Kanton Bern
Canton de Berne

1

Cloud in der Verwaltung

26. Symposium on Privacy and Security vom 15. Juni 2022

Ueli Buri, Datenschutzbeauftragter des Kantons Bern / Präsident der Konferenz der schweizerischen Datenschutzbeauftragten (privatim)

1

Kanton Bern
Canton de Berne

2

Ab in die Cloud (wie die Privatwirtschaft), oder nicht?

«Allgemein kann festgehalten werden, dass der Verzicht auf die M365-Cloud-Lösung dazu führt, dass der Kanton Zürich sich technologisch ins Abseits manövriert, da er sich im Unterschied zur Privatwirtschaft und zu fortschrittlichen Gemeinwesen dem technologischen Fortschritt verschliesst.»

Quelle: Protokoll des Regierungsrates des Kantons Zürich vom 30.03.2022 («542. Einsatz von Cloud-Lösungen in der kantonalen Verwaltung [Microsoft 365], Zulassung»)

2

Kanton Bern
Canton de Berne

3

Legalitätsprinzip

Art. 5 BV Grundsätze rechtsstaatlichen Handelns

[1] Grundlage und Schranke staatlichen Handelns ist das Recht.

→ Staat darf Private nur im Rahmen des Rechts einschränken

Datenschutzrecht: Private dürfen Personendaten bearbeiten, solange sie die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen

→ Staat darf selber nur im Rahmen des Rechts handeln

Datenschutzrecht: Öffentliche Organe dürfen Personendaten nur bearbeiten, soweit dafür eine genügende Rechtsgrundlage besteht

3

Kanton Bern
Canton de Berne

4

Privates Datenschutzrecht

Art. 30 nDSG Persönlichkeitsverletzungen

[1] Wer Personendaten bearbeitet, darf die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen.

Art. 31 nDSG Rechtfertigungsgründe

[1] Eine Persönlichkeitsverletzung ist widerrechtlich, wenn sie nicht durch Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist.

→ Abwägung zwischen zwei privaten Interessensphären, welche sich *beide* auf verfassungsmässige Rechte stützen

4

Kanton Bern
Canton de Berne

5

Einwilligung der betroffenen Person

z.B. Allgemeine Geschäftsbedingungen der Zürcher Kantonalbank:

15. Auslagerung von Geschäftsbereichen und Dienstleistungen

Die Bank kann Geschäftsbereiche und Dienstleistungen, z.B. […] Betrieb von Informations- und Kommunikationstechnologien, ganz oder teilweise an Konzerngesellschaften oder Dienstleister im In- und Ausland auslagern.

16. Datenschutz und Bankkundengeheimnis

Die Bank bearbeitet Kundendaten zur Abwicklung ihrer Leistungen und für eigene oder gesetzlich vorgeschriebene Zwecke. Dazu gehören z.B. Marketing, Marktforschung, Statistik und Planung, Produkteentwicklung und Geschäftsentscheide, die den Kunden oder die Bank betreffen […].

Der Schutz von Kundendaten, die ins Ausland gelangen, richtet sich nach dem jeweiligen ausländischen Recht. Dessen Bestimmungen regeln Zulässigkeit und Umfang einer Bekanntgabe dieser Kundendaten an Behörden oder weitere Dritte.

Der Kunde nimmt zur Kenntnis, dass das schweizerische Bankkundengeheimnis und Datenschutzrecht in diesen Fällen keinen Schutz gewährt, und entbindet die Bank von ihrer Wahrung.

5

Kanton Bern
Canton de Berne

6

«Wo kein Kläger, da kein Richter…»

- Durchsetzung des privaten Datenschutzrechts via ZGB / ZPO
  - Dispositions- und Verhandlungsgrundsatz (Art. 58/55 ZPO)
  - Beweislast für Persönlichkeitsverletzung und allfälligen Schaden (Art. 8 ZGB)

    Botschaft nDSG, Ziff. 1.7.2 :
    «Auf eine Beweislastumkehr nach dem Beispiel von Artikel 13a des Bundesgesetzes […] über den unlauteren Wettbewerb (UWG) hat der Bundesrat verzichtet»
- Busse bei vorsätzlicher Verletzung von Sorgfaltspflichten (Art. 61 nDSG)
  - auf Antrag einer verletzten Person
  - Beweislast bei Strafverfolgungsbehörden

→ Privatwirtschaft: Beurteilung der Cloud-Risiken für sich selber !

