# Contra Cloud

Thilo Weichert, Leiter des ULD
Landesbeauftragter für Datenschutz Schleswig-Holstein

DAV-Symposium: In den Wolken – Schutz der anwaltlichen Verschwiegenheitspflicht auch bei grenzüberschreitendem Outsourcing und Cloud-Computing

Berlin, 29.03.2012

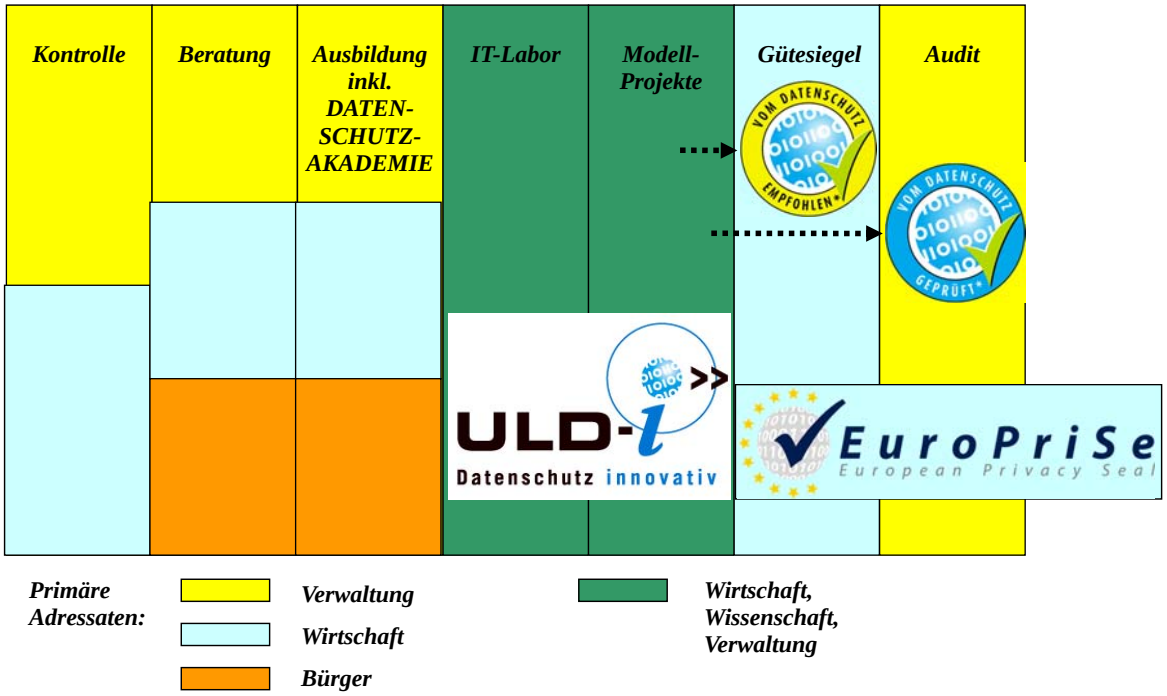
ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein



## *Inhalt*

- Unabhängiges Landeszentrum für Datenschutz - ULD
- Cloud Computing
- Auftragsdatenverarbeitung
- Anwaltliche Schweigepflicht
- Technisch-organisatorische Sicherungen
- Perspektiven

# Unabhängiges Landeszentrum für Datenschutz








# 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 u. Sicherheitsrecht, auch Ausland (USA)
- Generell IT-Vertragsrecht
- Berufsrecht – z. B. Anwaltsrecht
- Zentral: Datenschutzrecht

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





# 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 möglich

> Doppelverantwortung ist möglich

Gegenstand der Verantwortung

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

Erfüllung der Betroffenenrechte, Haftung (Schadenersatz)

Technisch-organisatorische Maßnahmen (TOM)

# Auftragsdatenverarbeitung I

- 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





# 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

# Sonderproblem ausländische Beschlagnahme

- Beschlagnahme für Zwecke Strafverfolgung, Gefahrenabwehr und Nachrichtendienst nach dem Recht des Cloud- od. Ressourcen-Anbieters
- US-Recht (z. B. Patriot Act): Zugriff auf externe Datenbestände über rechtliche Verpflichtung von US-Niederlassungen (trifft auch z. B. deutsche Unternehmen)

> Kompromittierung der Vertraulichkeit





# Anwaltliche Schweigepflicht

- § 203 StGB, § 43a BRAO – parallele Anwendung zu BDSG
- Cloud- und Ressourcenanbieter ist kein Gehilfe (Angestellter)
- Offenbarung bei faktischer Zugriffsmöglichkeit > bei Lesbarkeit Einsatz unzulässig
- Anwendbarkeit der datenschutzrechtlichen Aufsicht (§ 38 BDSG) in jedem Fall bei TOM
- Rolle der Kammeraufsicht?

# Problem: (il)-legaler Zugriff

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

Angriff beim „schwächsten Glied“ möglich

Angriffs- und Zugriffsdetektion oft nicht gesichert

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





# Technisch-organisatorische Maßnahmen

Nicht Security by Obscurity, sondern by Transparency

- Virtualisierung einzelner Anwendungen und Nutzungen
- Zugriffsbeschränkung auf vom Nutzer benannte Berechtigte
- Verschlüsselung und Pseudonymisierung
- Verteilte Cloud
- 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

- Personenbeziehbare 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-Zertifizierung von US-Unternehmen genügt nicht
- EU-Standardvertragsklauseln zur DViA (Art. 26 II EU-DSRL)
- Analog Binding Corporate Rules (BCRs)





# Handlungsbedarf

- Herstellung von Markttransparenz und Transparenz bzgl. Cloud-Datenverarbeitungen
- Bewusstseinsbildung bei Beteiligten
- Erarbeitung von Datenschutzstandards für Clouds (Protection Profiles, vgl. Orientierungshilfe der DSB-Konferenz http://www.datenschutz.hessen.de/download.php?download_ID=237 )
- Etablierung von Auditierungsverfahren für Clouds
- Europäische Datenschutz-Grundverordnung
- Erarbeitung von Cloud-BCRs/Standardverträgen
- Evtl. Internationale Verträge zum Cloud-Datenschutz

➢ Trusted and trustworthy clouds – **oder gar nicht**

# „Contra Cloud“ bei Anwaltsanwendungen

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