Cloud Computing aus datenschutzrechtlicher Sicht

Thilo Weichert, Leiter des ULD

4. Österreichischer IT-Rechtstag

INFOLAW, 18.06.2010, Wien

ULD

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Inhalt

- Unabhängiges Landeszentrum für Datenschutz – ULD
- Cloud Computing?
- Rechtliche Fragestellungen
- Anwendbarkeit des Datenschutzrechts
- Klärung der Verantwortlichkeit
- Abgrenzung Funktionsübertragung – DV im Auftrag
- Probleme (u. Lösungen): (il)legale Zugriffe, DS-Kontrolle
- Mindestanforderung Auftragsdatenverarbeitung
- Technische und organisatorische Lösungen
- DV außerhalb des EU-/EWR-Raumes
- Diskussionsstand und Handlungsbedarf

Unabhängiges Landeszentrum für Datenschutz

- Datenschutzkontrollbehörde für öffentlichen und nicht-öffentlichen Bereich (u.a. Telemedienanbieter in Sch.Holst.)
- Ausbildung, Beratung und Unterstützung von Betroffenen, Politik, Verbänden, verarbeitenden Stellen, Forschung u. Entwicklung
- Erstellung von Gutachten und Stellungnahmen
- Durchführung von Projekten (z.B. zu Identity-Management PRIME-life. Verbraucherschutz)
- Datenschutz-Gütesiegel und –Audit (seit 2001, incl. European Privacy Seal - EuroPriSe, seit 2008)

Cloud Computing?

- Outsourcing, ähnlich Grid Computing
- Angebote
  Software as a Service (SaaS)
  Storage as a Service (Datensicherung, Archivierung)
  Platform as a Service (PaaS)
  Infrastructure as a Service (IaaS)
- Erscheinungsformen
  Private Cloud
  Public Cloud
  Hybrid Cloud
  Community Cloud

Rechtliche Fragestellungen

- Haftung, Gewährleistung
- Urheberrecht
- Steuer- und Handelsrecht (Revisionsfähigkeit)
- Verbraucherrecht, AGB-Recht
- Strafprozessrecht
- Sicherheitsrecht
- Generell IT-Vertragsrecht
- Zentral: Datenschutzrecht

Begriffe: Cloud-Nutzer, Cloud-Anbieter, Ressourcen-Anbieter

Anwendbarkeit des Datenschutzrechts

- Verarbeitung personenbezogener od. -beziehbarer Daten
- Anonymisierte Datenverarbeitung unproblematisch (unverhältnismäßig großer Aufwand an Zeit, Kosten, Kraft)
- Pseudonyme Datenverarbeitung ist relevant
- Reidentifizierung bei Cloud-Anwendungen i.d.R. immer möglich bei irgendwo vorhandenem Zusatzwissen

Welches nationale Datenschutzrecht?

- Territorialitätsprinzip
- Im EU/EWR-Raum Sitzprinzip (bzgl. Niederlassung)
- Bei Sitz außerhalb EU/EWR Vertretungsmöglichkeit
- Problem: Drittländer, Offshoring, evtl. Vertragslösung

Klärung der Verantwortlichkeit

- § 3 VII BDSG: Verarbeitung für sich selbst bei sich oder „durch andere“
- § 11 BDSG: Bei Datenverarbeitung im Auftrag „ist der Auftraggeber für die Einhaltung der Vorschriften ... über den Datenschutz verantwortlich“

  > Entbindung von Verantwortlichkeit ist nicht zulässig

  > Doppelverantwortung ist möglich
- Gegenstand der Verantwortung

  materielle Zulässigkeit der Verarbeitung (DS, Strafrecht, Zivilrecht usw.)

  Erfüllung der Betroffenenrechte, Haftung (Schadenersatz)

Abgrenzung Funktionsübertragung - DViA

- Datenverarbeitung im Auftrag (DViA) nur im EU/EWR-Raum möglich
- Sonst Funktionsübertragung > §§ 4b, 4c, 28 Abs. 1 Nr. 1, 2 BDSG

  Statt „dienlich“ jetzt „erforderlich“, Erforderlichkeit der Verarbeitung außerhalb des EU/EWR-Raum nicht gegeben

  Kostenersparnis kann „berechtigtes Interesse“ darstellen

  „Schutzwürdiges Interesse“ überwiegt grds. außerhalb EU/EWR-Raum
- Anforderungen nach § 11 BDSG/Art. 17 II EU-DSRL in jedem Fall notwendig, aber nicht hinreichend

Probleme und Lösungen: legaler Zugriff

- „Legaler Zugriff“ durch innerstaatliche Behörden od. Dritte nach nationalem Recht des Dienstleisters (Polizei, Strafverfolgung, Geheimdienste, Finanzbehörden, Konkurrenten)
- Gefährdungen des RiS durch niedrigeres/fehlendes DS-Niveau im Land des Dienstleisters
- Existenzielle Gefährdungen (insbes. in Ländern ohne Grundrechts- und Rechtsschutzstandard, nicht nur China, Iran)
- Techn. Lösung: Verschlüsselung, hinreichende Pseudonymisierung, Verarbeitung in virtuellen Räumen
- Evtl. gesetzliche Pflicht zur Schlüsselherausgabe, Zwangszugriff

