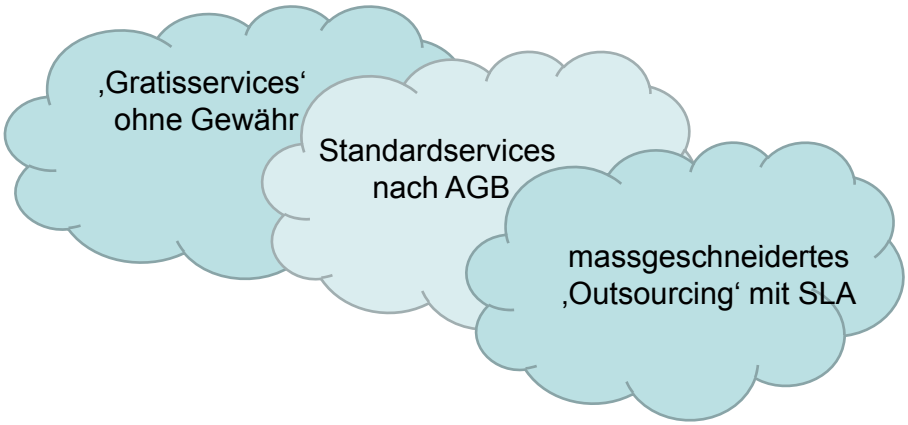
ICT – Recht und Praxis
5. September 2013

Von der Cumuluswolke bis zum Hurrikan: Vertragliche Absicherung cloudspezifischer Risiken

Peter Neuenschwander
Wolfgang Straub

Was ist anders in der Cloud?

‚Cloud' ist schwer fassbar:



2

Was ist anders in der Cloud?

- Fehlende Lokalisierbarkeit der Datenspeicherung
- Eigene Daten in Plattformen, die von Dritten betrieben werden

3

Was ist gefährdet?

- Daten
- Eigene Handlungsfähigkeit
- Compliance mit Vorschriften
- Kostenkontrolle

4

Wem gehören Daten?

- Datenträger → Eigentümer (allenfalls Nutzungs-einschränkungen)
- Schutzrechte (z.B. Urheberrecht) stehen dem Rechteinhaber zu
- Sonderfall Datenbankrechte
- Ansprüche zwischen Kunden und Cloud Provider gemäss Vertrag

5

Wer hat Anspruch auf Daten?

Massnahmen zur Sicherung der Ansprüche bei Insolvenz des Cloud Anbieters:

- Ausschluss eines Retentionsrechts
- Vertragliches Verwertungsverbot von Kundendaten
- Vorsichtsmassnahmen beim "rechtlichen" Zugriff durch Dritte

6

Datensicherheit I

«Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.»

Art. 7 DSG

7

Datensicherheit II

Risiken:

- unbefugte oder zufällige Vernichtung bzw. Verlust
- technische Fehler
- Fälschung, Diebstahl oder widerrechtliche Verwendung
- unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen

8

Datensicherheit III

«Angemessenheit» ist aufgrund folgender Kriterien zu bestimmen:

- Zweck der Datenbearbeitung
- Art und Umfang der Datenbearbeitung
- Einschätzung der möglichen Risiken für die betroffenen Personen
- gegenwärtiger Stand der Technik

→Beurteilung im Einzelfall

9

Zugriff durch Dritte

- US Patriot Act
- Foreign Intelligence Surveillance Act
- US Code 1881a

10

Beispiel einer möglichen Formulierung

"The confidentiality obligations shall not apply to the extent disclosure of confidential information is required to comply with mandatory laws or to comply with the final handout order by a competent judicial body. In the event of a judicial handout request, disclosure will be made only after prior written notice to Customer (where lawfully possible to do so) and Provider will cooperate with Customer regarding the data concerned, the manner of the disclosure or any action, which any of them may elect to take to challenge legally the validity of or otherwise limit that requirement."

11

Compliance I

Bearbeitung von Daten im Ausland

- Rundschreiben FINMA als ‚best practice'?
- Bestimmung des Orts der tatsächlichen Datenbearbeitung/Bearbeitungsmöglichkeit
- Effektive Anonymisierung/Verschlüsselung
- ‚Gleichwertige Datenschutzgesetzgebung , (auch Daten von jur. Pers.) /'hinreichende Garantien' (z.B. EDÖB Mustervertrag)
- Angemessene technische und organisatorische Sicherung (insbesondere Audits)

12

Compliance II

Weitere Problemfelder **Datenschutz**

- Datentrennung zwischen Kunden
- Problematik von Sicherungskopien: Löschung bei Vertragsende/Berichtigungsansprüchen
- Durchsetzung von Ansprüchen gegenüber Mitarbeitenden/Subakkordanten
- Durchführbarkeit von Audits

13

Portierbarkeit

- Portierbarkeit/Pflicht zur Migration von Daten auf ein standardisiertes Format
- Mitlieferung/Portierbarkeit von Benutzerverwaltungsinformationen
- Vertragsauflösungsrechte bei Einstellung der Unterstützung bestimmter Schnittstellen

14

Kostenkontrolle

- Verlust der Kostenübersicht (z.B. Nutzung kostenpflichtiger Services durch Endbenutzer)
- Kontrolle der effektiven Nutzung
- Leistungsbeschreibung
- Versteckter Zusatzaufwand (z.B. Adaptierung, Pflege von Schnittstellen, Drittlizenzen, Support)
- Falsche wirtschaftliche Anreize (z.B. durch Pönalen)

15

Insolvenz

- Bestimmung des anwendbaren Insolvenzrechts
- Probleme der Aussonderung von Daten und Individualentwicklungen
- Externe Speicherung von Sicherungskopien / gekennzeichnete Datenträger im Eigentum des Kunden
- Escrow von Softwareentwicklungen
- Vertraglicher Ausschluss der Verwertbarkeit von Personendaten

16

Früherkennung

Während der Vertragsdauer

- Information über finanzielle Kennzahlen
- Verifikationsmöglichkeit der Informationen durch Audits
- Prüfung der Kreditwürdigkeit durch eine Agentur
- Eventuell Übernahmemöglichkeiten bei Unterschreitung von Schwellenwerten

17

Vertragsbeendigung

- Beschreibung der Prozesse bei Vertragsbeendigung
- Zugangsbeendigung
- Formate der Datenübermittlung, Abnahme,
- Übergabe elektronischer Schlüssel
- Abrechnung

18

Wahrung der eigenen Handlungsfreiheit

- Technische Lock-in-Effekte (Portabilität, Schnittstellen, Standards)
- Auflösungsklauseln für den Insolvenzfall (durch Spezialisten prüfen lassen!)
- (Teil-)Auflösungsoptionen vor Insolvenz
- Aussonderung und Nichtverwertbarkeit von Daten und Individualentwicklungen

19

Fragen, Anregungen, Kritik?

Dr. Peter Neuenschwander
Suffert Neuenschwander & Partner, Zollikon
www.snplegal.com

Dr. Wolfgang Straub
Deutsch Wyss & Partner, Bern
www.advobern.ch

20