Cloud Computing: datenschutz- und arbeitsrechtliche Anforderungen

Thilo Weichert, Leiter des ULD

Global – Digital - Total

8. dtb-Forum für Arbeitnehmervertreter 2013

Grenzenlose Überwachung? NICHT mit uns!
Die Zukunft des Datenschutzes gestalten

5. November 2013, Berlin

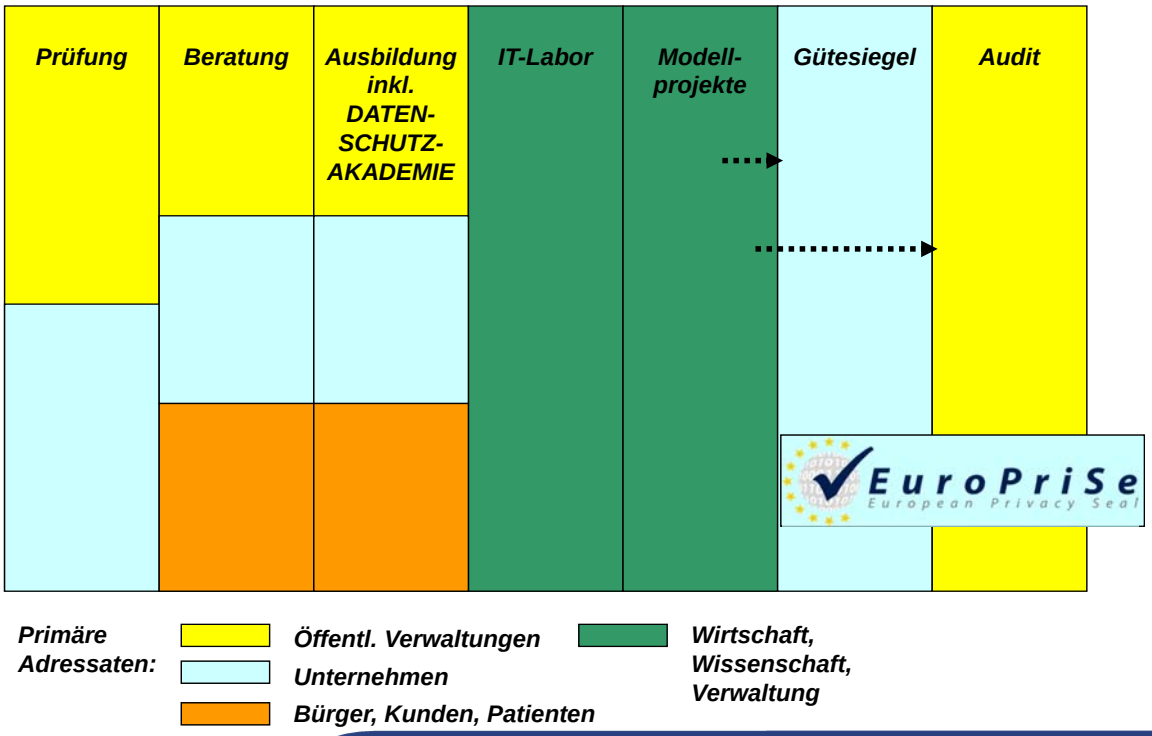
ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Inhalt

- Unabhängiges Landeszentrum für Datenschutz – ULD
- Cloud Computing
- Datenschutzrecht
- Verantwortlichkeit
- Auftragsdatenverarbeitung
- Besonderer Vertrauensschutz
- Datenzugriff durch Behörden (und Dritte)
- Ausländische Cloud
- Mitbestimmung
- Technisch-organisatorische Maßnahmen
- Handlungsoptionen

Kurzvorstellung: Was macht das ULD?

Datenschutz und Informationsfreiheit



Cloud Computing?