6

Kanton Bern
Canton de Berne

7

Grundrecht auf informationelle Selbstbestimmung

Art. 13 BV Schutz der Privatsphäre

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

BGE 147 I 346 E. 5.3: «Im Bereich des Datenschutzes garantiert das verfassungsmässige Recht auf informationelle Selbstbestimmung, dass grundsätzlich ohne Rücksicht darauf, wie sensibel die Informationen tatsächlich sind, jede Person gegenüber fremder […] Bearbeitung von sie betreffenden Informationen bestimmen können muss, ob und zu welchem Zweck diese Informationen über sie bearbeitet werden».

Art. 35 BV Verwirklichung der Grundrechte

1 Die Grundrechte müssen in der ganzen Rechtsordnung zur Geltung kommen.

2 Wer staatliche Aufgaben wahrnimmt, ist an die Grundrechte gebunden und verpflichtet, zu ihrer Verwirklichung beizutragen.

7

Kanton Bern
Canton de Berne

8

Legalitätsprinzip im öffentlichen Datenschutzrecht

Art. 36 BV Einschränkungen von Grundrechten

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

→ Öffentliche Organe dürfen Personendaten nur bearbeiten, wenn dafür eine gesetzliche Grundlage besteht (z.B. Art. 34 Abs. 1 revDSG)

→ «Bearbeiten» ist jeder Umgang mit Personendaten, auch Bekanntgabe* an einen Auftragsbearbeiter

→ Gesetzliche Erlaubnis zum Outsourcing ist für öffentliche Organe konstitutiv, Anforderungen sind zwingend einzuhalten

8

Kanton Bern
Canton de Berne

9

Anforderungen an Auftragsbearbeitung

Outsourcing von Datenbearbeitung ist nur zulässig, sofern:

- der Auftragsbearbeiter die Daten nur so bearbeitet, wie das öffentliche Organ selbst es dürfte,
- keine Geheimhaltungspflichten entgegenstehen,
- der Auftragsbearbeiter die Datensicherheit gewährleistet und
- Unterbeauftragte nur mit vorgängiger Zustimmung des öffentlichen Organs beizieht,
- keine Daten in Staaten ohne angemessenen Datenschutz übermittelt werden.

Öffentliches Organ bleibt für den Datenschutz verantwortlich, Verstoss gegen gesetzliche Vorgaben ist Grundrechtsverletzung!

9

Kanton Bern
Canton de Berne

10

Vom Risiko im öffentlichen Datenschutzrecht

Grundrechte sind ihrer selbst willen (= nicht erst im Hinblick auf konkrete Nachteile/mögliche Folgeschäden für die betroffene Person) zu schützen

ABER: Verhältnismässigkeit jedes staatlichen Handelns (Art. 5 Abs. 2 BV)
→ auch öffentliches Datenschutzrecht ist risikobasiert

z.B. **Art. 8 nDSG**:

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

Risiko = je nach Eintrittswahrscheinlichkeit einer Grundrechtsverletzung sowie deren Umfang und Schwere bei tatsächlichem Eintritt

10

Kanton Bern
Canton de Berne

11

Cloud: nur «Lawful Access» als Risiko?

«Bei Cloud-Lösungen bestehen grundsätzlich nicht höhere Risiken für die Informationssicherheit und den Datenschutz als bei On-Premise-Lösungen. Das Risikoprofil kann sich aber unterscheiden. Während Schutzziele wie Verfügbarkeit in der Cloud grundsätzlich besser erreicht werden können, gibt es in Bezug auf Cloud-Lösungen von ausländischen Unternehmen ein Risiko im Bereich 'Lawful Access'.»

Quelle: Protokoll des Regierungsrates des Kantons Zürich vom 30.03.2022 («542. Einsatz von Cloud-Lösungen in der kantonalen Verwaltung [Microsoft 365], Zulassung»)

11

Kanton Bern
Canton de Berne

12

Übersicht Cloud-spezifische Risiken

Kernrisiko = Kontrollverlust beim Schutz von Grundrechten !

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

…mmt zu, dass sein Volumenlizenzvertrag […] zusammen mit …kumentation und der Verwendung und Konfiguration der …odukte durch den Kunden die vollständigen und dokumen-…gen des Kunden gegenüber Microsoft […] darstellen».

…r Kunde Microsoft, […] personenbezogene Daten in die Ver-…n von Amerika oder in jedes andere Land zu übermitteln, in … oder ihre Unterauftragsverarbeiter tätig sind, […] ausge-…n anderer Stelle in den DPA-Bestimmungen beschrieben».

