Cloud-Zertifizierung aus Sicht des Datenschutzes

Thilo Weichert, Leiter des ULD

Dezentral und mobil: die Zukunft der Datenverarbeitung

A-i3/BSI Symposium

17.04.2013, Ruhr-Universität Bochum

ULD

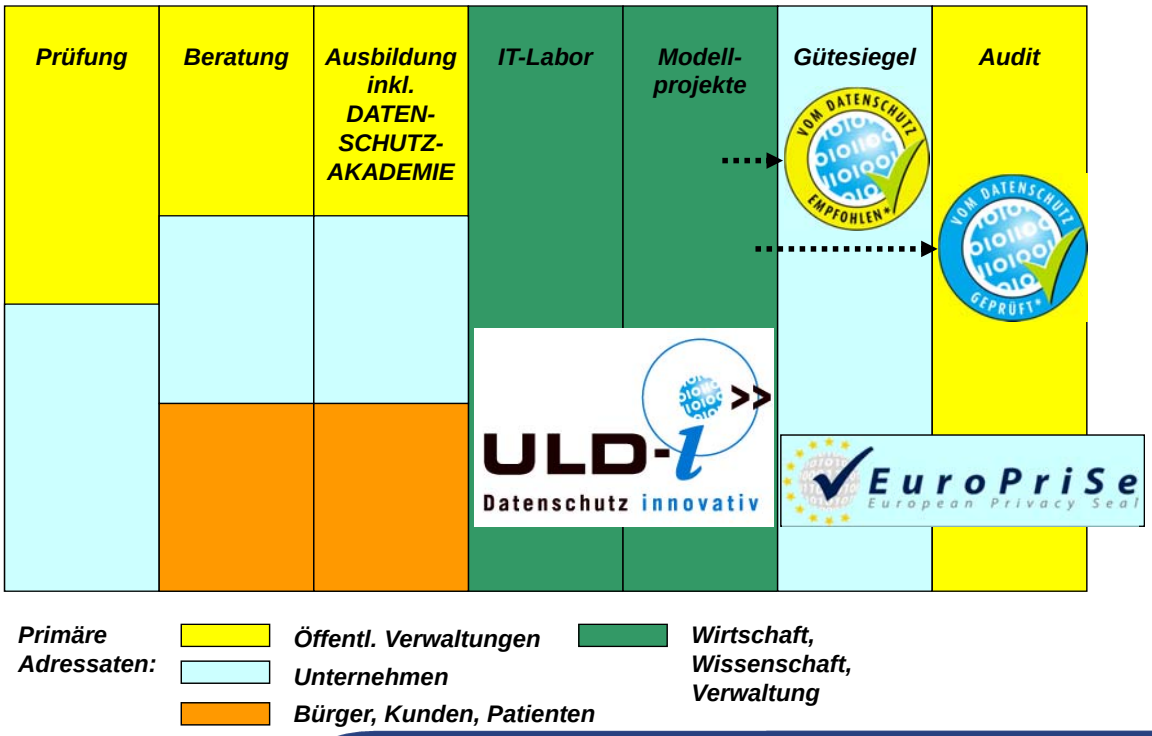
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Inhalt

- Unabhängiges Landeszentrum für Datenschutz – ULD
- Datenschutzzertifizierung
- Cloud Computing
- Probleme komplexer Auftragsdatenverarbeitung
- Kriterien Rechtmäßigkeit
- Entwurf Europäische Datenschutz-Grundverordnung (EU-DSGVO)
- Kritik und Fazit

Kurzvorstellung: Was macht das ULD?

Datenschutz und Informationsfreiheit



Grundlagen Datenschutzzertifizierung

§ 9a Bundesdatenschutzgesetz

Zur Verbesserung des **Datenschutzes** und der **Datensicherheit** können Anbieter von Datenverarbeitungssystemen und -programmen und Daten verarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter **prüfen** und **bewerten** lassen sowie das Ergebnis der Prüfung **veröffentlichen**. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes **Gesetz** geregelt.