= IT-Outsourcing:

Weltweite Verfügbarkeit, Keine Hard- und Softwarepflege, Stufenfreie Skalierbarkeit

Angebote

- Software as a Service (SaaS)
- Storage as a Service (Datensicherung, Archivierung)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Erscheinungsformen

- Private C. - Public C. - Hybrid C. - Community C.
- Unternehmens-Cloud – Nutzer-Cloud

Rechtliche Fragestellungen

- Haftung, Gewährleistung
- Urheberrecht
- Steuer- und Handelsrecht (Revisionsfähigkeit)
- Verbraucherrecht, AGB-Recht
- Strafprozessrecht u. Sicherheitsrecht, evtl. Ausland (USA)
- Generell IT-Vertragsrecht
- Berufsrecht – z. B. Anwaltsrecht
- Zentral: (Arbeitnehmer-) Datenschutzrecht

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

Verantwortlichkeit

§ 3 VII BDSG: Verarbeitung für sich selbst bei sich oder „durch andere“ (Art. 2 d, e EG-DSRl)

§ 11 BDSG: Bei Datenverarbeitung im Auftrag „ist der Auftraggeber für die Einhaltung der Vorschriften ... über den Datenschutz verantwortlich“ (Art. 17 II, III EG-DSRl)

> 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

Besondere Vertraulichkeiten

- Berufliche Schweigepflicht: u. a. § 203 StGB – parallele Anwendung zu BDSG
- Sozialgeheimnis (§ 35 SGB I),
- Steuergeheimnis (AO)
- Personalaktengeheimnis

> Cloud- und Ressourcenanbieter ist nicht Teil der verantwortlichen Stelle > eingeschränkte AG-Kontrolle

> Offenbarung schon bei faktischer Zugriffs- bzw. Lesemöglichkeit

> Anwendbarkeit der datenschutzrechtlichen Aufsicht (§ 38 BDSG) > zusätzliche TOM nötig

Problem Datenzugriff

- 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 u. Speicherortkontrolle oft nicht gesichert

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

Ausländischer Behördenzugriff

- Datennutzung für Zwecke Strafverfolgung, Gefahrenabwehr, Besteuerung, Nachrichtendienst gemäß Recht des Cloud- od. Ressourcen-Anbieters
- US-Recht (insbes. Patriot Act und FISA): evtl. keine Auskunftsbefugnis d. Cloud-Anbieters, keine Betroffenenrechte, kein Rechtsschutz
- Etvl. Zugriff auf externe Datenbestände über rechtliche Verpflichtung von US-Niederlassungen (trifft mögl.w. deutsche Unternehmen)

> Kompromittierung der Vertraulichkeit

> Direkte Nachteile denkbar (z. B. Reiseverbote)

DV außerhalb des EU-/EWR-Raumes

- Personenbeziehbare Clouds außerhalb EU/EWR-Raum sind generell unzulässig, aber Problem GB (Tempora - GCHQ)

  > Optionsmöglichkeit der räumlichen Beschränkung
- Ausnahmemöglichkeit bei festgestellter Angemessenheit des DS-Niveaus (§ 4b II 2, 3 BDSG): CH, CN, Argentinien
- Safe-Harbor-Selbst-Zertifizierung von US-Unternehmen genügt nicht
- EU-Standardvertragsklauseln zur DViA (Art. 26 II EU-DSRL)
- Analog Binding Corporate Rules (BCRs)

Mitbestimmung beim Cloud Computing

- Betriebsrat (BR) zuständig für Persönlichkeitsschutz der Arbeitnehmer (AN) § 75 Abs. 2 BetrVG
- Überwachungsbefugnis des Betriebsrats (BR) § 80 I Nr. 1 BetrVG: DSR-schützt Arbeitnehmer
- Informationspflicht des AG gegenüber BR § 80 II 1 BetrVG, Cloud Computing ist wesentlich
- Kontrollmöglichkeiten des BR (evtl. Einbeziehung von Sachverständigen, § 80 III BetrVG)
- Mitbestimmungspflicht nach § 87 I Nr. 6 BetrVG bei DViA mit eigener Überwachungsqualität
- Möglichkeit der Einschaltung der DS-Aufsicht (§ 38 BDSG)

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)

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 (evtl. Zertifizierung)
- Erarbeitung von Cloud-BCRs/Standardverträgen
- Evtl. Internationale Verträge zum Cloud-Datenschutz

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

Cloud Computing: datenschutz- und arbeitsrechtliche Anforderungen

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