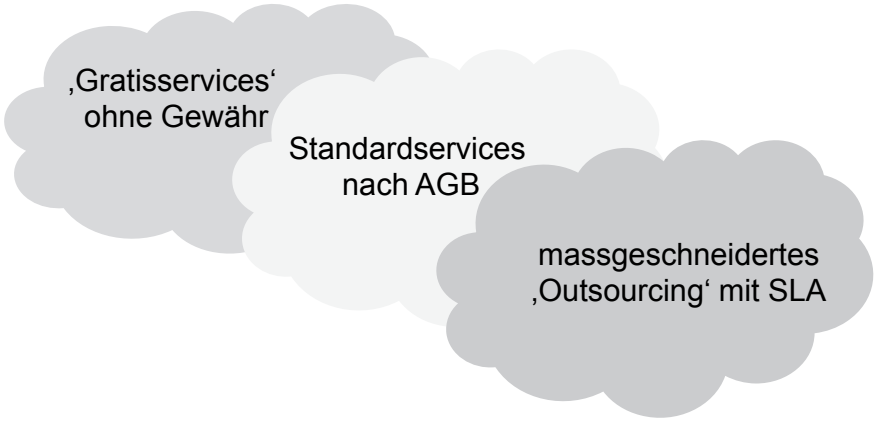
IT Valley Fribourg
Techmeeting 23.03.2017

Vertragliche Absicherung cloudspezifischer Risiken

Wolfgang Straub

‚Cloud' ist schwer fassbar



2

Technische Herausforderungen

- Abhängigkeit von **performanten Netzwerken**
- **Kontrollverlust**
  - Lokalisierbarkeit der Daten
  - Hilfspersonen/Subunternehmer des Providers
  - Eingeschränkte Kontrollmöglichkeiten
    → Audits durch unabhängige Zertifizierungsstellen
- **Integration** mit anderen Systemen und Anwendungen
- **Portabilität der Daten**

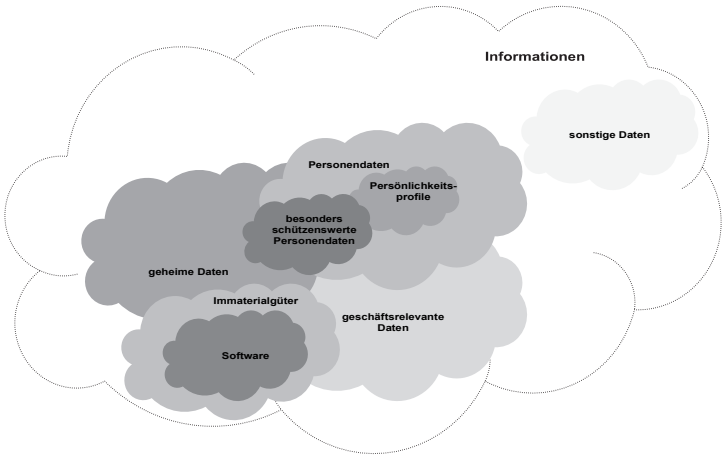
3

Was kann gefährdet sein?

- Daten
- Handlungsspielräume
- Compliance
- Kostenkontrolle

4

Informationen



→ je nach Art der Information gelten unterschiedliche rechtliche Anforderungen

5

Datensicherheit

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

Art. 7 DSG

6

Compliance

Outsourcing der Datenbearbeitung

- Rundschreiben FINMA 2008/7 als ‚best practice'?
- Von wo aus können die Daten bearbeitet werden?
- Bearbeitung im Ausland
  - ‚gleichwertige Datenschutzgesetzgebung, (auch Daten von jur. Pers.) oder 'hinreichende Garantien' (z.B. EDÖB Mustervertrag)
  - angemessene technische und organisatorische Sicherung (insbesondere Audits)
  - Anonymisierung/Verschlüsselung als Lösung?

7

Zugriff durch ausländische Behörden

Mögliche **Anknüpfungen** (z.B. US Patriot Act, Foreign Intelligence Surveillance Act, US Code 1881a):

- Standort des Rechenzentrums
- Sitz oder Kotierung des Unternehmens/Konzerns
- Geschäftsniederlassungen

8

Kostenkontrolle

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

9

Früherkennung von Problemen

Während der Vertragsdauer

- Information über finanzielle Kennzahlen des Provider
- Audit- und Kontrollrechte
- Vertragliches Claim Management Verfahren
- Vertragliches Konflikteskalationsverfahren

10

Vertragsbeendigung

- Beschreibung der Prozesse bei Vertragsbeendigung
- Regelung der Zugangsbeendigung
- Formate und Abnahme der Daten
- Übergabe elektronischer Schlüssel
- Abrechnungsmodalitäten

11

Wahrung der eigenen Handlungsfreiheit

- Lock-in-Effekte vermeiden (Portabilität, Schnittstellen, Verwendung von Standards etc.)
- Vertragliche Auflösungsoptionen
- Auflösungsmodalitäten für den Insolvenzfall (Aussonderung und Verwertungsverbot von Daten und Individualentwicklungen)

12

Vorgehensempfehlungen

- Analyse der **Interessenlage**
- Bestimmung des **auszulagernden Bereiches**
- Analyse der **rechtlichen Anforderungen** Analyse der wirtschaftlichen, technischen und rechtlichen **Chancen und Risiken**
- Festlegung einer **Strategie**
- Festlegung der **Kriterien für die Auswahl** und die Zusammenarbeit mit dem Provider
- Regelung der Zuständigkeiten und **Verantwortlichkeiten** zwischen den Parteien

→ siehe auch *Checkliste Cloud Verträge*

13

Fragen, Anregungen, Kritik?

Dr. Wolfgang Straub
Augsburger Deutsch & Partner
Effingerstrasse 17/Postfach
3001 Bern

wolfgang.straub@ad-p.ch
www.ad-p.ch
www.it-recht.ch

14