Datenschutzzertifizierung in Schl.-Holstein

§ 4 Abs. 2 LDSG SH: Produkte, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren festgestellt wurde, sollen vorrangig eingesetzt werden. Die Landesregierung regelt durch Verordnung Inhalt, Ausgestaltung und die Berechtigung zur Durchführung des Verfahrens.

> **Datenschutz-Gütesiegel Schleswig-Holstein**

§ 43 Abs. 2 LDSG SH: Öffentliche Stellen können ihre technischen und organisatorischen Maßnahmen bei der Verarbeitung personenbezogener Daten sowie die datenschutzrechtliche Zulässigkeit der Datenverarbeitung durch das Unabhängige Landeszentrum für Datenschutz prüfen und beurteilen lassen.

> **Datenschutz-Audit Schleswig-Holstein**

§ 43 Abs. 3 S. 2 LDSG SH: Es (das ULD) berät nicht-öffentliche Stellen auf Anfrage in Fragen von Datenschutz und Datensicherheit.

> **Europäisches Datenschutz-Gütesiegel** (European Privacy Seal)

Zielsetzungen Datenschutzzertifizierung

- Präventive Grundrechtssicherung
- Kollateral-Effekt: Sicherung der Vertraulichkeit generell, z. B. auch bzgl. Geschäftsgeheimnissen
- Kundenbindung, Wettbewerbsfaktor
- Teil der Unternehmens-Compliance (Verhinderung von Sanktionen)

Erfolgsfaktoren für Zertifizierung

- ***Zertifizierungsstelle(n)***
  Unabhängigkeit und fachliche Qualifikation
- **Zertifizierungsstandards**
  Gesetz, evtl. Datenschutzmehrwert, internationale technische und organisatorische Standards
- **Transparenz**
  Vergabekriterien, Eigenschaften des Produktes/Verfahrens
- **Nachhaltigkeit**
  Dauer der Geltung
  Regelmäßige Überprüfung der Einhaltung der Kriterien

Besonderheiten Cloud Computing

- Vernetzung
- Arbeitsteilung u. geteilte Verantwortung/-lichkeit
- Hohe technische Komplexität
- Geringe Transparenz
- (Oft) Internationalität/Globalität mit unterschiedlichen Rechtsregimes

Schutzziele

- Integrität (Zurechenbarkeit, Unversehrtheit)
- Vertraulichkeit (Unbeobachtetheit)
- Verfügbarkeit (jederzeitige Find- und Nutzbarkeit)
- Transparenz (Revisionssicherheit)
- Intervenierbarkeit (Eingreifbarkeit, Abstreitbarkeit)
- Nichtverkettbarkeit (Zweckbindung, Zwecktrennung, Datensparsamkeit)

in einem verteilten komplexen System

> hohe technische, rechtliche u. organisatorische Anforderungen an Dienstleister und Dienstleistung

Rechtliche Konstruktion

Auftragsdatenverarbeitung (§ 11 BDSG, Art. 17 Abs. 2 EG-DSRI, Art. 26 EU-DSGVO-E):

- Rechtliche Verantwortung verbleibt beim Auftraggeber
- Dokumentierter und gelebter Auftrag:
  - Festlegung von Gegenstand, Dauer, Umstand, Zweck
  - Technisch-organisatorische Maßnahmen
  - Datenkorrektur, Betroffenenrechte, Löschung n. Abschluss
  - Qualitätssicherung und Kontrolle
  - Unterauftragsverhältnisse
  - Anzeige- und Meldepflichten
  - Weisungen

Cloud-Probleme bei Auftragsverarbeitung

- Spannung zw. faktischer Macht des Auftragnehmers (AN) und Inkompetenz und Verantwortlichkeit des Auftraggebers (AG)
- Insbesondere Intransparenz: Wo werden von wem unter welchem Rechtsregime welche Daten verarbeitet?
- **Ausgleich des Ungleichgewichts** und des Kontrolldefizits durch Zertifizierung mit dem Ziel der Ermöglichung von Rechtskonformität

> Sicherung von Transparenz und Intervenierbarkeit für Auftraggeber, Aufsichtsbehörde und Betroffene

