Datenschutz-Zertifizierung von IT-Produkten

Erfahrungen mit dem Datenschutzgütesiegel und EuroPriSe

Thilo Weichert, Leiter des ULD

Symposium zu 15 Jahre TELEPAXX

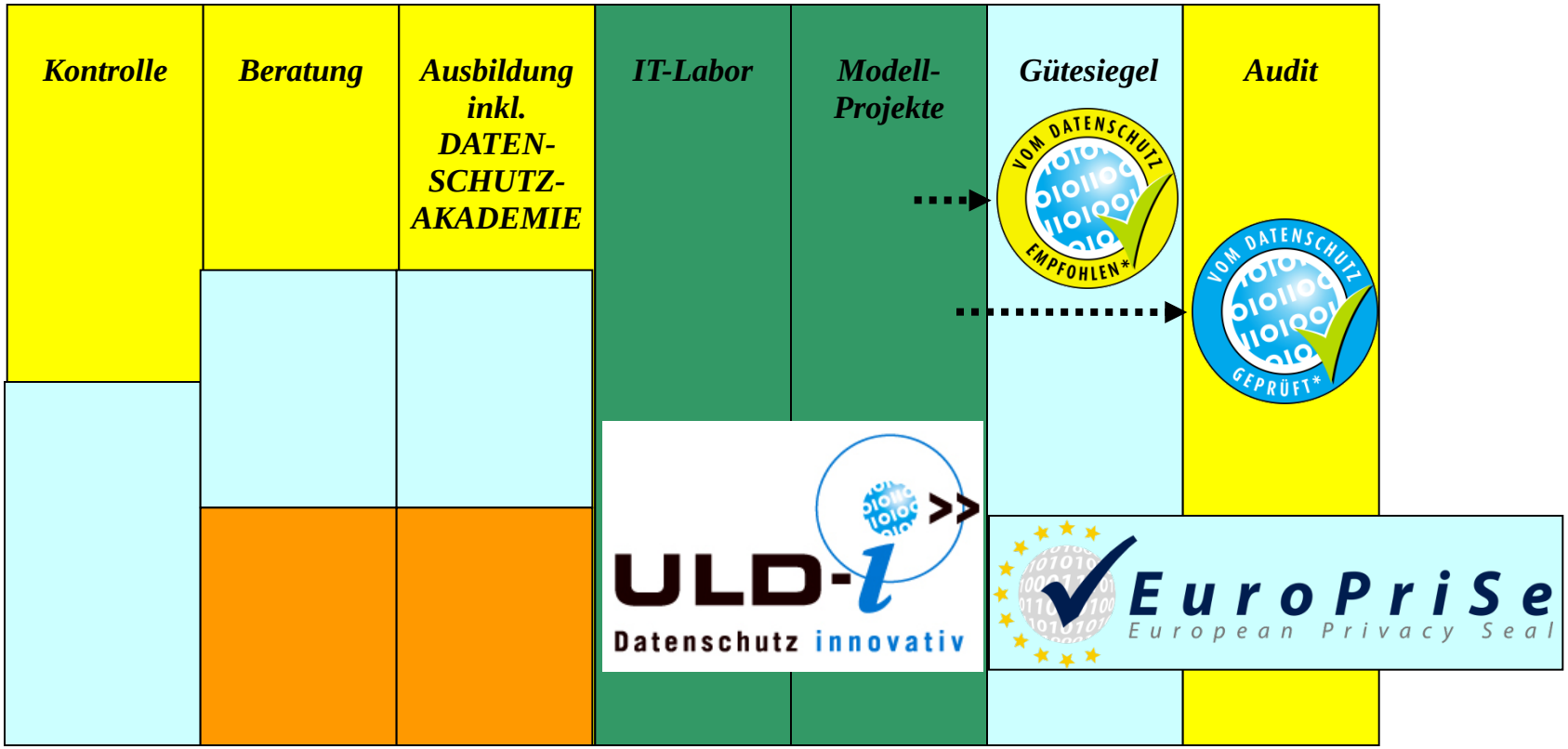
Museum Industriekultur Nürnberg

Montag, 04.07.2011

Inhalt

- Unabhängiges Landeszentrum für Datenschutz – ULD
- Datenschutz schadet oder nützt
- Entwicklungen im In- und Ausland
- Nutzen, Mehrwert und Zielsetzung
- Erfolgsfaktoren für Zertifizierung
- Datenschutzgütesiegel Schleswig-Holstein
  – European Privacy Seal (EuroPriSe)
- Kriterien, Ablauf und Erfahrungen bei Zertifizierungen
- Stiftung Datenschutz
- Perspektiven