…n Unterauftragsverarbeiter beauftragen, bestimmte […] …n für Microsoft zu erbringen. Der Kunde erklärt sich einver-…eine solche Beauftragung erfolgt […] Microsoft stellt Infor-… Unterauftragsverarbeiter auf einer Microsoft-Website zur

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

12

Kanton Bern
Canton de Berne

13

Vertraulichkeit

z.B. **Art. 22 nDSG**:

[2] Das hohe Risiko ergibt sich, insbesondere bei Verwendung neuer Technologien, aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. Es liegt namentlich vor:
a. bei der umfangreichen Bearbeitung besonders schützenswerter Personendaten.

→ 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 (→ ist nachvollziehbar darzulegen)

13

Kanton Bern
Canton de Berne

14

Geheimnisschutz

Darf Cloud-Anbieter (inkl. Mitarbeitende/Subunternehmen) Zugang zu Geheimnis erhalten?

- Unterschiedliche Lehrmeinungen zum Berufsgeheimnis
- Amtsgeheimnis:
  - Richtet sich an Geheimnisträger:in als Einzelperson, nicht an öffentliches Organ
  - «Geheimnis» = nicht allgemein bekannt oder zugänglich
  - Ermöglichen der Kenntnisnahme genügt
  - Art. 320 StGB gilt zzt. für Behördenmitglieder und Beamte, nicht für Hilfsperson

    → Bundesrat: Bekanntgabe an Hilfsperson ohne Einwilligung ist strafbar, indirekte Änderung im ISG (2023)

    BR Keller-Sutter in Fragestunde NR vom 14.03.2022: Änderung wird auch für ICT-Leistungserbringer im Ausland gelten (?), letztlich werden Gerichte im Einzelfall entscheiden (!)

→ Empfehlung: Beizug vorgesetzte Behörde + besondere Vertraulichkeit

14

Kanton Bern
Canton de Berne

15

Ausländische Behördenzugriffe auf Daten in der Schweiz

z.B. **CLOUD Act**:

«This bill amends the federal criminal code to specify that an electronic communication service (ECS) or remote computing service (RCS) provider must comply with existing requirements to preserve, backup, or disclose the contents of an electronic communication or noncontent records or information pertaining to a customer or subscriber, regardless of whether the communication or record is located within or outside the United States.»

– Tatsächlicher Zugriff wäre unzulässige Bekanntgabe an Dritten (kein Staatsvertrag – auch nicht CCC! – und nicht gemäss IRSG), ggf. in Staat ohne angemessenes Datenschutzniveau
– Cloud-Anbieter kann Vertraulichkeit nicht verbindlich versprechen

Deshalb: Unklar, inwieweit Raum für risikobasierten Ansatz besteht → je nach Schutzbedarf unterschiedliche Massnahmen (inkl. Verzicht)

15

Kanton Bern
Canton de Berne

16

Daten über Nutzerinnen und Nutzer

z.B. **Art. 57*j* RVOG**:

[1] Bundesorgane […] dürfen Personendaten, die bei der Nutzung ihrer oder der in ihrem Auftrag betriebenen elektronischen Infrastruktur anfallen, nicht aufzeichnen und auswerten, ausser wenn dies zu den in den Artikeln 57*l*–57*o* aufgeführten Zwecken nötig ist.

– Cloud-Anbieter darf nur Daten und nur zu Zwecken erheben/bearbeiten, wie das öffentliche Organ es dürfte
– Cloud-Anbieter ist nicht «Controller» mit eigenen privaten Interessen: keine Rechtsgrundlage für Bekanntgabe

beitet Personendaten zur Leistungserbringung und für tigkeiten von Microsoft, d.h. «(1) Abrechnungs- und g; (2) Vergütung (z. B. Berechnung von Mitarbeiter- Partner-Incentives); (3) interne Berichterstattung und llierung (z. B. Prognose, Umsatz, Kapazitätsplanung, e); (4) Bekämpfung von Betrug, Cyberkriminalität oder die Microsoft oder Microsoft-Produkte betreffen rbesserung der Kernfunktionalität in Bezug auf Barrie- nschutz oder Energieeffizienz; und (6) Finanzberichter- haltung gesetzlicher Verpflichtungen».

16

Kanton Bern
Canton de Berne

17

Umfassende Risikobeurteilung

z.B. **Art. 22 nDSG**:

3 Die Datenschutz-Folgenabschätzung enthält eine Beschreibung der geplanten Bearbeitung, eine Bewertung der Risiken für […] die Grundrechte der betroffenen Person sowie die Massnahmen zum Schutz […] 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 für die Grundrechte beseitigen oder auf ein tragbares Mass reduzieren

17

Kanton Bern
Canton de Berne

18

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

18

Kanton Bern
Canton de Berne

19

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

19