Vertrauenswürdiges Cloud Computing - ein Widerspruch?

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Inhaltsüberblick

Was ist Cloud Computing?

Geltung des BDSG für Cloud Computing

Die Verantwortlichkeit für Datenverarbeitung in der Cloud

Auftragsdatenverarbeitung und Datenübermittlung nach BDSG

Grenzüberschreitende Cloud-Services außerhalb EU/EWR

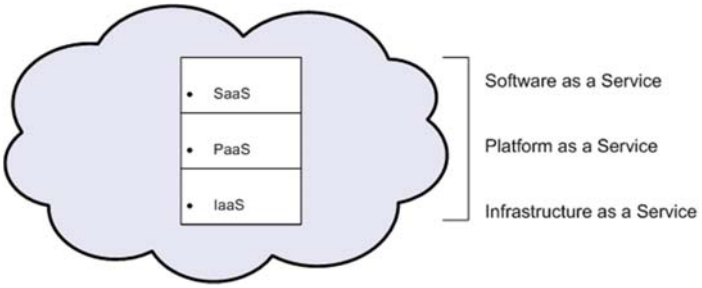
Sonderfall US-EU Safe Harbor

Worauf ist zusätzlich vertraglich zu achten?

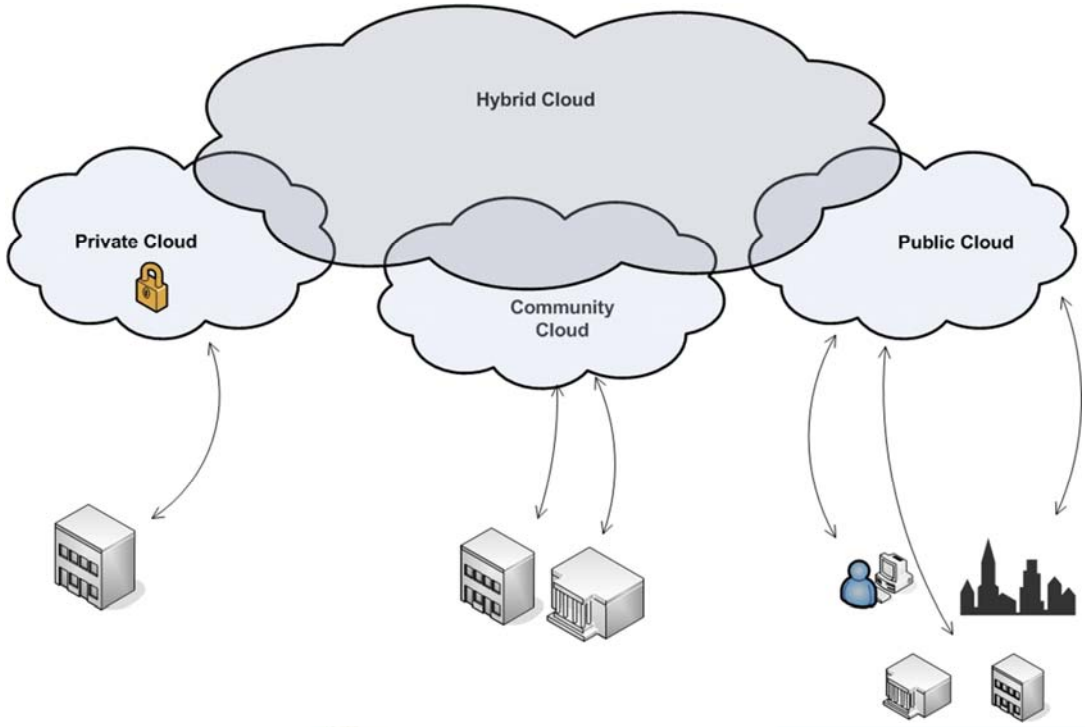
Fazit

Cloud Computing?

- Auslagerung von IT über Netzwerke
- Im Gegensatz zum vollständigen Outsourcing: geteilter Pool skalierbarer Ressourcen
- Gängige Servicemodelle:



Anwendungsmodelle des Cloud Computing



Die Cloud – vertrauenswürdig?