Unabhängiges Landeszentrum für Datenschutz



Datenschutz schadet…

- **kostet Geld**
- **produziert organisatorischen Aufwand**
- **hetzt Arbeitnehmer auf**
- **hindert ökonomische internationale Entfaltung**
- **verursacht Ärger mit Aufsichtsbehörden**
- **produziert Negativschlagzeilen**
- **beeinträchtigt u. U. das Unternehmensimage**

... kann aber auch nützlich sein

- **schützt nicht nur Personendaten, sondern auch Geschäftsgeheimnisse**
- **fördert eine ordnungsgemäße Unternehmens-IT**
- **unterstützt ein positives Klima zu Mitarbeitern**
- **schafft Vertrauen und bindet Kunden**
- **schafft Sicherheit vor öffentlichen Angriffen und bei Behördenkontrollen**

> Tue Gutes und sprich darüber!

> Lass Dich zertifizieren!

Entwicklung von Auditierungen

1996	provet-Gutachten für Online-Multimedia-Dienste
1997	Programmregelung § 17 MediendiensteStV
2000	Landesdatenschutzgesetz SH (§§ 4 II, 43 II)
2001	Gutachten Modernisierung des Datenschutzrechts
2001	§ 9a BDSG
2002/03	EU-Förderung DS-Gütesiegel/Audit und Auszeichnung durch EU
2000er	zunehmende Zertifizierungsangebote durch Private
2007	erstmals DS-Zertifizierung von ausländischen (US-)Produkten
2007	Start European Privacy Seal (EuroPriSe)
2009	Scheitern eines Bundesdatenschutzauditgesetzes
2009	Schwarz-gelbe Koalitionsvereinbarung: Stiftung Datenschutz

§ 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.“

Datenschutzaudit in anderen Staaten

- USA: seit 90er Jahre Privacy Seal Programs (z.B. BBB, TRUSTe), technisch orientiert, kein DS-Gesetz
- Japan: seit 1986 Zertifizierung statt Gesetz
- Schweiz: seit Ende 90er private Zertifizierung, 2007 Verordnung über die Datenschutzzertifizierungen
- Frankreich: gesetzliche Regelung ohne Praxis, 2009 Senatsbericht begrüßt und unterstützt EuroPriSe
- EU: Kommission fördert Zertifizierung und erwägt Regulierung

Nutzen und Mehrwert

durch

- **Bestätigung**
- **Akzeptanz**
- **Vertrauen**
- **Marktvorteil**

für

- **Produzenten und Verkäufer**
- **Verbraucher und Nutzer**
- **Markt**
- **Aufsichtsbehörden**

Zielsetzung

- mehr Transparenz
- mehr Compliance (Gesetzeskonformität)
- mehr Privatheit
- mehr Verbraucherschutz
- mehr Vertrauen in IT-Anwendungen
- geringeres Risiko bei IT-Anwendungen
- europaweite und internationale Wirkungen

Erfolgsfaktoren für Zertifizierung

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

Datenschutzgütesiegel SH - EuroPriSe

- (seit 2001 SH, seit 2008 EuroPriSe)
- Allgemein gültige öffentliche Kriterienkataloge
- Qualifizierte technische und rechtliche Gutachter durch Akkreditierung (Fachkunde, Zuverlässigkeit, Unabhängigkeit)
- Gutachterbeauftragung durch Unternehmen (kostenpflichtig)
- Qualifizierungsprozess unter Einschaltung von Auditstelle, Gutachter und Unternehmen
- Zertifizierung mit Veröffentlichung von Kurzgutachten u. Aufnahme in Register (Internet) (gebührenpflichtig)
- Nutzung des Siegels für Werbung und Marketing
- Rezertifizierung nach 2 Jahren od. wesentlicher Änderung

Allgemeine Prüfkriterien

- Rechtliche Zulässigkeit der Datenverarbeitung
- Beachtung der Rechte der Betroffenen
- Transparenz und Revisionssicherheit
- Datensparsamkeit/Datenvermeidung
- Datensicherheit
- Funktionstüchtiges Datenschutzmanagement (Audit)
- Besonderer Mehrwert (datenschutzfördernde Eigenschaften)