Probleme und Lösungen: illegaler Zugriff

- Illegaler Zugriff auch bei hohem Datenschutzstandard nicht auszuschließen mit Konsequenzen auf sämtliche Schutzziele:
  - Vertraulichkeit, - Integrität, - Verfügbarkeit,
  - Authentizität, - Transparenz, - Revisionssicherheit,
  - Unverknüpfbarkeit

Angriff beim „schwächsten Glied“ möglich

Angriffsdetektion oft nicht gesichert

Technisch-organisatorische Lösungen nach § 9 BDSG/Art. 17 EU-DSRL (TOM)

Problem Datenschutzkontrolle

- Datenschutzkontrollen nach § 38 BDSG/Art. 28 EU-DSRL knüpfen an territorialer Datenverarbeitung an
- Grenzüberschreitende (anlasslose) Kontrollen sind faktisch innerhalb von EU/EWR unrealistisch
- Cloud-Nutzung mit Drittlandsbezug ermöglicht Aushebelung der staatlichen Datenschutzkontrolle
- Rückgriff auf Strafermittlungskompetenzen nur bei Datenschutz-Straftatbeständen

Mindestanforderung Auftragsdatenverarbeitung I

§ 11 BDSG seit 1.1.2009 neu geregelt

- Sorgfältige Auswahl des Auftragnehmers (AN) und Unterauftragnehmer durch Auftraggeber (Nutzer)
- Schriftlicher Auftrag mit Benennung von Gegenstand, Dauer, Umfang, Art, Zweck, Betroffene, Datenkorrektur, TOM, Dienstleister, Kontrollen, Weisungen, Vertragsstrafen, abschließende rückstandsfreie Datenlöschung
- Erkennbarkeit des rechnenden Auftragnehmers für Nutzer
- TOM: Benennung der konkreten Instrumente
- Notwendige Kontrollen durch AN
- Initiative Auskunfts- (Kontroll-) Rechte des Nutzers

Mindestanforderung Auftragsdatenverarbeitung II

- Meldepflichten des AN bei Sicherheitsverstößen (incl. den Fällen nach § 42a BDSG)
- Weisungen durch Wahloptionen der Nutzer (AG)
- Vergewisserungspflicht über TOM-Sicherungen ist für Cloud-Nutzer i.d.R. nicht selbst umsetzbar, daher dokumentierte externe unabh. Zertifizierung des AN nötig
- Haftungsregeln
- Vorgehen bei Insolvenz od. Übernahme
- Volle Datenschutzkontrolle n. § 38 BDSG muss möglich sein

Technische und organisatorische Lösungen

Nicht Security by Obscurity, sondern by Transparency

- Virtualisierung einzelner Anwendungen und Nutzungen
- Ausschließliche Zugriffsbeschränkung auf vom Nutzer benannte Berechtigte
- Verschlüsselung und Pseudonymisierung
- Optionsmöglichkeit für bestimmte Länder bzw. Dienstleister
- Anwendungssicherheit
- Ereignismanagement
- Einrichtung eines IT-Sicherheitsmanagements
- Einrichtung eines DS-Managements
- Transparente Auditierung durch unabhängige Stelle (vgl. § 9a BDSG, §§ 43 II LDSG SH)

DV außerhalb des EU-/EWR-Raumes

- Clouds außerhalb EU/EWR-Raum sind generell unzulässig
  > Optionsmöglichkeit der räuml. Beschränkung
- Ausnahmemöglichkeit bei festgestellter Angemessenheit des DS-Niveaus (§ 4b II 2, 3 BDSG): CH, CN, Argent.
- Safe-Harbor-Selbst-Zertifzierung von US-Unternehmen genügt nicht
- EU-Standardvertragsklauseln zur DViA (Art. 26 II EU-DSRL)
- Analog Binding Corporate Rules (BCRs)

Diskussionsstand

- Clouds gibt es auf dem Markt
- Angebotene Clouds i.d.R. intransparent
- Cloudanwendungen finden im Geheimen oder in scheinbar sicheren Räumen statt
- Datenschutzverstöße werden nicht bekannt
- Datenschutzdiskussion erst am Anfang
- Anbieter ignorieren Datenschutzfragen
- Wirtschaftsjuristen verharmlosen Datenschutzfragen

Handlungsbedarf

- Herstellung von Markttransparenz und Transparenz bzgl. Cloud-Datenverarbeitungen
- Öffentliche Diskussion aller Beteiligten über Datenschutzanforderungen
- Erarbeitung von Datenschutzstandards für Clouds (Protection Profiles)
- Etablierung von Auditierungsverfahren für Clouds
- Erarbeitung von Cloud-BCRs
- Evtl. Internationale Verträge zum Cloud-Datenschutz

➢ Trusted and trustworthy clouds – oder nicht

Cloud Computing aus datenschutzrechtlicher Sicht

Dr. Thilo Weichert
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
Independent Center for Privacy Protection Schleswig-Holstein (ICPP)
Holstenstr. 98, D- 24103 Kiel
mail@datenschutzzentrum.de
https://www.datenschutzzentrum.de