- Microsoft's UK head admitts that no cloud data is safe from the Patriot Act — and Microsoft will hand it over to U.S. authorities. *zdnet.com 28.06.2011*
- Google-Server in Europa vor US-Regierung nicht sicher. *wiwo.de 06.08.2011*
- Cloud-Dienste von Amazon in Irland für mehrere Stunden gestört nach Blitzschlag. Snapshots zur Datensicherung fehlerhaft. *heise.de 08.08.2011*

2) Geltung des BDSG für Cloud Computing

- Anwendbarkeit: personenbezogene Daten, § 3 (1) BDSG

- Anwendbares Recht: Wird durch Sitzlandprinzip bestimmt
- Cloud Services = i. d. R. typische Auftragsdatenverarbeitung nach § 11 BDSG

Allgemeine Vorgaben im Datenschutzrecht

- §§ 33-35 BDSG – regeln konkrete Rechte der Betroffenen
- Allgemeine Grundsätze:
  - Transparenz
  - Information
  - Kontrolle
  - Durchsetzbarkeit

Die Verantwortlichkeit für Datenverarbeitung in der Cloud

- Cloud-Kunde = verantwortliche Stelle, § 3 (7) BDSG
  - Cloud-Kunde – derjenige, der den Dienst in Anspruch nimmt
  - Betroffener ist derjenige, auf den sich die Daten beziehen

- Verantwortlichkeit des Kunden von Cloud Diensten für:
  - Wahrung der Betroffenenrechte
  - Einhaltung gesetzlicher Vorgaben
- Verantwortung im Regelfall nicht übertragbar!
- Es kommt immer darauf an, wer den Datenverarbeitungsprozess tatsächlich beherrscht

Problemfelder im Bereich Cloud Computing

- Umsetzung der allgemeinen Grundsätze von Transparenz, Information, Kontrolle und Durchsetzung
- Keine direkter Einfluss des Cloud-Kunden mehr bei bleibender Verantwortung
- Cloud Provider gibt die Rahmenbedingungen von Datenschutz und Datensicherheit vor
- Grenzüberschreitende Datenverarbeitung und komplizierte Anbieterstrukturen

Auftragsdatenverarbeitung

- Durch Cloud Service werden Daten im Auftrag verarbeitet
- Der Cloud-Kunde ist Auftraggeber
- Der Cloud Service Provider ist weisungsgebundener Auftragnehmer
- Strenge Voraussetzungen – **10 Punkte-Katalog nach § 11 BDSG**
- Dieser betrifft vor allem die Bereiche der
  - Auftragsspezifierung, (z.B. Zweck + Dauer der Datenverarbeitung)
  - Betroffenenrechte
  - Obliegenheiten des Auftragnehmers
  - Kontrollrechte des Auftraggebers

Datenübermittlung

- Ohne Auftragsdatenverarbeitungsverhältnis nur „Übermittlung“ von Daten an Dritte, § 3 (4) Nr. 3 BDSG
- Diese nur dann zulässig, wenn gesetzlich erlaubt
- Möglich: Interessenabwägung nach § 28 (1) Nr. 3 BDSG
- Die Glaubhaftmachung kann jedoch im Einzelfall schwierig sein
- Probleme:
  - Zusätzliche Vertragsgestaltungen zum Betroffenenschutz nötig
  - Mehrere Subunternehmerverhältnisse schwierig

Grenzüberschreitende Cloud-Services außerhalb EU/EWR

- Auftragsdatenverarbeitung nicht möglich, nur noch „Übermittlung“
- Angemessenes Datenschutzniveau im jeweiligen Land erforderlich
- Dies ist nur in wenigen Ländern gewährleistet
- Problem: Sitz des Providers bzw. Serverstandorte außerhalb EU
- Regelungen, die Datenübermittlung dennoch ermöglichen sollen:
  - US-EU Safe Harbor
  - EU Standardvertragsklauseln, ggf. erweitert durch nationale Vorgaben (z.B. BDSG)