Besondere Prüfkriterien

- Nationales Datenschutzrecht bzw. europäische Richtlinien und Regeln zum Datenschutz (EU-DSRL, ePrivacy-Directive, Art. 29-Arbeitspapiere, Rspr. EuGH usw., evtl. nat. Anforderungen)
- Datensicherheitsstandards (BSI-IT-Grundschutzkataloge, Common Criteria, ISO 27000)
- Prüfkomplexe, beschrieben im Anforderungskatalog:
  1. grundsätzliche Fragestellungen
  2. Rechtmäßigkeit der Datenverarbeitung
  3. Techn. und organisator. Datensicherheitsmaßnahmen
  4. Betroffenenrechte

Ablauf

- Evaluierung IT-Produkt od. -Dienstleistung (ToE – Target of Evaluation) durch rechtl. und technischen Gutachter
- Überprüfung des Gutachtens durch unabhängige Zertifizierungsstelle (Vollständigkeit, Nachvollziehbarkeit, Datenschutzkonformität)
- Evtl. Rückkoppelung nach Nachbesserung, evtl. Beendigg.
- Zertifizierung für 2 Jahre, vereinfachte Rezertifizierung, Veröffentlichung Kurzgutachten, Werbemöglichkeit
- Monitoring bei Dienstleistungen/Diensten nach 8/16 Mon.
- Freiwilliger Update-Check für Produkte
- Im Beschwerdefall Klärung mit Gutachter und Anbieter

Akkreditierung von Sachverständigen

- Akkreditierung für die Bereiche Recht und Technik
- Gütesiegel SH: Nachweis der Unabhängigkeit und Fachkunde durch Dokumente
- EuroPriSe: Teilnahme an Ausbildungsworkshop, Erstellung eines Trainingsgutachtens

  Akkreditierung für einen oder beide Bereiche für drei Jahre

  Verlängerung um zwei Jahre bei erfolgreicher Begutachtung od. weiterer Workshopteilnahme

Erfahrungen in Schleswig-Holstein

- 47 Einzelsachverständige, davon 24 R, 17 T, 6 R+T
- 12 sachverständige Prüfstellen, davon 1 R, 2 T, 9 R+T
- 69 zertifizierte Produkte, über 20 auditierte Verfahren

  Bspl.: e-pacs von TELEPAXX: Erstzertifizierung 27.05.2003, 3 Rezertifizierungen, zuletzt 26.04.2010

> Interessant und bezahlbar für kleine, mittlere und große Unternehmen

> Anerkennung durch Fachöffentlichkeit, Verbraucherschutz und Aufsichtsbehörden

> Wettbewerbsvorteil v.a. in sensiblen Bereichen (Medizin, Soziales, Internet, Kundendatenverarbeitung)

EuroPriSe

- Einführung als Projekt Juni 07 – Februar 09
- Markteinführung seit März 2009 durch ULD
- 118 zugelassene Experten in 15 Ländern (einschließlich Argentinien, Taiwan & U.S.)
- 19 (Erst-) + 2 (Rezert-) abgeschlossene Verfahren
- Unterstützt vom EDPS
- Vorbildlich lt. französischem Senatsbericht (06/09)
- EU-Parlament fordert Entwicklung eines Systems zur Kennzeichnung von Websites nach dem Vorbild von EuroPriSe (12/2010)

Projekt-Partner:

CNIL
Agencia de Protección de Datos de la Comunidad de Madrid
HRSJ
Ernst & Young
TÜViT
ITA
BORKING CONSULTANCY
VaF

Stiftung Datenschutz

- Erstmalige Erwähnung 2008 durch FDP-Abgeordnete
- Aufnahme in Koalitionsvereinbarung
- 5/2010 FDP-Eckpunktepapier - Aufgaben

  Bildung und Aufklärung

  Datentest (ähnlich Warentest)

  Datenschutzzertifzierung

  (Datenschutzforschung?)
- Organisatorische Vorgaben: Federführung Bundesinnenministerium, Stiftung privaten Rechts, Anschubfinanzierung 2011 10 Mio. Euro

Perspektiven

- Angebot von Zertifikaten durch verschiedene Stellen, künftig Stiftung Datenschutz
- Ineinandergreifen von regionalen/nationalen/europäischen Zertifikaten
- Angleichung von Datenschutzstandards auf hohem Niveau
- Abstimmung mit bestehenden Zertifikaten und Standards (BSI-Grundschutz, Common Criteria, ISO)
- Organisierte Kooperation zwischen Kontrolle und Zertifizierung bei Wahrung der Unabhängigkeit
- Entwicklung globalen Kriterien für Datenschutz und Datensicherheit

Datenschutz-Zertifizierung von IT-Produkten

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