dsb
datenschutzbeauftragter
kanton zürich

# Datenschutz in der Cloud

Herbsttagung Cloud?! – Sicher!?

Zürich, 11. September 2019

Dr. iur. Bruno Baeriswyl
Datenschutzbeauftragter des Kantons Zürich

# Übersicht

- Datenschutzrechtliche Vorgaben
  - Öffentliche Verwaltung
  - Privatwirtschaft
- Neue datenschutzrechtliche Bestimmungen
  - E-DSG / DSGVO
- Staatliche Zugriffe
  - Cloud Act
- Umsetzung in der Praxis

# Datenschutzrechtliche Vorgaben

- Bearbeiten von «Personendaten»
- Privatwirtschaft
  - Datenschutzgesetz (DSG)
- Öffentliche Organe Bund
  - DSG
- Öffentliche Organe Kantone, Gemeinden
  - (I)DSG Kantone

# Cloud Computing

- Datenbearbeitung durch Dritte
  - Art. 10a DSG / § 6 IDG ZH
- Dritter bearbeitet Daten nach Vorgabe (Umfang, Zweck)
- Dritter gewährleistet die Datensicherheit (Vorgaben, Umsetzung)
- Geheimhaltungsvorschriften werden nicht verletzt (z.B. Berufsgeheimnisse)

# Cloud Computing

- Datenbearbeiter bleibt für den Dritten verantwortlich

- Öffentliche Verwaltung
  - Datenbearbeiter kann Verantwortung nicht delegieren
- Privatwirtschaft
  - Die Verantwortung kann den betroffenen Personen auferlegt werden
  - (AGB / Einwilligung)

# Cloud Computing

## Öffentliche Organe

- Vereinbarung
- Kein Verbot der Auslagerung
- Gewährleistung der Geheimhaltungsvorschriften
- Keine Nutzung der Daten durch Dritte
- Angemessene Datensicherheitsmassnahmen und deren Überwachung

# Cloud Computing

## Privatwirtschaft

- (Freie) Vertragsgestaltung
- Datenschutzrechtliche Grundsätze
  - Einwilligung durch Kunden
- Geheimhaltung (Berufsgeheimnis)
- Bereichsspezifische Regelungen (z.B.: FINMA)

# Cloud Computing

## Datenschutzrechtliche Risiken

- Transparenz über Standorte und Server
- Kontrollmöglichkeiten
  - Abgrenzung der Datenbearbeitungen
  - Prüfungen?
- Gestaltungsraum bei Standardangeboten
  - Anwendbares Recht, etc.
- Durchsetzbarkeit von Ansprüchen
  - Löschungs-, Berichtigungsansprüche

# Cloud Computing

## Datenschutzrechtliche Risiken

- Vertraulichkeit
  - Verschlüsselung; Geheimnisschutz
- Transparenz über Sicherheitsmassnahmen
  - Datenverlust, -missbrauch
- Transparenz über weitere Beteiligte
  - Unterauftragsverhältnisse
- Verfügbarkeit der Dienste
- Transparenz bei Auflösung des Vertragsverhältnisses
  - Datenportabilität, Vernichtung der Daten

# Rechtliche Neuerungen

## DSGVO / GDPR

- Pflichten bei Auftragsverhältnis (Art. 28 DSGVO)
  - (1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser **nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt** und den Schutz der Rechte der betroffenen Person gewährleistet.
  - Unterauftragsverhältnisse, Vertrag (Zweckbindung), Vertraulichkeit, Datensicherheit (Art. 32 DSGVO), Dokumentation etc.

# Rechtliche Neuerungen

## E-DSG

- Auftragnehmer
  - Unterauftragsverhältnisse
  - Meldung von Datenschutzverletzungen
  - Verzeichnis der Bearbeitungstätigkeiten

# Staatliche Zugriffe

- Zwangsmassnahmen im Rahmen der Strafverfolgung / Nachrichtendienste
  - CH → CH-Recht
  - Ausland → ausländisches Recht
  - CH – Ausland → Rechtshilfe
  - USA – USA → US Recht
  - USA – US Firma im Ausland → US Recht !!

# CLOUD Act

## Clarifying Lawful Overseas Use of Data

- CLOUD Act, ergänzt «Stored Communication Act*»
  - https://www.congress.gov/115/bills/s2383/BILLS-115s2383is.pdf
- Zugriff auf Daten, die nicht in den USA gespeichert sind, durch «Law Enforcement»
  - US Unternehmen
- Einsprache
  - weder «US Person» noch US Aufenthalt
  - Verletzung ausländischen Rechts
- Erwägung Gericht

dsb
datenschutzbeauftragter
kanton zürich

* 18 U.S. Code CRIMES AND CRIMINAL PROCEDURE CHAPTER 121— STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

# CLOUD Act

- "A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."

# CLOUD Act

- "… file a motion to modify or quash the legal process where the provider reasonably believes—
- (i) that the customer or subscriber is not a United States person and does not reside in the United States; and
- (ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government…"

# CLOUD Act

- The **court** shall take into account, as appropriate—
  - (A) **the interests of the United States**, including the investigative interests of the governmental entity seeking to require the disclosure;
  - (B) **the interests of the qualifying foreign government in preventing any prohibited disclosure**;
  - (C) the **likelihood, extent, and nature of penalties** to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider;

# CLOUD Act

- (D) the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent of the subscriber or customer's connection to the United States, or if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the nature and extent of the subscriber or customer's connection to the foreign authority's country;
- (E) the nature and extent of the provider's ties to and presence in the United States;
- (F) **the importance to the investigation of the information required to be disclosed**;
- (G) **the likelihood of timely and effective access** to the information required to be disclosed through means that would cause less serious negative consequences; and
- (H) if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the investigative interests of the foreign authority making the request for assistance

# Cloud Computing

## Umsetzung in der Praxis

- Anwendbares Recht / Gerichtsstand
- Ort der Datenbearbeitung (Serverstandort)
- Geheimnisschutz
  - Verwaltung (Amtsgeheimnis)
  - Gesundheitsbereich (Berufsgeheimnis)
  - Finanzbereich (Bankkundengeheimnis)

# Fazit

## Cloud Computing

- (Umfassende) Risikoanalyse
- Datenschutzrechtliche Vorgaben
- Organisatorische und technische Massnahmen

# So erreichen Sie uns


- Adresse — Datenschutzbeauftragter des Kantons Zürich
  Postfach, 8090 Zürich
- Telefon — +41 (0) 43 259 39 99
  8.30 bis 12.00 Uhr und 13.30 bis 17.00 Uhr
- E-Mail — datenschutz@dsb.zh.ch
- Internet — www.datenschutz.ch
  mit verschlüsseltem Kontaktformular
- Twitter — twitter.com/dsb_zh