7) Sonderfall US-EU Safe Harbor

- Kein angemessenes Schutzniveau in den USA, daher Übermittlung eig. nur in Ausnahmefällen

➢ Safe Harbor-Abkommen zwischen der Europäischen Kommission und dem US Department of Commerce im Jahr 2000

➢ Federal Trade Commission (FTC) soll die Zertifizierung und Einhaltung überwachen

Kritik an Safe Harbor

- Prozess einer inhaltlich nicht geprüften Selbst-Zertifizierung
- Kaum Vorgaben hinsichtlich der Qualität der Datenschutzerklärung
- Kaum Kontrolle der FTC zur Einhaltung der 7 Grundsätze
- Zertifizierung beschränkt sich regelmäßig nur auf bestimmte Arten von Daten
- Kaum Enforcement (Galexia-Studie 2008)
  - Hochpreisige Schlichtungsstellen
  - Keine Sanktionen durch die FTC
  - 54 von 1597 Unternehmen erfüllten formal die Kriterien des Grundsatzes Enforcement

Düsseldorfer Kreis 2010

- Ein datenexportierendes Unternehmen darf sich nicht ohne weiteres auf eine proklamierte Safe Harbor-Zertifizierung des Datenimporteurs verlassen
- Prüfplicht für Mindestkriterien:
  - Zertifizierung gültig?
  - Inwiefern kommt das importierende Unternehmen seinen Informationspflichten gegenüber den von der Datenverarbeitung Betroffenen nach
  - Dokumentation dieser Prüfung

Konsequenzen

- Safe Harbor reicht für deutsche Cloud-Kunden als Sicherheit nicht aus
- Mindestprüfung laut Düsseldorfer Kreis greift inhaltlich zu kurz und verursacht gleichzeitig hohen Aufwand
- Absicherung/Nachweis der Compliance, bestenfalls durch
  - EU Standardvertragsklauseln oder
  - zusätzliche bilaterale Verträge

EU-Standardvertragsklauseln

- Vertragliche Regelung der Datenübermittlung
- Diese müssen unverändert übernommen werden
- Diese reichen für deutsche Cloud-Kunden jedoch nicht bei einer Übermittlung von Daten in ein außereuropäisches Drittland trotz Anerkennung angemessenen Schutzniveaus
- Zusätzlich analoge Anwendung des § 11 (2) BDSG erforderlich
- Empfehlung: Abschluss eines zweiten Vertrags oder eines Annex mit der 10-Punkte-Regelung nach § 11 (2) BDSG

Worauf ist zusätzlich vertraglich zu achten?

- Service Level Agreements und Vertragsstrafen
  - Was wird vertraglich tatsächlich zugesichert?
  - Woran sind Verfügbarkeitsgarantien gebunden?
  - Welche Strafen sind für den CSP vorgesehen?
- Vereinbarung von Sicherheitsstandards und Audits
- Business Continuity Planning und Desaster Recovery
- Haftung des CSP (wofür und mit welcher Summe?)
- Gerichtsstandsvereinbarungen

Fazit

- Kunden sollten CSP sorgfältig auswählen sowie Möglichkeiten der Kontrolle + Durchsetzung der Datenschutzanforderungen suchen und nutzen
- Europäische CSP bevorzugen. Auch Availability Zones sind bieten keine ausreichende Sicherheit.
- Verträge genau prüfen und ggf. nachverhandeln
- Standardisierung und Audits müssen in Zukunft eine größere Rolle spielen
- Cloud Provider hingegen sollten auch im Eigeninteresse nach mehr Transparenz streben; Privacy als Wettbewerbsvorteil

Vielen Dank für Ihre Aufmerksamkeit!

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

TClouds

Trustworthy Clouds
The TClouds project has received funding from the European Union's Seventh Framework Programme ([FP7/2007-2013]) under grant agreement number ICT-257243.

Ninja Marnau und Eva Schlehahn

http://www.datenschutzzentrum.de/

http://www.tclouds-project.eu/