Bewertungskriterien bei Zertifizierung

- Rechtliche Zulässigkeit der Datenverarbeitung (AG)
- Beachtung der Rechte der Betroffenen (AG, AN)
- Transparenz und Revisionssicherheit (AG, AN)
- Datensparsamkeit/Datenvermeidung (AG, AN)
- Datensicherheit (AN)
- Funktionstüchtiges Datenschutzmanagement (Audit) (AN)
- Evtl. besonderer Mehrwert (datenschutzfördernde Eigenschaften) (AN)

Verfahrensanforderungen Zertifizierung

- Allgemein gültige öffentliche Kriterienkataloge
- Qualifizierte technische und rechtliche Gutachter durch Akkreditierung (Fachkunde, Zuverlässigkeit, Unabhängigkeit)
- Gutachterbeauftragung durch Unternehmen (kostenpflichtig)
- Qualifizierungsprozess des Target of Evaluation (ToE) unter Einschaltung des Unternehmens (AN)
- Zertifizierung durch unabhängige Audit- (Erteilungs-) stelle mit Veröffentlichung von (Kurz-) Gutachten u. Aufnahme in Register (Internet) (gebührenpflichtig)
- Nutzung des Siegels für Werbung und Marketing
- Rezertifizierung nach Fristablauf od. wesentlicher Änderung

Regelungskonzepte nach EU-DSGVO

Art. 39 des Entwurfs (evtl. in Kombination mit Art. 26, 39a)

- Kommissionsvorschlag 1/2012: delegierter Rechtsakt und technische Standards der EU-Kommission
- Parlamentsberichterstatter 12/2012: Unabhängigkeit der Erteilungsstelle, delegierter Rechtsakt der EU-Kommission nach Stellungnahme des EU-DS-Ausschusses
- Kompetenzzentrum Trusted Cloud 2/2013: Entbindung von Verantwortlichkeit bei DViA über Zertifikat, Kontrollpflicht der Erteilungsstelle, Festlegung der Kriterien durch Einvernehmen zw. DS-Behörden und DV-Verbänden, Anforderung an Akkreditierung der Erteilungsstelle (unabhängig, geeignet), Haftung der Erteilungsstelle

Kritik I

- Rechtmäßigkeitsfiktion von Zertifikat beeinträchtigt Betroffenenrechte (Umkehr der Beweislast)
- Einvernehmen: Zu Kontrollierende dürfen nicht Kontroll- und Akkreditierungskriterien festlegen = Letztentscheidung muss bei Erteilungs- (Akkreditierungs-) Stelle liegen
- Kriterien müssen fachlich auf rechtlicher Grundlage festgelegt werden, sind gebunden, nicht verhandelbar
- (Private) Gutachter und (hoheitliche?) Erteilungsstelle sollten getrennt werden
- Vertrauenswürdigkeit der Erteilungs- und Akkreditierungsstellen unsicher

Kritik II

- Es fehlen Transparenz-Regelungen
- Technisch-organisatorische Zertifizierung ist nicht Rechtmäßigkeit/Datenschutzkonformität
- Target of Evaluation (Storage/Software/Infrastructure/ Platform as a Service) ist nicht klar abgrenzbar
- Haftungsfreistellung gefährdet Betroffenenrechte

Schlussfolgerungen

Cloud-Zertifizierung? Ja bitte, aber nur, wenn ...

- Verfahren, Kriterien und Ergebnisse transparent sind
- Kriterien Rechtskonformität abbilden
- keine Beschneidung, sondern Verstärkung von Betroffenenrechten erfolgt (z. B. Auskunft, Haftung, Rechtsweg)
- Erteilungs- (Zertifizierungs-) Stelle kompetent und unabhängig (u. a. ohne finanzielles Interesse) ist

Cloud-Zertifizierung aus Sicht des Datenschutzes

Dr. Thilo Weichert

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

Holstenstr. 98, D- 24103 Kiel

mail@datenschutzzentrum.de

https://www.datenschutzzentrum.de/