcing»)

Allgemeine Grundsätze (vgl. Art. 9 revDSG):

- zulässig, sofern keine Geheimhaltungspflicht entgegensteht
- Auftragsbearbeiter darf Daten nur so bearbeiten, wie es das öffentliche Organ darf (d.h. *nicht* für eigene Zwecke)
- Auftragsbearbeiter muss die Datensicherheit gewährleisten
- Beizug von Unterbeauftragten nur mit Zustimmung des öffentl. Organs
- Öffentliches Organ bleibt für die Datenbearbeitung verantwortlich

→ *Geeignete* vertragliche Vereinbarung notwendig !

Einsatz von Online-Diensten («Cloud»)

Besondere Herausforderungen:

- Gestaltungsspielraum Vertragsbedingungen
  - ISDS-Verhaltens- und Sorgfaltspflichten des Auftragsbearbeiters
  - Kontrollrecht und -möglichkeit
  - Durchsetzbarkeit
- Ort(e) der Datenbearbeitungen
- Einsatz von Unterbeauftragten
- Vertraulichkeit / Geheimnisschutz
- Umgang mit Benutzerdaten
- Zugriffe von ausländischen Behörden

z.B. Microsoft 365

- SIK/MS Business und Service-Vertrag (2010): Recht/Gerichte von IRL
- Einheitliche Online Services Terms mit Datenschutznachtrag (DPA) für alle (privaten/kommerziellen und öffentlichen) Kunden weltweit

  → beschränkte Bereitschaft / Möglichkeit für kundenspezifische Zusicherungen
- Enthalten weitreichende Ermächtigungen zugunsten von Microsoft
  - Datenbearbeitungen für «legitime Geschäftstätigkeiten» von MS
  - Orte der Datenbearbeitungen (≠ Ort der ruhenden Kundendaten)
  - Einsatz von Unterbeauftragten
- Enthalten zwar Standardvertragsklauseln für Datenübermittlungen in Länder ohne angemessenen Datenschutz, aber … («Schrems II»)

MS 365: Legitime Geschäftstätigkeiten von MS

– MS verarbeitet Kundendaten und weitere Personendaten für «legitime Geschäftstätigkeiten von Microsoft», d.h.:

  (1) Abrechnungs- und Kontoverwaltung;

  (2) Vergütung (z.B. Berechnung von Mitarbeiterprovisionen und Partner-Incentives);

  (3) interne Berichterstattung und Geschäftsmodellierung (z.B. Prognose, Umsatz, Kapazitätsplanung, Produktstrategie);

  (4) Bekämpfung von Betrug, Cyberkriminalität oder Cyberangriffen;

  (5) Verbesserung der Kernfunktionalität in Bezug auf Barrierefreiheit, Datenschutz oder Energieeffizienz; und

  (6) Finanzberichterstattung und Einhaltung gesetzlicher Verpflichtungen.

– Unverbindliches «White Paper»: meist mit pseudonymisierten Daten

MS 365: Datenbearbeitungsorte

– «[…] beauftragt der Kunde Microsoft, Kundendaten und personenbezogene Daten in die Vereinigten Staaten von Amerika oder in jedes andere Land zu übermitteln, in dem Microsoft oder ihre Unterauftragsverarbeiter tätig sind, und Kundendaten und personenbezogene Daten zur Bereitstellung der Onlinedienste zu speichern und zu verarbeiten, ausgenommen wie an anderer Stelle in den DPA-Bestimmungen beschrieben».

– EuGH Urteil C-311/18 («Schrems II») / EDÖB: kein angemessenes Datenschutzniveau in den USA

  Grund: ungenügende Garantien bei Zugriffen der US-Behörden

MS 365: Unterbeauftragte

Pro memoria: Beizug von Unterbeauftragten nur mit Zustimmung des öffentlichen Organs

- DPA enthält
  - pauschale Zustimmung zu allen aktuellen und künftigen Unterbeauftragten
  - Zusicherung von vertraglichen Pflichten der Unterbeauftragten gegenüber MS
  - Prozess bei neuen Unteraufträgen: Information + a.o. Kündigungsrecht des Kunden
- MS Trust Center:
  - Weitergehende Zusicherungen zum Datenzugriff von Unterbeauftragten
  - «Subprocessors List»:

Subprocessor	Service Provided	Corporate Location	Type of Data
AT&T Inc	Multi-factor Authentication	United States	Customer Data Pseudonymous

Subprocessor	Corporate Location	Type of Data
Infosys Ltd	India	Customer Data Pseudonymous

MS 365: Gelöste und offene Punkte

- Zusatzvereinbarung SIK/MS vom Oktober 2020 (bis April 2022)
  - DPA bleibt während Vertragslaufzeit unverändert
  - Schweizer Recht und Gerichtsbarkeit für Klagen wegen Verletzung des DPA (bei Geldklagen erst ab Streitwert von CHF 150'000)
  - Haftungsbeschränkung auf Lizenzkosten für 6 Monate
- Individuelle Zusagen zu «legitimen Geschäftstätigkeiten» möglich
- Schutz der Vertraulichkeit nur beschränkt kontrollierbar (auch mit 🔒)
- «EU Data Boundary for the Microsoft Cloud» angekündigt
- Risiko von Zugriff durch US-Behörden bleibt (CLOUD Act)

Nutzungs- und ISDS-Konzept

Art. 22 revDSG Datenschutz-Folgenabschätzung

[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 (ggf. differenziert nach Inhalten)
- Massnahmen zur Risikobewältigung: technisch, organisatorisch und ggf. vertraglich

Nochmals MS 365: Azure MFA im Kanton Bern

- Formelles Projekt mit fachlicher Evaluation möglicher Lösungen
- Risikoanalyse zu MS Azure AD und MFA:
  - Klärung der Datenflüsse (was wird wo verarbeitet/gespeichert), soweit möglich
  - Erläuterung von tatsächlichen und rechtlichen Fragen mit MS Schweiz
  - Durchführung Pilotphase mit pseudonymiserten Benutzern
- Massnahmen:
  - Verzicht auf Authentisierungsmethoden mit ständiger Verarbeitung in den USA
  - Formelle Protokollierung der Erläuterungen von MS Schweiz
- Schriftliche Bestätigung der akzeptierten Restrisiken (GL KAIO)

Erkenntnisse

für einen datenschutzkonformen Einsatz von Cloud Services:

- «Datenschutz ist Chef*innen-Sache»
- fachliche Bedürfnisse klar beschreiben / dokumentieren
- sich nicht voreilig von «einfachen» Lösungen verführen lassen
- Schutzbedarf & Risiken für *alle* Betroffenen sauber analysieren
- untragbare Risiken beseitigen, Restrisiken bewusst akzeptieren
- auf Einsatz mit hohen Restrisiken verzichten

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